]

Universidade do Estado do Rio de Janeiro

Centro de Ciências Sociais

Faculdade de Direito

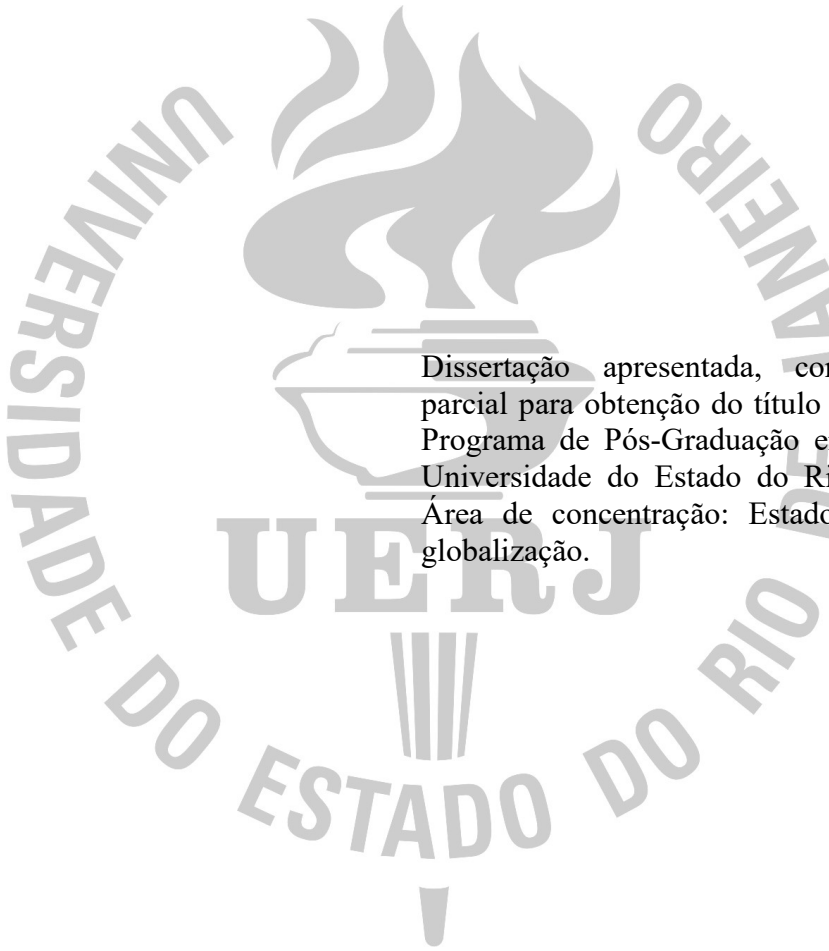
Kellen Dobler

Cooperação internacional em matéria penal e o crime cibernético no Brasil

Rio de Janeiro
2023

Kellen Dobler

Cooperação Internacional em matéria Penal e o Crime Cibernético no Brasil



Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao Programa de Pós-Graduação em Direito, da Universidade do Estado do Rio de Janeiro. Área de concentração: Estado cidadania e globalização.

Orientador: Prof. Dr. Carlos Eduardo Adriano Japiassú

Rio de Janeiro

2023

CATALOGAÇÃO NA FONTE
UERJ/REDE SIRIUS/BIBLIOTECA CCS/C

D633c Dobler, Kellen

Cooperação internacional em matéria penal e o crime cibernético no Brasil / Kellen Dobler. - 2023.
159f.

Orientador: Prof. Dr. Carlos Eduardo Adriano Japiassú.

Dissertação (Mestrado). Universidade do Estado do Rio de Janeiro, Faculdade de Direito.

1. Direito penal - Teses. 2. Cooperação internacional- Teses. 3. Crime cibernético - Teses. I. Japiassú, Carlos Eduardo Adriano. II. Universidade do Estado do Rio de Janeiro. Faculdade de Direito. III. Título.

343.45

Bibliotecária: Ana Clara Brandão CRB7/6346

Assinatura

Data

KELLEN DOBLER

Cooperação internacional em matéria penal e o crime cibernético no Brasil

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao Programa de Pós-Graduação em Direito, da Universidade do Estado do Rio de Janeiro. Área de concentração: Estado cidadania e globalização.

Aprovada em 06 de outubro de 2023.

Banca Examinadora:

Prof. Dr. Carlos Eduardo Adriano Japiassú (Orientador)
Faculdade de Direito − UERJ

Prof. Dra. Ana Lúcia Tavares Ferreira
Faculdade de Direito – Estácio de Sá

Prof. Dr. José Danilo Tavares Lobato
Faculdade de Direito − UERJ

Rosalina Alves Nante
Universidade Federal de Rondônia

Rio de Janeiro

2023

DEDICATÓRIA

A Stenio Castiel (*in memoriam*), meu eterno orientador que permanecerá imortal em minha trajetória acadêmica, dedico minha mais profunda gratidão pelo estímulo erudito que me proporcionou durante os anos de graduação. Em seu nome, presto minha homenagem a todas as vítimas da COVID-19 que partiram sem a chance de se vacinar.

Para os opressores, o que vale é ter mais e cada vez mais, à custa, inclusive, do ter menos ou do nada ter dos oprimidos. Ser, para eles, é ter e ter como classe que tem.

Paulo Freire.

AGRADECIMENTOS

Devo agradecer, em primeiro lugar, a Deus por me fortalecer na fé revelando que é nas adversidades que germina a resiliência. A todos da minha família, pelo apoio, incentivo e respeito ao meu trabalho. Em especial, gostaria de dedicar um agradecimento à minha mãe, por todo o amor e luta que compartilhamos ao longo da vida, por ser minha força e fonte de inspiração.

Agradeço imensamente a todos os professores do PPGD-UERJ, que, com determinação, dedicação e amor pelo ensino, adaptaram suas metodologias às aulas online impostas pela pandemia da COVID-19.

À minha orientadora, a professora Ana Lúcia Tavares Ferreira, cujas extensas e enriquecedoras reuniões virtuais, motivadas pela distância geográfica, foram fonte inesgotável de inspiração, energia e imprescindíveis contribuições para o meu desenvolvimento acadêmico.

Meus agradecimentos a EMERON, que generosamente abriu as portas e viabilizou a oportunidade dessa integração de conhecimento entre o Tribunal de Justiça do Estado de Rondônia e a PPGD-UERJ. Em especial aos servidores Eduardo Ribeiro Santos e Rosalina Alves Nantes pela dedicação, competência e principalmente paciência no acompanhamento ao longo desses dois anos de jornada.

Por fim e não menos importante gostaria de expressar minha sincera gratidão aos colegas de trabalho que testemunharam meu cansaço, estresse e momentos de desmotivação ao longo desta jornada de pesquisa. Em especial, gostaria de agradecer ao meu chefe, Edeonilson Souza Moraes, que sempre compreendeu minhas ausências e exaustão, e diante dos vários episódios de desmotivação, foi um constante incentivador para que eu não desistisse. A empatia e apoio de vocês foram fundamentais para minha perseverança.

RESUMO

DOBLER, Kellen. *Cooperação internacional em matéria penal e o crime cibernético no Brasil*. 2023. 159 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2023.

Os avanços tecnológicos provocaram revoluções em diversos setores da sociedade em especial nas atividades humanas, reconfigurando o mundo numa sociedade hiperconectada denominada a era da informação. Nesse contexto, surgem novos cenários e condutas apresentando novos desafios ao Direito Penal. Com o surgimento do ciberespaço modificou-se a interpretação e definição das fronteiras geográficas, levantando questionamentos sobre a eficácia dos instrumentos jurídicos diante da crescente criminalidade no ambiente digital. Esse panorama propicia uma revisão de conceitos fundamentais, especialmente no que concerne à jurisdição, à aplicação da lei e à determinação do local do crime. O caráter transnacional da criminalidade cibernética demanda uma reinterpretação do conceito de soberania. Nesse sentido o objetivo deste estudo é investigar os desafios político-criminais enfrentados pelo ordenamento jurídico brasileiro diante do cenário dos crimes cibernéticos, além de avaliar a importância da cooperação internacional em matéria penal na perspectiva da adesão do Brasil à Convenção de Budapeste. Assim, a pesquisa pretende demonstrar a relevância da cooperação em matéria penal para uma eficaz persecução penal nos crimes cibernéticos, bem como o impacto da adesão do Brasil à Convenção de Budapeste – um tratado internacional específico sobre criminalidade cibernética – e as consequências jurídicas e práticas dessa inserção no ordenamento jurídico brasileiro. Com uma abordagem dedutiva e utilizando pesquisa bibliográfica documental, o estudo estrutura-se em quatro partes: a primeira discorre sobre o surgimento da sociedade da informação e as categorizações do crime cibernético; a segunda examina a trajetória legislativa brasileira diante dos crimes digitais; a terceira enfatiza a importância da cooperação penal internacional e a posição do Brasil nesse cenário; o quarto e último segmento foca nos impactos da adesão brasileira à Convenção de Budapeste, refletindo sobre os possíveis desafios legislativos decorrentes desse compromisso.

Palavras-chave: Convenção de Budapeste; cooperação penal internacional; crime cibernético.

ABSTRACT

DOBLER, Kellen. *Cooperação internacional em matéria penal e o crime cibernético no Brasil*. 2023. 159 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2023.

Technological advancements have sparked revolutions in various sectors of society, especially in human activities, reshaping the world into a hyper-connected society known as the information age. Within this context, new scenarios and behaviors arise, presenting fresh challenges to Criminal Law. With the emergence of cyberspace, the interpretation and definition of geographical boundaries have changed, raising questions about the effectiveness of legal instruments in the face of increasing criminality in the digital environment. This landscape prompts a review of fundamental concepts, especially concerning jurisdiction, the application of the law, and the determination of the crime's location. The transnational nature of cybercrime calls for a reinterpretation of the concept of sovereignty. In this regard, the aim of this study is to investigate the political-criminal challenges faced by the Brazilian legal system in the face of cybercrimes, as well as to evaluate the importance of international cooperation in penal matters from the perspective of Brazil's accession to the Budapest Convention. Thus, the research intends to demonstrate the significance of cooperation in penal matters for effective prosecution in cybercrimes, as well as the impact of Brazil's accession to the Budapest Convention – a specific international treaty on cybercrime – and the legal and practical consequences of this integration into the Brazilian legal framework. Adopting a deductive approach and using documentary bibliographical research, the study is structured in four parts: the first discusses the emergence of the information society and the categorizations of cybercrime; the second examines the Brazilian legislative trajectory in the face of digital crimes; the third emphasizes the importance of international penal cooperation and Brazil's position in this setting; the fourth and final segment focuses on the impacts of Brazil's adherence to the Budapest Convention, reflecting on the possible legislative challenges arising from this commitment.

Keywords: Budapest convention; international penal cooperation; cybercrime;.

LISTA DE TABELAS

SUMÁRIO

INTRODUÇÃO

A evolução da tecnologia ultrapassou fronteiras geográficas até então desconhecidas pela humanidade, transformando, assim, a dinâmica da sociedade contemporânea. O surgimento da internet impactou tanto a esfera profissional quanto a pessoal, resultando em uma dependência contínua e global desta tecnologia.

Essas transformações estão intrinsecamente ligadas ao percurso histórico, impulsionadas pelos avanços tecnológicos e científicos, nomeadamente pelo surgimento da internet, que teve sua origem e expansão no cenário de pós-segunda guerra mundial. Este progresso tecnológico desencadeou revoluções em diversas esferas da atividade humana, culminando na criação de uma sociedade intensamente interligada, conhecida como era da informação.

Com o surgimento e a popularização da internet, surge também um novo espaço de interação social: o chamado ciberespaço. Estes novos elementos, impulsionados pela era digital, trazem benefícios significativos para a sociedade, mas também podem ser utilizados de forma prejudicial e até mesmo para a prática de crimes. Os crimes cibernéticos, como são conhecidos os crimes praticados no ambiente virtual, representam um importante desafio para o Direito Penal contemporâneo.

No ciberespaço, as definições tradicionais de fronteiras foram reconfiguradas, suscitando questionamentos sobre a aplicabilidade dos instrumentos legais diante da criminalidade cibernética. Esse cenário instigou a necessidade de repensar conceitos jurídicos fundamentais, particularmente no que diz respeito à jurisdição, aplicação da lei e conceitos temporais e espaciais relacionados aos crimes cibernéticos. O caráter transnacional desses delitos tem demandado uma reinterpretação do conceito de soberania.

É nesse contexto que a presente pesquisa desenvolve sua proposta, examinando os crimes cibernéticos no cenário da cooperação internacional. A ideia surgiu da constatação de que os indivíduos são agora muito mais vulneráveis a atividades criminosas do que em épocas anteriores. Isso ocorre porque o advento da internet aproximou pessoas de diferentes localidades, aumentando as oportunidades de atuação dos criminosos. Naturalmente, o contexto global atual não é composto apenas pela internet, mas também abrange avanços nas técnicas de comunicação que geraram esta paisagem global intensamente conectada.

Diante disso, surge o problema central desta pesquisa: investigar os desafios político-criminais enfrentados pelo ordenamento jurídico brasileiro diante do cenário dos crimes cibernéticos e avaliar a importância da cooperação internacional em matéria penal na

perspectiva da adesão do Brasil à convenção de Budapeste. O tema é de extrema relevância, uma vez que a propagação da internet pelo mundo tem trazido tanto benefícios quanto efeitos negativos, sendo a criminalidade cibernética um dos maiores desafios das sociedades da era digital.

Para o enfrentamento do problema proposto, a presente pesquisa emprega uma pesquisa teórica realizada pela abordagem dedutiva. O método utilizado é bibliográfico, baseado no conteúdo de artigos e livros já publicados sobre os assuntos relativos a este tema, bem como dos textos legislativos e documentos internacionais.

A pesquisa é estruturada em quatro capítulos. O primeiro trata sobre a sociedade da informação, surgimento da internet e dos crimes cibernéticos. Dada a natureza contemporânea do tema em questão, torna-se crucial entender a partir de que momento a sociedade teve acesso a tecnologias tão sofisticadas. Dessa forma, o capítulo inicial aborda o surgimento e da sociedade em rede e a internet, introduzindo conceitos essenciais para a melhor compreensão do tema.

O segundo capítulo abordará a evolução legislativa brasileira frente aos crimes cibernéticos. Será realizada uma análise das iniciativas legislativas que surgiram no Brasil para lidar com os crimes cibernéticos, considerando tanto os aspectos históricos quanto os debates jurídicos que permearam essa evolução. Será discutida a necessidade de uma resposta legislativa eficiente e atualizada diante dos desafios apresentados pela criminalidade digital e a importância de uma política jurídica mais célere, capaz de acompanhar o ritmo acelerado das transformações tecnológicas.

No capítulo três, será abordada a importância da cooperação em matéria penal no cenário internacional e seus reflexos frente a essa nova modalidade de criminalidade. Será realizada uma análise aprofundada sobre a importância da cooperação entre os países no combate aos crimes cibernéticos. Serão explorados os mecanismos existentes para promover a colaboração internacional na investigação e repressão desses delitos, levando em consideração as peculiaridades e desafios apresentados por essa forma de criminalidade.

Serão discutidos os instrumentos jurídicos e as iniciativas internacionais que visam fortalecer a cooperação penal no âmbito global, bem como os impactos dessas ações na prevenção e repressão dos crimes cibernéticos. Será destacada a importância da troca de informações, da harmonização de leis e da atuação conjunta dos países para enfrentar efetivamente essa ameaça transnacional.

O último capítulo abordará a convenção de Budapeste sobre cibercrime e os aspectos inerentes à Cooperação Penal Internacional. Merece atenção especial o processo de sua

construção, a partir das discussões iniciais sobre o tema no âmbito do Conselho da Europa, e sua consolidação como o principal documento internacional sobre criminalidade virtual. Além disso, o capítulo analisará as implicações da recente adesão do Brasil à convenção, examinando os potenciais desafios e oportunidades no alinhamento de sua legislação penal interna com os padrões internacionais delineados na convenção. Esta avaliação lançará luz sobre o impacto da adesão do Brasil no cenário internacional sobre crimes cibernéticos e suas implicações para a harmonização no ordenamento jurídico interno.

Ao fim, a presente pesquisa almeja contribuir para o desenvolvimento de um arcabouço teórico que ofereça fundamentação para orientar a implementação de uma política criminal mais adequada aos crimes cibernéticos, em consonância com o cenário de cooperação penal internacional. Considera-se a importância da colaboração entre os países como uma das ferramentas essenciais para enfrentar essa nova forma de criminalidade.

Ao estabelecer essa discussão, espera-se que esta pesquisa possa contribuir para a formulação de políticas criminais mais eficazes e harmonizadas internacionalmente, capazes de lidar de forma adequada diante dos desafios apresentados pelos crimes cibernéticos para o Direito Penal. A compreensão aprofundada dessas questões é essencial para promover uma maior segurança cibernética e proteger os indivíduos e organizações contra ameaças virtuais cada vez mais sofisticadas.

1 SOCIEDADE DA INFORMAÇÃO E OS CRIMES CIBERNÉTICOS

1.1 Sociedade da informação

Desde o final do século XX, a humanidade experimenta o impacto da chamada revolução da tecnologia da informação, que se caracteriza principalmente pelo crescente poder e importância da transmissão e controle da informação.

De acordo com Castells, grandes avanços têm sido alcançados em torno dessa crescente transferência da informação desde as últimas décadas, e descreve como um evento histórico de grande importância, equivalente à Revolução Industrial do século XVIII, transformando as bases materiais da economia, sociedade e cultura.

Nas palavras de Castells, esse início foi marcado principalmente pela evolução tecnológica, caracterizada não apenas pela centralização do conhecimento e da informação, mas também pela aplicação destes para gerar novos conhecimentos de comunicação e informação. Pela primeira vez na história, a capacidade mental humana assumiu um papel direto na produção, indo além de ser um mero componente do sistema produtivo[1].

A partir da chegada dessas novas tecnologias de processamento, armazenamento e transmissão de dados, foi possível observar uma mudança profunda na sociedade contemporânea. A quase ilimitada troca e difusão dessas informações, independentemente de distâncias geográficas ou fronteiras nacionais, afetou vários aspectos da sociedade, em especial o ordenamento jurídico.

Dessa forma, a internet, a informação e as tecnologias desempenham um papel essencial dessa nova realidade social, influenciando diretamente o cenário jurídico e proporcionando uma nova perspectiva dos direitos fundamentais consagrados na no artigo 5º da Constituição Federal, tais como: liberdade de expressão, vedação ao anonimato, liberdade de atividade intelectual, artística, científica e comunicativa, e principalmente o acesso à informação[2].

É relevante destacar que o contexto social atual não se limita apenas à utilização cotidiana da internet para a troca de informações. As transformações decorrentes da sociedade

[1] CASTELLS, M. A Galáxia da internet: reflexões sobre à internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar, 2003, pg. 69.

[2] BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidente da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 14 ago. 2023.

da informação reconfiguraram não somente conceitos na sociedade, mas também no ordenamento jurídico, impactando as esferas sociais, econômicas e culturais[3].

Por outro lado, como contrapartida ao desenvolvimento da internet e dos dispositivos tecnológicos, os quais passam a desempenhar um papel central nas relações sociais pacíficas, também possibilitaram práticas socialmente indesejadas e prejudiciais, inclusive ameaçando bens que antes não eram considerados relevantes para o ordenamento jurídico[4].

Nas Palavras de Crespo, o progresso tecnológico trouxe consigo a observação das condutas delitivas que começam a ocorrer por meio de dispositivos tecnológicos. Essas formas de influenciar e controlar ações futuras dos seres humanos possuem um impacto direto ou indireto na prática das atividades criminosas[5].

Nesse sentido, o cenário de revolução tecnológica e social deram espaço para o surgimento dos chamados crimes cibernéticos, objeto dessa pesquisa, como um dos efeitos decorrentes dessa era da informação. A utilização inadequada da tecnologia cotidiana gerou uma série de ameaças, incluindo a delinquência informática como um fenômeno social[6].

Nas palavras de Fiorillo, o ordenamento jurídico necessita estar sempre se adaptando as mudanças, sob o risco de perder sua função primordial, que é regular as interações sociais e estabelecer padrões de comportamento[7].

Portanto, a relação entre direito e a informação não é apenas um fenômeno temporário, esta é uma realidade ainda em grande parte não explorada, mas que requer análise em todos os âmbitos das disciplinas jurídicas, visando assegurar o estabelecimento de novos direitos fundamentais, além de garantir a eficácia daqueles já existentes[8].

Nesse contexto, o presente capítulo dessa pesquisa explorará a interseção entre a sociedade da informação e o surgimento dos crimes cibernéticos. Pretende-se compreender as origens, os padrões, os impactos e as medidas de combate a esse fenômeno bastante complexo e em constante evolução.

---

[3] FIORILLO, Celso Antônio Pacheco. Princípios constitucionais do direito da sociedade da informação: a tutela jurídica do meio ambiente digital, pg 152. *Ebook Kindle.*

[4] FIORILLO. Op. Cit, pg152.

[5] CRESPO,Op. Cit. Pg. 37.

[6] FIORILLO, Celso Antônio Pacheco. Op. Cit, pg. 152.

[7] *Ibidem''.*

[8] *Ibidem.*

1.1.1 Definição e características da sociedade da informação

A sociedade da informação pode ser compreendida como uma configuração sociocultural em que a informação e o conhecimento desempenham papéis centrais na organização da economia, da política, das relações sociais e da cultura[9].

Nesse sentido a sociedade é caracterizada por uma série de elementos distintivos. Primeiramente, a ubiquidade da informação e a capacidade de compartilhá-la instantaneamente permitindo uma nova forma de participação e colaboração em larga escala. Depois a conectividade global, que proporcionada pela Internet transcende fronteiras físicas e temporais, permitindo que indivíduos e grupos se engajem em atividades sociais, políticas e econômicas de maneira descentralizadas[10].

Além disso, a economia da sociedade da informação é impulsionada pela produção, distribuição e uso de informações e conhecimentos. A criação de valor está cada vez mais relacionada à capacidade de processar, analisar e aplicar informações de maneira inovadora. A tecnologia da informação e a automação transformaram a forma como as atividades produtivas são realizadas, abrindo caminho para setores emergentes e novos modelos de negócios baseados na economia digital[11].

No entanto, essa sociedade caracterizada pelo valor atribuído à informação também apresenta desafios significativos. Como já mencionado, a dependência de sistemas digitais e a ampliação do acesso à informação suscitam questões relacionadas à privacidade, segurança cibernética, criminalidade virtual e desigualdade no acesso ao conhecimento. Além disso, a velocidade das mudanças tecnológicas frequentemente ultrapassa a capacidade das instituições sociais e políticas de se adaptarem, resultando em um desequilíbrio entre os avanços tecnológicos e as estruturas regulatórias.

1.1.2 A Sociedade em rede

A teoria da sociedade em rede, proposta por Castells, é entendida como uma das mais significativas transformações sociais e culturais impulsionadas pelas tecnologias da informação e comunicação. Essa teoria postula que a estruturação da sociedade contemporânea é moldada,

---

9 CASTELLS, Manuel**.** A era da informação: economia, sociedade e cultura. Vol. 2 – A sociedade em Rede. Paz e Terra. 1999. Pg. 61.

[10] CASTELLS, Manuel**.** A era da informação: economia, sociedade e cultura. Op. Cit., p 61.

[11] *Ibidem*

em grande parte, pela interconexão global proporcionada pelas redes de comunicação. Castells argumenta que a sociedade em rede é caracterizada pela ascendência da informação como elemento central de organização e poder[12].

A terminologia sociedade em rede criada por Castells, expressa uma sociedade que está conectada como nós que formam redes. Essas redes promovem interações até então nunca vistas, que se caracterizam pela ausência de fronteiras, pela interconexão de valores e interesses comuns e pela mudança da compressão do espaço-tempo[13].

Nesse sentido, a interconexão global em tempo real possibilitada pela internet e outras tecnologias está redefinindo as dinâmicas sociais, econômicas e políticas, influenciando a forma como as pessoas se relacionam, trabalham, se informam e participam da vida em sociedade. Essa teoria proporciona um arcabouço analítico fundamental para compreender as complexas interações entre tecnologia, cultura e sociedade na era contemporânea[14].

Conforme apontado por Castells, observa-se uma forte transformação nas relações interpessoais na sociedade em rede. Embora seja evidente o declínio da interação face a face e o aumento do isolamento decorrente do avanço tecnológico, é importante ressaltar que tais mudanças não necessariamente prejudicaram as relações de amizade e do engajamento social[15].

Nesse cenário defendido por Castells, a sociedade em rede é uma sociedade hipersocial, não uma sociedade de isolamento. Para o autor, as pessoas não disfarçam sua identidade na internet, isso porque as tecnologias foram integradas à vida das pessoas, de modo a ligar a realidade virtual à virtualidade real, levando os indivíduos a vivenciarem diferentes formas tecnológicas de comunicação e articulá-las conforme suas necessidades[16].

Nessa perspectiva, as redes digitais desempenham um papel central na organização e na dinâmica social, permitindo a formação de novas configurações interpessoais, novas identidades e a reconfiguração dos espaços de poder. A teoria da sociedade em rede de Castells oferece uma visão crítica e complexa das interações entre tecnologia, economia, cultura e

[12] CASTELLS, Manuel**.** A era da informação: economia, sociedade e cultura. Op. Cit., p 61.

[13] CASTELLS, Manuel. A sociedade em rede. 23. ed. Rio de Janeiro: Paz e Terra, 2021. 629 p.22.

[14] *Ibidem*

[15] *Ibidem*

[16] *Ibidem*

política, destacando a importância de compreendermos as dinâmicas sociais em um contexto global e digitalmente conectado[17].

Do ponto de vista de Castells, a sociedade em rede é um fenômeno positivo que amplia as possibilidades de comunicação e interação social por meio da tecnologia. No entanto, essa visão otimista e romantizada da sociedade em rede contrasta com a realidade do século XXI, marcada por altos índices de doenças mentais relacionadas ao excesso de informação e de estímulos virtuais[18].

O que se tem observado é que essa sociedade hiperconectada que produz e consome uma enorme quantidade de informação por meio das redes, tem gerado impactos preocupantes na saúde mental do indivíduo. Estudos apontam que os usuários têm desenvolvido transtornos como depressão, transtorno de déficit de atenção, transtorno de personalidade limítrofe, síndrome de burnout entre outras. Essas patologias estão diretamente associadas à dificuldade de lidar com a diversidade de opções e o excesso de informação que as redes propiciam, bem como à indistinção entre o real e o virtual[19].

É fundamental encontrar um equilíbrio entre a atual era da informação e seus efeitos sobre a vida social, física e psicológica da sociedade. Simplesmente avançar na criação de novas ferramentas de interação e tecnologia não é suficiente; é crucial considerar os possíveis impactos que essas inovações possam ter no dia a dia das pessoas e em suas perspectivas futuras de bem-estar mental.

1.2 Ciberespaço e a internet: origem, evolução e características

1.2.1 Surgimento da Internet

A internet é considerada a maior invenção tecnológica dos últimos tempos, em virtude do seu poder de alcance, da mudança da compressão espaço-tempo, das informações instantânea e principalmente na sua capacidade de conectar pessoas do mundo todo independente da localidade[20].

Para Castells, essa possibilidade de comunicação simultânea com múltiplas pessoas em qualquer local do planeta, a qualquer momento, resultou na criação de um novo conceito de

[17] CASTELLS, Manuel. A sociedade em rede. Op. Cit pg. 21

[18] HAN, B.-C. Sociedade do cansaço. 2. ed. Petrópolis: Vozes, 2017. Disponível em: https://edisciplinas.usp.br/pluginfile.php/5000148/mod_resource/content/1/Sociedade%20do%20cansa%C3%A7o.pdf. Acesso em: 14 ago. 2023.

[19] HAN, B.-C. Sociedade do cansaço. Op. Cit.

[20] CASTELLS, M. A galáxia da Internet: reflexões sobre a internet, os negócios e a sociedade, pg 100.

mundo, o que chamou de ‘a galáxia da internet”[21]. Essa expressão busca ilustrar o tamanho da abrangência que a internet, enquanto sistema de informação consegue alcançar num curto espaço de tempo e em diferentes localidades ao mesmo tempo.

Em termos técnicos, a internet representa uma extensa malha de conexão que viabiliza a interligação de computadores em escala global, propiciando a troca de informações entre eles. Seu surgimento remonta à década de 1960, precisamente em 1966, quando diversas instituições acadêmicas uniram esforços para conceber a *ARPANET* (Administração de Projetos e Pesquisas Avançados), uma iniciativa originalmente voltada para as Forças Armadas dos Estados Unidos, no contexto da guerra fria[22].

Durante a década de 70, a *ARPANET* passou por aprimoramentos com a colaboração de cientistas e foi inicialmente disponibilizada para universidades. No entanto, em 1983, preocupado com possíveis vulnerabilidades de segurança, o departamento de defesa dos Estados Unidos optou por dividir os objetivos da rede, originando a *MILNET*, que possuía propósito similar. Enquanto esta última era designada para uso militar, a *ARPANET* continuou a ser utilizada no ambiente acadêmico, evoluindo para *ARPAnet-Internet*. Subsequentes fases contemplaram a criação e adoção do protocolo de controle de transmissão *TCP/IP*. Após a abertura da rede para o público em geral, sua administração foi privatizada. Desde então, empresas provedoras de acesso emergiram e direcionaram investimentos para sua comercialização, estabelecendo suas próprias vias de acesso à rede e ampliando ainda mais seu alcance para diferentes partes do globo[23].

A popularização da internet teve início na década de 1990, com a introdução do sistema de hipertexto *WWW (World Wide Web)*, desenvolvido pelo programador inglês Tim *Burners-Lee*[24]. Desde então, essa rede tem experimentado um crescimento exponencial, impulsionado pelo desenvolvimento de softwares acessíveis e de fácil utilização. Atualmente, a Internet se estende globalmente, conectando bilhões de usuários em todo o mundo. De acordo com dados

---

21 CASTELLS, M. A galáxia da Internet: reflexões sobre a internet, os negócios e a sociedade, pg 100. Op. Cit.

22 CRESPO. Op. Cit, pg. 32.

23 CONTE, Christiany Pegorari; FIORILLO, Celso Antônio Pacheco. Crimes No Meio Ambiente Digital. 2. ed. São Paulo: Saraiva, 2016, pg. 23

24 CONTE. Op. Cit. pg. 23.

de janeiro de 2023, estima-se que o número de usuários ativos tenha alcançado a impressionante marca de 5,16 bilhões[25].

Esse aumento significativo no número de usuários destaca a dimensão que a internet é para o mundo hoje, sendo uma ferramenta essencial para a comunicação, o acesso à informação e a interconexão global. Seu uso se tornou um elemento fundamental na vida cotidiana das pessoas, transformando a maneira como nos comunicamos, trabalhamos, aprendemos e interagimos com o mundo ao nosso redor.

Esse protagonismo da internet na vida das pessoas está intrinsecamente ligado à sua capacidade de permitir a interconexão entre indivíduos, organizações e instituições em diferentes partes do mundo, transcendendo as barreiras geográficas, possibilitando a formação de redes de comunicação descentralizadas e flexíveis. Essa interconexão virtual não apenas agiliza a disseminação de informações, mas também facilita a colaboração, a troca de conhecimento e a mobilização social em escala global[26].

Nas palavras de Castells a internet seria como um espaço de interação onde a produção e o compartilhamento de conteúdo estão ao alcance de uma ampla gama de indivíduos. Isso permite a emergência de novas formas de participação e engajamento cívico, possibilitando que vozes anteriormente marginalizadas tenham a oportunidade de se expressar e influenciar as dinâmicas sociais e políticas[27].

Observa-se que a internet desempenha um papel essencial na construção da sociedade em rede, atuando como um canal de comunicação que conecta indivíduos e instituições em escala global, sendo um catalisador de mudanças sociais, econômicas e culturais, promovendo a descentralização do poder da informação, a colaboração em rede e a ampliação das possibilidades de participação e engajamento entre as pessoas[28].

Em suma, a internet se tornou um elemento fundamental na vida cotidiana das pessoas, transformando a maneira como nos comunicamos, trabalhamos, aprendemos e interagimos com o mundo ao nosso redor. Sua interligação global, e seus sistemas e dispositivos eletrônicos

---

[25] VERVIEW, Global. Essential Digital Headlines: overview of the adoption and use of connected devices and services. Overview Of the Adoption and Use of Connected Devices And Services. 2023. Disponível em: https://www.amper.ag/post/we-are-social-e-hootsuite-digital-2023-visao-geral-global-resumo-e-relatorio-completo. Acesso em: 15 ago. 2023

[26] CASTELLS, M. A galáxia da Internet: reflexões sobre a internet, os negócios e a sociedade, pg 100.

[27] CASTELLS, Manuel. A sociedade em rede. Op. Cit, pg, 38-39

[28] *Ibidem*

instauraram um novo contexto de interação e comunicação, reconfigurando as fronteiras convencionais e apresentando desafios inéditos no âmbito jurídico.

1.2.2 Ciberespaço e as novas fronteiras jurídicas

O ciberespaço pode ser compreendido como uma nova forma de sociedade, na qual surgem novas modalidades de relações sociais. Ao migrarmos do mundo real para o ambiente virtual, percebemos que o território não é demarcado e não possui fronteiras físicas. Em vez disso, o ciberespaço é apropriado por meio de subjetividades que simulam uma projeção do mundo real. Ao executarmos uma tarefa diante do computador, experimentamos a sensação de estar em um local específico e presente, mesmo que seja apenas uma representação virtual.

A abordagem de Castells em relação à percepção de tempo e espaço representa uma perspectiva marcante na análise das transformações socioculturais na era da informação. Para o autor, o advento das tecnologias de comunicação e informação provocaram uma redefinição fundamental na maneira pelas quais os indivíduos compreendem e vivem o tempo e o espaço[29].

Nesse sentido a interconexão global, facilitada pela internet, resultou na formação de um espaço de fluxos, no qual a distância física já não é o principal determinante da interação, surgindo um novo conceito de território[30].

Nesse sentido, o termo ciberespaço surgiu como um novo domínio de interação social, mesmo que à distância, de forma a exercer influências significativas nas esferas cultural e social. Sendo esse ambiente um espaço virtual moldado por redes informacionais, permitindo essa interconexão social entre indivíduos[31].

Diversas nomenclaturas são utilizadas para definir esse novo território virtual, porém o termo ciberespaço, criado por William Gibson[32], é o mais adotado para invocar esse ambiente de comunicação, embora o próprio autor tenha esclarecido que a palavra não foi originalmente criada com essa intenção. Na realidade a expressão *cyberspace* refere-se a sua obra de ficção cientifica Neuromancer, publicada em 1984[33].

---

[29] CASTELLS, Manuel. A sociedade em rede. Op. Cit, pg, 38-39.

[30] *Ibidem*

[31] CASTELLS, Manuel. A sociedade em rede. Op. Cit, pg, 38-39

[32] GIBSON, Willian. Neuromancer. São Paulo: Aleph, 2003, pg 381. *Ebook Kindle.*

[33] GIBSON. *Op. Cit.*

Já nas palavras de Rohrmann o termo surgiu com a revolução das telecomunicações, sendo equiparado aos conceitos de mundo online ou mundo virtual, sendo mais usualmente definido como ciberespaço pois representa o ambiente que interconecta dispositivos eletrônicos, possibilitando que indivíduos realizem uma multiplicidade de ações, muitas das quais com implicações jurídicas[34].

Nesse contexto de ciberespaço, Theophilo expande a compreensão ao relacioná-la com o novo paradigma da sociedade global. Ele a descreve como uma disciplina emergida do estudo comparativo entre máquinas eletrônicas automáticas e os processadores do sistema nervoso em seres vivos, abrangendo suas conexões nervosas. A simulação desse comportamento por computadores resultou na prática da concepção da cibernética[35].

Nesse sentido com o progresso tecnológico, o termo foi estendido às máquinas capazes de realizar movimentos distintos baseados em condições internas variáveis. Com o advento da eletrônica e sua evolução marcante, surgiu a possibilidade de aplicar as condições elétricas, magnéticas e ópticas, as quais formam as bases dos processadores digitais e da cibernética contemporânea[36].

Por sua vez, o ciberespaço na visão de Fragoso, se apresenta como o mais recente avanço de uma linhagem de tecnologias de comunicação com o objetivo central de proporcionar ao receptor a sensação de estar imediatamente presente no objeto representado. Essa inserção na linha dominante da evolução dos meios visuais de representação implica que, especialmente em sua fase inicial, os sistemas de realidade virtual continuem ligados a modalidades de representação espacial tidas como 'realistas' e 'transparentes' dentro do atual contexto cognitivo e cultural[37].

Pierre Lévy explora o Ciberespaço como um território nômade, uma genialidade informática e um cenário de pontes e calçadas líquidas do conhecimento, abarcando modos de percepção, sensação, memória, trabalho, entretenimento e convivência[38].

---

[34] ROHRMANN, Carlos Alberto. Curso de direito virtual. Belo Horizonte: Del Rey, 2005.

[35] THEOPHILO JÚNIOR, Roque. Cibernética Tecnologia e Psicologia. São Paulo, Academia Brasileira de Psicologia, 2000. Disponível em: <http://www.psicologia.org.br/internacional/ap11.htm>. Acesso em 1ago.2008.

[36] *Ibidem*

[37] FRAGOSO, Suely. Realidade Virtual e Hipermídia - somar ou subtrair? São Leopoldo: Cyberlegenda nº9, 2002. Disponível em:<http://www.uff.br/mestcii/sueli1.htm>. Acesso em: 1 set.2023.

[38] LÉVY, Pierre. Cibercultura. São Paulo: Editora 34, 2010. Pg15.

A definição mais clássica de ciberespaço seria a de uma fronteira eletrônica, uma terra da era da informação e um domínio onde o futuro deve residir. Embora existam algumas críticas quanto ao termo, devido a crescente popularização da Internet o que resultou na sobreposição do mundo virtual com o real, ao invés de criar um espaço separado[39].

Para Leonardi, há uma certa inclinação para os termos espaço cibernético ou espaço virtual, fundamentando sua preferência na ausência da palavra ciberespaço em vários dicionários, e consideram seu uso um barbarismo linguístico. No entanto, é importante destacar que ciberespaço é reconhecido e definido nos principais léxicos. Ele é caracterizado como uma dimensão ou domínio virtual da realidade, composto por entidades e ações estritamente informacionais. Este conceito serve como um análogo ao espaço físico, proporcionando um ambiente onde humanos, máquinas e programas computacionais coexistem e interagem, encapsulando, em essência, o ecossistema da internet[40].

Nesse contexto seja como um domínio apartado da realidade material ou interligado a ela, o ciberespaço se caracteriza por ser um elemento crucial para o funcionamento da sociedade em rede. Essa união entre informação, comunicação e tecnologia não se limita a isolar segmentos da população, mas sim a integrar diversos grupos de diferentes locais e com distintos propósitos.

Dessa forma, a sociedade da informação moldada pelo ciberespaço, trouxe à tona a necessidade de delinear fronteiras jurídicas coerentes com essa nova realidade. A complexidade das relações e a velocidade das mudanças tecnológicas exigem uma revisão profunda das abordagens tradicionais do Direito. Fiorillo aponta para a urgência de desenvolver mecanismos legais capazes de lidar com crimes e infrações ocorrendo em um ambiente intangível, muitas vezes ultrapassando limites territoriais[41].

As reflexões trazidas Fiorillo oferecem uma análise aprofundada das implicações jurídicas resultantes da intersecção entre tecnologia e sociedade. Questões como a proteção de dados pessoais, os desafios na persecução penal dos crimes cibernéticos e a adaptação do ordenamento jurídico às dinâmicas mutáveis do ciberespaço. As referências e análises de

---

[39] LEONARDI, Marcel. Fundamentos de Direito Digital. Revista dos Tribunais. São Paulo. *Ebook Kindle*.2019. Pg 21.

[40] LEONARDI, Marcel.Op. Cit. Pg 22.

[41] FIORILLO, Celso Antônio Pacheco. Princípios constitucionais do direito da sociedade da informação: a tutela jurídica do meio ambiente digital. Saraiva Educação SA, 2017. Pg.159. *Ebook Kindle.*

Fiorillo contribuem para a compreensão das lacunas e necessidades regulatórias desse ambiente em constante evolução[42].

Na análise da sociedade em rede delineada por Castells, o ciberespaço, acompanhado da cibercultura, traça um panorama tecnológico que se enraíza de maneira intrínseca na esfera humana, assumindo a forma de uma vasta teia de interconexões. Essa proposta não apenas lança luz sobre a construção e a desestabilização de novos contextos de interação social, como também identifica a emergência de uma era inédita, que propicia o desenvolvimento e a ampliação da sociedade em rede[43].

Observa-se, portanto, que a cibercultura é um conceito que descreve a interação complexa entre a tecnologia da informação e a sociedade contemporânea. Para Castells a cibercultura seria uma nova forma de cultura que emerge do ciberespaço. Ele destaca que a essa nova cultura é caracterizada pela fluidez, pela interatividade e pela capacidade de criar e compartilhar informações de forma instantânea e global. Além disso, enfatiza que a cibercultura não é apenas uma cultura virtual, mas também está enraizada na vida cotidiana das pessoas, influenciando suas identidades, relações sociais e práticas culturais[44].

Já na visão de Pierre Lévy, a determinação da cibercultura está intrinsicamente ligada à definição de ciberespaço. O ciberespaço, configura-se como o meio de comunicação originado da interconexão global dos sistemas computacionais. Similarmente a outros meios comunicativos, o ciberespaço não deve ser compreendido meramente como uma infraestrutura física ou um suporte tecnológico, mas sim como um conjunto de informações e de indivíduos que habitam esse espaço e contribuem com informações[45].

Nesse contexto, a cibercultura pode ser caracterizada como o conjunto de técnicas materiais e intelectuais, práticas, mentalidades, modos de pensamento e valores que emergem em conjunto com a expansão do ciberespaço[46].

Em suma, a interseção entre a sociedade em rede, o ciberespaço e o direito delineiam um cenário complexo e em constante evolução. A compreensão e a regulamentação adequada desses aspectos tornam-se essenciais para o estabelecimento de um ambiente digital seguro e

---

[42] FIORILLO. Pg.159, Op. Cit.

[43] ROHRMANN, Carlos Alberto. Op. Cit.

[44] CASTELLS, M. A galáxia da Internet: reflexões sobre a internet, os negócios e a sociedade, pg 100.

[45] LÉVY, Pierre. Cibercultura. Op. Cit, pg15.

[46] LÉVY, Pierre. Cibercultura. Op. Cit, pg15

equitativo. Nesse sentido, já se encontra em pauta a discussão acerca do surgimento de uma área jurídica intitulada direito do ciberespaço, a qual englobaria um conjunto de normas, regulamentações abrangentes e práticas contratuais de diversas naturezas, permeando as redes de software e computadores[47].

1.3 O Crime cibernético como fenômeno jurídico

1.3.1 Surgimento dos crimes cibernéticos

A chegada da tecnologia e das redes de comunicação trouxeram consigo não apenas novas perspectivas, mas também uma gama diversificada de novas atividades criminosas. Esse cenário digital proporcionou um ambiente propício para atividades ilícitas, uma vez que as estratégias para explorar vulnerabilidades e executar tais atos evoluíram paralelamente. Essa facilidade e acessibilidade da internet, combinada com nossa crescente dependência dela para atividades cotidianas, se tornou um atrativo para criminosos.

Entre os pesquisadores sobre o tema, não há consenso sobre quando e como teria sido a primeira prática criminosa no ambiente virtual. Para Jesus e Milagres, o primeiro grande evento envolvendo um crime informático teria ocorrido no âmbito *do Massachusetts Institut of Technology* (MIT), no ano de 1964, quando um estudante de apenas 18 anos teria perpetrado uma ação na internet caracterizada como *cybercrime*[48].

Outros registros ainda apontam para o ano de 1978, na Universidade de Oxford no Reino Unido, como o primeiro caso documentado de *hacking*, no qual um aluno teria acessado uma rede de computadores para obter a cópia de uma prova[49].

Entretanto, foi na década de 1980 e 1990 que os crimes cibernéticos tomaram uma dimensão maior, concomitantemente ao surgimento dos primeiros computadores pessoais. Foi a partir dessa época que os criminosos passaram a explorar as potencialidades da rede e a desenvolver técnicas voltadas à invasão de sistemas digitais[50].

---

[47] CERQUEIRA, Tarcisio Queiroz. O Direito do ciberespaço. Jus Navigandi, Teresina,1 nov.1999. Disponível em: ttps://edisciplinas.usp.br/pluginfile.php/114200/mod_resource/content/1/O%20Direito%20do%20ciberespa%C3%A7o%20-%20Revista%20Jus%20Navigandi%20-%20Doutrina%20e%20Pe%C3%A7as_Tarciso%20Cerqueira.pdf. Acesso em: 16 maio 2023

[48] JESUS, Damasio de. MILAGRE, José Antônio. Manual de Crimes Informatics. São Paulo: Saraiva, 2016, pg24 *Ebook Kindle*

[49] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg,23.

[50] SOUZA, Thiago. História da internet. Disponível em https://www.todamateria.com.br/historia-dainternet/. https://www.todamateria.com.br/historia-da-internet. Acesso em 14 abr. 2023

Vale ressaltar que nesse mesmo período houve o registro do primeiro crime cibernético com a característica de "*worm*"[51], praticada pelo estudante estadunidense Robert Tappan Morris. A intenção do programa idealizado por Morris consistia em avaliar a extensão da internet, todavia sua disseminação ocorreu em proporções mais rápidas e abrangentes do que imaginava, culminando na interrupção dos serviços em aproximadamente 6.000 computadores, totalizando 10% dos servidores de internet da época. Esse episódio, tido como o primeiro grande incidente de *cybercrime*, resultou na condenação de Morris com base na lei de fraude e abuso de computador dos Estados Unidos[52].

No Brasil, os primeiros acontecimentos envolvendo crimes cibernéticos remonta ao ano de 1997, com o surgimento dos chamados "*phishing scam* " (pescaria de senhas). Nessa ocasião, o indivíduo foi acusado de enviar um e-mail para o mercado financeiro, veiculando informações falsas que suscitavam o risco iminente de falência de uma instituição bancária[53]. Outros incidentes envolvendo crimes cibernéticos que se encontram registrados também datam a década de 1990. Um desses casos refere-se a uma jornalista, que passou a receber e-mails de teor erótico e sexual, acompanhados de ameaças à sua integridade física. No mesmo ano, a justiça de Belo Horizonte tomou medidas para remover da internet páginas contendo imagens explícitas de crianças envolvidas em atividades sexuais, destacando-se que o responsável por tais conteúdos contava com apenas 15 anos de idade[54].

No ano de 1998, um caso de destaque foi analisado pelo Supremo Tribunal Federal, por meio do julgamento do HC 76.689/PB, sob a relatoria do então ministro Sepúlveda Pertence. Nesse cenário jurídico, até então novo para o judiciário, tratava de uma situação envolvendo pornografia infantil em antigas *BBS (Bulleting Board Systen/Internet*)[55]. Naquela época, talvez

---

[51] Em computação, worm ou computer worm é um programa independente, do tipo malware, que se replica com o objetivo de se espalhar para outros computadores. Geralmente, usa uma rede de computadores para se espalhar, ou mesmo unidades USB, contando com falhas de segurança no computador de destino para acessá-lo

[52] WINDER, Davey. This 20-Year-Old Virus Infected 50 million Windows Computers In 10 Days: Why The ILOVEYOU Pandemic Matters In: 2020. FORBES, 2020.Disponívelem: 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=10aa7f8b3c7 c. Acesso em: 15 mai. 2023

[53] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit. Pg24.

[54] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit. Pg24.

[55] BBS é a abreviação de Bulletin Board System (em inglês, sistema de quadro de avisos), um sistema de comunicação via mensagens de texto. Funciona em microcomputadores conectados a uma rede paga ou gratuita por meio de uma linha telefônica e um modem. Disponível em: https://www.insper.edu.br/noticias/bbs-o-que-e-um-bulletin-board-system/

não fosse plenamente concebível que uma legislação específica fosse necessária para lidar com tais delitos. No entanto, o ministro proferiu um esclarecedor entendimento no sentido de que nem todos os crimes cibernéticos demandavam de uma tipificação específica, visto que, em muitos casos, a tecnologia representava apenas um novo meio empregado para a realização de delitos já conhecidos no ambiente físico[56].

De acordo com a decisão do ministro, o delito de publicação de cena de conteúdo sexual envolvendo menores, conforme estabelecido no Artigo 241º do Estatuto da Criança e do Adolescente[57], através da inclusão em redes de computadores como a internet, atribuída a menores de idade, demandava a verificação de sua tipicidade, nesse caso o tipo penal em questão, referente à disseminação de conteúdo explícito ou pornográfico, não era restritivo, diferentemente das disposições da lei de imprensa. Dessa forma, para a configuração da conduta criminosa, bastava que o meio utilizado para a divulgação da imagem possuísse a capacidade técnica de alcançar um número indeterminado de pessoas. Nesse contexto, a utilização de fotografias obscenas em redes de computadores preenchia os requisitos para a tipificação[58].

É importante observar que muito embora o judiciário, já nessa época, demostrava preocupação com o novo cenário de crimes no ambiente virtual, o entendimento proposto pelo ministro no caso analisado era inovador não apenas no preenchimento da lacuna legislativa por meio de analogia, a decisão trazia uma inovação jurídica, pois caso a conduta criminosa fosse adequadamente enquadrada no âmbito da legislação vigente, a tecnologia empregada para sua concretização poderia ser posterior à promulgação da lei penal.

Nesse sentido, desde a década de 1990, tem se observado uma real preocupação em como o sistema jurídico brasileiro deve caminhar e se adaptar às inovações experimentadas pela sociedade nesse novo ambiente de criminalidade, considerando que o ritmo de mudança legislativa é notoriamente mais lento em relação aos avanços tecnológicos e suas implicações[59].

Nas palavras de Milagres e Jesus, nesse contexto de inovações, os profissionais do direito não podem simplesmente cruzar os braços e aguardar por medidas legislativas que abordem as novas técnicas criminosas. Quando é viável enquadrar uma conduta antissocial em

---

[56] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg,27.

[57] Estatuto da Criança e do Adolescente: Lei federal nº 8069, de 13 de julho de 1990. Rio de Janeiro: Imprensa Oficial, 2002. BRASIL.

[58] BRASIL. Superior Tribunal de Justiça. Habeas-corpus nº 76689/PB, da 1ª Turma, Brasília, DF, 22 de setembro de 1998. Disponível em: ttps://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=76856.

[59] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 29

uma norma já em vigor, os aplicadores do direito não devem permanecer inertes diante da situação[60].

Sobre esse tema, a advogada Patrícia Peck[61], afirma que os crimes cibernéticos são um fenômeno crescente e inquietante na era do direito. Para a autora a relação do Brasil e a criminalidade digital se delineia por meio de uma abordagem abrangente, que abarca a revisão das legislações vigentes, a cooperação em âmbito internacional, o fomento à educação, à sensibilização da sociedade, a implementação de medidas de segurança da informação nas empresas e a responsabilização das entidades provedoras de serviços de internet[62].

Dessa forma, a internet, como uma rede global de informação, apresenta novos desafios para a sociedade e para ordenamento jurídico, sobretudo para o Direito Penal. Os crimes cibernéticos são cometidos em sua maioria um espaço indefinido, envolvendo ofensores e vítimas de diferentes países. Isso gera problemas para as autoridades, que muitas vezes não conseguem definir o local do crime, a jurisdição competente e as medidas de investigação e uma punição eficiente[63].

Nesse contexto, vale ressaltar que o arcabouço jurídico brasileiro já engloba algumas condutas de crimes cibernéticos, tais como a invasão de sistemas informáticos, adulteração de documentos eletrônico e outros diversos projetos de lei em andamento no congresso que tratam especificamente de crimes praticados no ambiente virtual. Entretanto, lacunas notáveis persistem, sobretudo quando se pondera a rápida evolução tecnológica.

Observa-se que um dos principais obstáculos para o enfrentamento do crime cibernético no Brasil é a falta de conscientização pública sobre os perigos da internet, a insuficiência de recursos e a carência de especialistas em segurança cibernética. De acordo com dados da *Fortinet*[64], no primeiro semestre de 2022, houve 31,5 bilhões de tentativas de ataques cibernéticos a empresas no Brasil, um crescimento de 94% em comparação com o mesmo período do ano anterior, que teve 16,2 bilhões de registros. Uma das razões para essa alta

---

[60] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 29.

[61] PINHEIRO, Patrícia Peck, Direito digital. 6.ed., atual. e ampl. São Paulo: Saraiva, 2016, pg. 58.

[62] *Ibidem*

[63] 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-específica-2. Acesso em 14 de abr. 2023.

[64] 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-cre sceram-94

incidência de ataques é o baixo investimento em cibersegurança. Além disso, o Brasil é considerado um dos principais focos de origem de ataques cibernéticos no mundo, conforme um relatório da Kaspersky, empresa de segurança cibernética, que atribui ao Brasil 10% dos ataques cibernéticos globais[65].

Dessa forma, a complexa relação entre a sociedade da informação e o crime cibernético, reside a necessidade de desenvolver estratégias multidisciplinares que abordem tanto as dimensões tecnológicas quanto as sociais. A colaboração entre setores, como governos, juristas e a comunidade científica, é essencial para a criação de marcos regulatórios adequados, investimento em segurança cibernética e educação pública sobre os riscos e as práticas seguras nesse novo cenário de criminalidade.

1.3.2 Definição jurídica para os crimes cibernéticos

O conceito atribuído aos crimes que se utilizam dos dispositivos informáticos para cometer ilícitos penais, com ou sem auxílio da rede de transmissão de dados, varia de acordo com o entendimento de cada autor.

Na linguagem cotidiana, é comum depararmos com a expressão crimes cibernéticos sendo utilizada para descrever um conjunto específico de condutas que violam interesses jurídicos protegidos pelo Direito Penal e que estão de alguma forma relacionadas a dados e sistemas informáticos. No entanto, para Leonardi a essa expressão não é adequada, pois se baseia apenas no uso popular do termo cibernética, associando-o a tudo o que está relacionado às tecnologias modernas, especialmente a informática[66].

Outras diversas nomenclaturas são empregadas para se referir aos delitos cometidos no ambiente virtual, tais como "Crimes de computador", "Crimes de informática", "Cibercrimes", "Delitos computacionais", "Crimes eletrônicos", "Crimes telemáticos", "Crimes informacionais" e outras similares[67].

Verifica-se a existência de múltiplas terminologias para classificar os crimes cibernéticos devido à ampla gama de atividades que essas ações englobam. A designação atribuída aos delitos que empregam dispositivos informáticos para cometer transgressões

[65] 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.

[66] PIMENTEL, Alexandre Freire. Direito cibernético: um enfoque teórico e lógico-aplicativo. Rio de Janeiro: Renovar, 2000. p. 83

[67] CRESPO. Op. Cit, pg 50

penais, com ou sem o auxílio de redes de transmissão de dados, varia de acordo com a perspectiva de cada pesquisador sobre essas infrações e a forma como são executadas, resultando em uma falta de consenso terminológico[68].

A nomenclatura proposta por Jesus e Milagre seria crimes informáticos ou delitos informáticos, já que englobam as ações cometidas por meio de computadores, direcionados a esses dispositivos ou realizados por intermédio deles, e conceitua como sendo fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação[69].

Leonardi utiliza a nomenclatura delitos digitais, e entendem que englobam uma gama de condutas, incluindo o acesso indevido a sistemas informáticos, ações destrutivas em tais sistemas, interceptação de comunicações, manipulação de dados, violações de direitos autorais, incitação ao ódio e discriminação, difamação religiosa, divulgação de material pornográfico envolvendo menores, atos de terrorismo, dentre outros[70].

Para Paulo Lima o termo crime de computador é a melhor forma de descrever esses tipos de infrações, fundamentando sua escolha no argumento de que o computador constitui o instrumento primordial para a realização desses atos ilícitos. Ele também ressalta que quando o computador é empregado como um meio facilitador para a execução de práticas criminosas, essa conduta também deve ser classificada como um crime dessa natureza[71].

Sandra Gouvêa opta por utilizar a expressão crimes por meio da informática, justificando sua escolha ao argumentar que os computadores não são os únicos instrumentos capazes de serem utilizados em práticas criminosas[72].

Na doutrina espanhola, desde o início dos anos 1980, adotou-se a terminologia de delitos informáticos. Essa expressão foi traduzida a partir do termo anglo-saxão "*computer crime*", amplamente utilizado pelo Departamento de Justiça norte-americano[73].

---

[68] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg.69.

[69] *Ibidem.*

[70] LEONARDI, Marcel. Op. Cit. Pg21.

[71] LIMA, Luciano Flores de (Org.). Cooperação Jurídica Internacional em matéria penal. Porto Alegre: Verbo Jurídico, 2010.

[72] GOUVÊA, Sandra. O direito na era digital: crimes praticados por meio da informática. Manual Editora Ltda, 1997.

[73] CRESPO. Op. Cit, pg. 48

Já a convenção de Budapeste vale-se da expressão "*Cybercrime*", como o melhor termo para definir todas as atividades criminosas no ambiente digital[74].

No Brasil, a nomenclatura normalmente utilizada para os crimes digitais é chamada de delitos informáticos, termo usual utilizado por países de língua espanhola que se relaciona à ideia de proteção do objeto jurídico informático e informação[75].

Percebe-se, portanto, que não há consenso nos termos empregados pelos estudiosos, isso decorre das múltiplas formas de ações delituosas no amplo espectro da informática, abarcando diversas tecnologias de processamento e transmissão de dados. Essa abrangência gera uma manifestação criminal que, mesmo com suas distintas classificações, pode ser identificada pelo seu objeto ou pelos métodos empregados. Estes últimos fornecem um elemento comum, embora variem em terminologia nos diversos países ou entre diferentes autores[76].

Nesse sentido, para caracterizar se uma conduta é criminosa ou não é necessária uma análise prévia, inicialmente para discernir se a ação se qualifica como cibercrime ou não, seguida pela aplicação do dispositivo penal adequado, considerando a salvaguarda do bem jurídico afetado, ou seja, a prática de transgressões perpetradas pela internet e passíveis de enquadramento no ordenamento jurídico nacional[77].

Para Viana, uma boa prática na área jurídica é atribuir nomes aos delitos com base no bem jurídico que eles protegem. Nesse sentido a denominação delitos virtuais seria completamente absurda, uma vez que, mesmo considerando que esses delitos são cometidos em um ambiente virtual, não faz sentido falar de um bem jurídico virtual, tendo, portanto, apenas duas opções viáveis: delitos informáticos ou delitos computacionais[78].

De acordo com Delgado, a questão central na definição da terminologia a ser adotada reside na possibilidade de os dados e sistemas informáticos serem tanto o objeto de uma conduta criminosa quanto o instrumento utilizado para cometer o crime. Essa dualidade amplia as modalidades possíveis de crimes cibernéticos, abrangendo não apenas aqueles que visam

---

[74] CONSELHO DA EUROPA. Disponivel em:https://rm.coe.int/16802fa428. Acesso em 14 ago.2023.

[75] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 70

[76] FERREIRA, Ivette Senise. A Criminalidade Informática. In: LUCCA, Newtow de; SIMÃO FILHO, Adalberto (Coord.). Direito & Internet – Aspectos Jurídicos Relevantes. São Paulo: Edipro, 2001. p 207-237

[77] SANCHES, A. G.; ANGELO, A. E. 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/1> Acesso em: 03 jan. 2023.

[78] VIANNA, Túlio Lima. Fundamentos de direito penal informático: do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003, pg 55.

diretamente os sistemas informáticos, mas também outros delitos quando praticados por meio da informática[79].

Para Wang, houve uma evolução da terminologia de "crimes computacionais" ou "crimes informáticos" para "crimes virtuais", "crimes digitais" ou "crimes cibernéticos" atribuída à crescente relevância da internet e das redes informacionais. Inicialmente, o foco estava no envolvimento de computadores e sistemas informáticos nos delitos. No entanto, com a popularização da internet, termos como "crimes cibernéticos" ou "virtuais" ganharam destaque, refletindo o papel preponderante das redes e da conectividade no ciberespaço nas infrações[80].

Castro afirmar em sua pesquisa que a falta de consenso na doutrina acerca das terminologias referente aos crimes cibernéticos pode variar, mas não altera a essência dos atos que envolvem o uso de tecnologia informática e redes de transmissão de dados para cometer infrações, atentando contra um bem jurídico específico. Para que seja caracterizado como crime, a ação deve ser típica, antijurídica e culpável[81].

Em suma, embora não haja consenso sobre a melhor nomenclatura a ser utilizada para os atos ilícitos cometidos em ambiente virtual, essa variação terminológica é meramente superficial, uma vez que o cerne reside na identificação das condutas. Fundamentalmente, é necessário considerar o uso de dispositivos informáticos, a utilização das redes de transmissão de dados para perpetrar os crimes e a análise do bem jurídico lesado[82].

Para fins desta pesquisa, será utilizado o termo crime cibernético para se referir aos delitos praticados no ambiente virtual. Optou-se pela referida nomenclatura devido ser o mesmo termo empregado na versão do texto em português da convenção de Budapeste, inserido no ordenamento jurídico pelo decreto 11.491/2023[83], que também será objeto de análise nesta pesquisa.

---

[79] DELGADO, Vladimir Chaves. Cooperação internacional em matéria penal na convenção sobre o cibercrime. Tese de Doutorado. Centro Universitário de Brasília. Brasília: 2007.Pg 19.

[80] WANG, Qianyun. A Comparative Study of Cybercrime in Criminal Law: China, US,England, Singapore and the Council of Europe. Tese (doutorado) – Erasmus University.Rotterdam. Rotterdam, 2016, pg 15.

[81] CASTRO, José Roberto Wanderley de. A tipicidade dos crimes cibernéticos no direito penal brasileiro: um estudo sobre o impacto da lei 12.737/2012 e a (des) construção de uma dogmática penal dos crimes cibernéticos. 2018. pg115.

[82] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 70.

[83] CONSELHO DA EUROPA. Disponível em: https://rm.coe.int/16802fa428. Acesso em 14 ago.2023.

1.3.3 Características dos cibernéticos

Os crimes cibernéticos são caracterizados principalmente pelo uso de tecnologias, como computadores, internet ou qualquer dispositivo que tenha acesso a rede. Esses crimes são considerados meios, pois sua inovação reside na forma como são cometidos, e possuem como principal característica o uso internet. Ocorre que muito embora sejam cometidos em ambientes virtual, tem impacto direto no mundo real[84].

A convenção de Budapeste define crime cibernético ou cibercrime como está na redação do dispositivo, como sendo atos praticados contra a confidencialidade, integridade e dispositivo de sistemas informáticos de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados[85].

Dessa forma os crimes virtuais compreendem um espectro de condutas que se enquadram nos parâmetros de tipicidade, antijuridicidade e culpabilidade, realizadas por meio do emprego de dispositivos informáticos ou quaisquer sistemas de informática[86].

Na visão de Sieber, devido à ampla variedade de crimes cibernéticos e à notável incidência de crimes não registrados judicialmente, é desafiador tirar conclusões precisas sobre a extensão e natureza da criminalidade cibernética a partir dos números comumente divulgados. Ele destaca que as diferenças nas definições e classificações desses crimes complicam ainda mais a análise histórica da evolução da criminalidade cibernética. Essa questão se torna especialmente problemática em um contexto internacional, onde as variações nas classificações e procedimentos de registro podem levar a interpretações distorcidas sobre a extensão e natureza desses crimes[87].

Jonathan Clough identifica seis obstáculos associados aos crimes cibernéticos, sendo eles a escala, acessibilidade, anonimato, portabilidade e transferibilidade, alcance global e a falta de guardiões eficientes. Ele explica que a escala é um desafio devido à capacidade da internet de facilitar comunicações rápidas e econômicas entre muitas pessoas, aumentando

[84] BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. Investigação Cibernética á Luz do Marco Civil da Internet**.** Sao Paulo: Brasport, 2016. Pg,240.

[85] CONSELHO DA EUROPA. Op. Cit.

[86] CAIADO, F.; CAIADO, M. Combate à pornografia infantojuvenil com aperfeiçoamentos na identificação de suspeitos e na detecção de arquivos de interesse. In: Ministério público federal. Crimes cibernéticos. Brasília: MPF, 2018. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos. Acesso em: 02 ago 2023.

[87] SIEBER, Ulrich. Legal aspects of computer-related crime in the information society.European Comission. University of Würzburg, 1998. Disponível em: http://www.oas.org/juridico/english/COMCRIME%20Study.pdf. Acesso em 03 ago. 2023.

assim o número de indivíduos potencialmente vulneráveis a ofensas cibernéticas. A acessibilidade é outro problema, uma vez que o uso da internet se popularizou e não requer conhecimento técnico especializado, ampliando o escopo de potenciais vítimas e perpetradores[88].

O anonimato representa um desafio nos crimes cibernéticos, pois favorece o criminoso, tornando sua identificação difícil para a vítima e para os órgãos de aplicação da lei. A complexidade aumenta quando as informações atravessam várias jurisdições. A portabilidade e a transferibilidade de dados também são problemáticas, uma vez que a tecnologia permite o armazenamento e a transferência rápida e barata de dados. O alcance global é um desafio adicional, pois os crimes podem ocorrer e ter impactos além das fronteiras jurisdicionais devido à conectividade da internet. A falta de guardiões eficazes ressalta o baixo risco percebido pelo criminoso de ser identificado e perseguido, um obstáculo ampliado pela necessidade de técnicas forenses avançadas e comunicação rápida entre autoridades de diferentes jurisdições[89].

A natureza transnacional dos crimes cibernéticos é outra característica que deve ser enfatizada, onde a conduta criminosa e seus efeitos podem se manifestar em vários países, levando a conflitos de jurisdição. Isso ocorre quando há incerteza sobre qual país tem a autoridade para processar o infrator. Assim, embora os crimes cibernéticos ocorram dentro de um território específico, seus impactos podem ser sentidos internacionalmente.[90]

1.3.4 Classificação dos crimes cibernéticos

Possivelmente, o maior desafio inerente a esta pesquisa residiu na abordagem das categorizações dos delitos cibernéticos. A dificuldade se justifica ao observar que há também muita divergência doutrinária sobre esse tema, não havendo consenso entre os estudiosos sobre a melhor classificação para os crimes cibernéticos.

Tal divergência, por vezes, é atribuível ao fato de que a constante evolução tecnológica ocasionou uma mudança de perspectiva ao longo dos anos. Ainda que as algumas classificações possam parecer incorretas ou equivocadas, a necessidade de categorizar os crimes digitais se

[88] CLOUGH, Jonathan. A world of difference: the Budapest Convention on cybercrime and the challenges of harmonisation. 2014. Monash University Law Review, vol. 40, nº.3, p. 698-736. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2615789. Acesso em 23/09/2023.

[89] CLOUGH,. Op. Cit.

[90] WANG. Op. cit, pg 17.

faz imperiosa, uma vez que isso fornece o alicerce para a subsequente explanação de condutas específicas.

No entanto, é crucial estabelecer algumas noções primordiais acerca das classificações delineadas na doutrina. Essa demanda se justifica pela observação de que, em diversas circunstâncias, o sistema informático desempenha um papel meramente instrumental na realização do delito[91].

Nesses casos, a utilização desse sistema poderia ser dispensada sem comprometer a execução da conduta em questão. Em outras palavras, estamos tratando de delitos de natureza livre, suscetíveis de serem perpetrados por distintos *modus operandi*. Contudo, em contrapartida, há condutas que somente podem ser efetuadas contra um sistema informático ou as informações nele contidas[92]. Dessa forma para uma melhor análise será demonstrado algumas classificações encontradas na doutrina.

Na metade da década de 1980, Tiedemann tratou da criminalidade informática no contexto dos delitos econômicos, e os classificou conforme a tabela mencionada[93]:

Manipulações	Podem afetar o input (entrada) ou output (saída) ou mesmo o processamento de dados.
Espionagem	Subtração de informações arquivadas, abarcando-se ainda o furto ou emprego indevido de software
Sabotagem	Destruição total ou parcial de programas
Furto de tempo	Utilização indevida de instalações de computadores por empregados desleais ou estranhos.

Tabela 01

O trabalho de Sieber contribuiu significativamente para a compreensão dos crimes vinculados à informática. Suas pesquisas, especialmente elaborado para a Comissão Europeia, além de atualizar concepções anteriores, trouxe uma classificação dos delitos da seguinte maneira[94]:

Ofensas contra direitos individuais	a)Uso incorreto de informação.

[91] CRESPO. Op. Cit, pg. 61

[92] CRESPO. Op. Cit, pg. 62.

[93] TIEDEMANN, Klaus. Lecciones de derecho penal económico.Barcelona: PPU, 1993

[94] SIEBER,Op. Cit.

	b)Obtenção ilegal de dados e posterior arquivo da informação. c) Revelação ilegal e mau uso da informação d) dificuldade de se distinguir entre obtenção, arquivamento ou revelação de informações.
Crimes econômicos:	a) Fraude por manipulação de dados em sistemas de processamento; b) Espionagem de dados e pirataria de programas; c) Furto de serviço ou furto de tempo; d) Sabotagem e extorsão; e) Acesso não autorizado a sistemas de processamento de dados; f) uso do computador para crimes empresariais;
Ofensas contra direitos supraindividuais	a)Ofensas contra interesses estaduais e políticos; b)Extensão desta categoria para crimes contra a integridade humana;

Tabela 02

Entre doutrinadores nacionais citamos duas classificações mais utilizadas. A primeira adotada por Viana[95], que entende da seguinte forma:

Delitos Informáticos Impróprios	Delitos em que o computador foi o instrumento para a execução do crime, mas que não provocou lesão à bem jurídica “inviolabilidade da informação automatizada” (dados)
Delitos Informáticos Próprios	Delitos em que são afetados os dados
Delitos Informáticos Complexos	Nos quais , além da inviolabilidade dos dados há outro bem jurídico lesado e recebem a denominação de Delitos Informáticos Mistos
Delitos Informáticos Mediatos ou Indiretos	Que atuam como crime meio para a realização de um crime fim.

Tabela 03

[95] VIANA. Op. Cit, pg 29.

A segunda que é adotada por Ivete Senise Ferreira e Vicente Greco Filho, divide os crimes digitais em: A) condutas perpetradas contra um sistema informático e b) condutas perpetradas contra outros bens jurídicos[96].

Na visão de Damásio e Milagres, a classificação mais precisa que se assemelha à realidade brasileira é a proposta por Briat, que classifica os crimes informáticos em: A) crimes onde a informática é o meio para a prática dos velhos crimes ou agressão ao bem jurídico protegido pelo Direito Penal, e B) crimes informáticos em que a informática (inviolabilidade dos dados) é bem jurídico protegido, propriamente dito[97].

De acordo com Crespo, as condutas dirigidas a sistemas informáticos ou dados podem ser categorizadas como delitos de risco informático, enquanto outras ações podem ser classificadas como delitos relacionados à informática. Sob essa perspectiva, é possível afirmar que todas as ações voltadas a bens jurídicos informáticos, como sistemas e dados, podem ser consideradas delitos próprios de risco informático. Em contrapartida, aquelas ações que têm como alvo bens jurídicos tradicionais, não relacionados à tecnologia, podem ser identificadas como crimes digitais impróprios[98].

Nesta pesquisa, optou-se pela classificação proposta por Damásio e Jesus, a qual se revela mais adequada para o ordenamento jurídico. Segundo os autores, os crimes informáticos podem ser categorizados em três tipos distintos: próprios, impróprios mistos e mediato ou indireto. Essa classificação permite uma compreensão mais precisa e abrangente dos delitos cometidos no âmbito digital[99].

1.3.4.1 Crimes cibernéticos próprios, impróprios, mistos e mediatos ou indiretos.

No caso dos crimes cibernéticos próprios, sua principal característica são 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.

Nos 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

---

[96] FERREIRA, Ivette Senise. Op Cit. p 207-237

[97] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 78.

[98] CRESPO. Op. Cit, pg. 64.

[99] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg78.

eletrônica, clonagem de cartões de crédito e sequestro de dados. A caracterização e distinção desses crimes têm como base não somente a utilização de computadores, mas também a ampla gama de sistemas de informática que possibilitam a materialização dessas ações[100].

Segundo Luís Castro, crimes virtuais próprios são aqueles que necessitam do uso da tecnologia da informação para serem cometidos. A execução e a informação utilizada são impossíveis sem um meio eletrônico. Atualmente, os crimes informáticos próprios nasceram como resultado direto da digitalização e informatização de dados, podendo ser executados apenas no ambiente virtual. São na verdade crimes informáticos, pois nasceram destes são o bem juridicamente protegido[101].

Delgado aponta que, no contexto dos crimes cibernéticos próprios, o foco da proteção jurídica não se limita aos sistemas informáticos, mas se estende também à segurança informática, tratada como uma entidade distinta dos direitos da personalidade. Ele enfatiza que essa segurança, analogamente à segurança digital, é caracterizada pela preservação da confidencialidade, disponibilidade e integridade dos dados e informações contidos no sistema[102].

Para Delgado, a conduta criminosa nos crimes cibernéticos próprios envolve o uso indevido do sistema informático e dos dados nele armazenados, processados ou transmitidos. Isso pode incluir práticas como acesso não autorizado ao sistema, divulgação ou transmissão não autorizada de informações, coleta ou interceptação não autorizada de dados e interferência no funcionamento do sistema[103].

As características distintas dos crimes cibernéticos muitas vezes se manifestam em ações isoladas, mas impactantes. Um exemplo típico envolve um ato único onde a vítima, inadvertidamente, baixa um software malicioso. Este pode ser um gravador de assinatura digital ou um cavalo de troia, ambos explorando vulnerabilidades ou falhas de segurança existentes no sistema do usuário. A sofisticação desses ataques reside na habilidade dos criminosos de

---

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

[101] CASTRO, Luís Fernando Martins. Direito da informática e do ciberespaço. Revista de Derecho. Informático. n. 064, novembro 2003. Disponível em: <http://www.alfa-redi.org/rdi-articulo.shtml?x=1270>.Acesso em: 3 abr.2009.

[102] DELGADO . Op. Cit. Pg 26.

[103] *Ibidem.*

infiltrar-se de maneira eficaz, aproveitando-se das lacunas e fragilidades na segurança cibernética[104].

Já no caso dos crimes cibernéticos impróprios, eles se distinguem por serem cometidos de qualquer forma, podendo ou não ser em um dispositivo eletrônico. O uso da internet por si só não é um meio de eliminar a atividade criminosa. Crespo afirma que não há muita diferença na forma de atuação em casos de crimes cibernéticos impróprios. Em outras palavras, independentemente da forma como a ação penal é realizada, o método utilizado não é necessário para especificar o crime[105].

Segundo Viana, os crimes informáticos impróprios se caracterizam pelo uso do computador como meio para cometer o crime, mas sem que ocorra uma violação ao bem jurídico associado à inviolabilidade da informação automatizada. Nesse ponto, a característica definidora de um crime cibernético impróprio é a ausência de ofensa à inviolabilidade do sistema informacional ou das informações automatizadas[106].

São crimes tradicionais que utilizam a tecnologia da informação para sua realização sem necessariamente exigir uma conexão íntima com o ambiente virtual. Eles usam a internet como uma ferramenta para ocultar ou facilitar atividades criminosas, o que pode trazer sérias repercussões para as vítimas. Como resultado, ao contrário dos crimes cibernéticos próprios, esses crimes não exigem conhecimento técnico em redes de computadores ou sistemas de armazenamento de dados. O objetivo desses crimes não é necessariamente violar a segurança dos dados digitais, mas sim violar outros direitos legais que já são protegidos por penalidades criminais existentes ao se envolver em atividades criminosas cotidianas[107].

Nesses tipos de crimes cibernéticos, as características essenciais que os distinguem é a interação repetida com a vítima, através da qual os criminosos visam aproveitar-se do relacionamento estabelecido para cometer o crime. Além disso, é comum que esses criminosos utilizem programas não classificados como atividades ilegais, tais como aplicativos de conversação instantânea, como uma forma de camuflar suas ações ilícitas[108].

---

[104] CRESPO. Op. Cit, pg. 67.

[105] *Ibidem.*

[106] VIANA. Op. Cit, pg.38-39.

[107] CRESPO, Marcelo Xavier de Freitas. Op. Cit, pg 68.

[108] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg.77

Sobre os crimes impróprios, Jose Roberto Castro defende que a legislação atual é suficiente, uma vez que a maioria dos bens jurídicos tutelados já são contemplados pelo ordenamento jurídico[109]. Um exemplo relevante são os crimes contra a honra, que incluem a calúnia (Art. 138), difamação (Art. 139) e injúria (Art. 140). Além disso, também é possível citar crimes como o induzimento ou instigação ao suicídio (Art. 122) e a apologia de crime ou de criminoso (Art. 287), entre outros[110].

Um exemplo que ganhou destaque na mídia nacional e internacional foi o Jogo da Baleia Azul (Blue Whale). Tratava-se de um jogo que indicava uma série de desafios de alto risco, culminando no incentivo ao suicídio por parte do jogador. O russo Philipp Budeikin, de 21 anos, criador do jogo de suicídio afirmou que via suas vítimas como lixo biológico. Preso e em julgamento por incitar o suicídio de vários adolescentes, confessou os crimes e disse à polícia que estava limpando a sociedade[111]. É importante ressaltar que o induzimento ao suicídio ocorreu por meio da internet, mais especificamente das redes sociais.

Nesse contexto, é relevante destacar que o bem jurídico afetado é a vida, e não a informação contida nos computadores, caracterizando assim um crime informático impróprio[112]. A maior parte dos crimes perpetrados na internet ocorrem também no mundo físico, sendo que a rede mundial de computadores atua apenas como um instrumento facilitador devido à possibilidade de anonimato que ela proporciona[113].

Ainda no contexto da classificação dos crimes informáticos, emerge uma categoria peculiar conhecida como crimes informáticos mistos, esses crimes caracterizam-se pela intersecção entre condutas perpetradas no ambiente digital e suas implicações no mundo real, constituindo uma convergência entre o ciberespaço e o espaço físico[114].

---

[109] CASTRO, José Roberto Wanderley de. A tipicidade dos crimes cibernéticos no direito penal brasileiro: um estudo sobre o impacto da lei 12.737/2012 e a (des) construção de uma dogmática penal dos crimes cibernéticos. 2018. pg 115.

[110] BRASIL. Código de processo penal. Disponível em: <http://http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm> Acesso em 25/07/2023.

[111] Preso, criador do jogo de suicídio Baleia Azul fala em "limpeza da sociedade". Disponível em: http://ultimosegundo.ig.com.br/mundo/2017-05-10/baleia-azul.html

[112] CABETTE, Eduardo Luiz Santos. Jogo da Baleia Azul: Tipificação penal e competência para processo e julgamento**.** 2017. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2017/04/24/jogo-da-baleia-azul-tipificacao-penal-e-competencia-para-processo-e-julgamento/. Acesso em: 14 ago. 2023.

[113] PINHEIRO, Patrícia Peck, Direito digital. Op. Cit. pg. 58.

[114] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg.68

Nessa abordagem, são contempladas situações em que as ações em meios eletrônicos culminam em repercussões tangíveis, afetando bens, indivíduos ou sistemas para além do ambiente virtual. Tais delitos denotam a complexidade da criminalidade contemporânea, em que as fronteiras entre os universos *online e offline* tornam-se tênues, desafiando os sistemas jurídicos a adequarem-se a essa realidade em constante evolução[115].

Conforme explicação de Mirabete, é possível discernir que, em contraposição aos crimes simples em que o tipo é singular e a transgressão atinge um único bem jurídico, os crimes complexos apresentam uma configuração distinta. Estes se caracterizam pela presença de dois ou mais tipos delitivos em uma mesma norma penal (denominados crimes complexos em sentido estrito) ou abrangem uma ação tipificada e outras que, por si só, não seriam consideradas típicas (denominados crimes complexos em sentido amplo)[116].

Para ilustrar um delito misto, é possível citar a disposição consagrada no Art. 67, VII, da Lei nº 9.100, de 29 de setembro de 1995[117], que tipifica como infração eleitoral a conduta de adquirir indevidamente acesso ao sistema de informações eleitorais com o intuito de manipular a apuração dos votos, inclusive punindo a tentativa[118].

Observa-se que o artigo mencionado já estabelece a tipificação da conduta de acessar um sistema de tratamento automático de dados (sistema computacional), desde que com o objetivo de interferir na apuração ou contagem de votos. No entanto, essa tipificação se aplica apenas aos sistemas utilizados pelo serviço eleitoral, não havendo previsão para os sistemas particulares. Um detalhe extremamente importante da tipificação do artigo 72º é que o acesso não é punido sem a intenção de interferir na apuração ou contagem de votos. Existe um elemento subjetivo específico no tipo penal. Portanto, aqueles que praticarem essa conduta com um elemento subjetivo específico (por exemplo, obter dados dos eleitores para a prática de extorsão ou envio de material comercial) não estarão sujeitos à tipificação mencionada[119].

---

[115] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg.68.

[116] MIRABETE, Julio Fabbrini. Manual de direito penal: parte geral. 23. ed. São Paulo: Atlas, 2006. Vol. 1. Revista e atualizada por Renato N. Fabbrini.

[117] BRASIL. Código Eleitoral. Lei nº 4.737, de 15 de julho de 1965. Disponível em: https://www.tse.jus.br/legislacao/codigo-eleitoral/codigo-eleitoral-1/codigo-eleitoral-leinb0-4.737-de-15-de-julho-de-1965.

[118] Lei nº 9.100, de 29 de 1995.Estabelece normas para a realização das eleições municipais de 3 de outubro de 1996, e dá outras providências. Planalto. Disponível em:<http://www.planalto.gov.br/ccivil_03/leis/L9100.htm>. Acesso em: 13 jul. 2023.

[119] CRESPO. Op. Cit, pg. 70.

No caso dos crimes informáticos mediatos, também conhecidos como crimes informáticos indiretos, o computador é utilizado como uma ferramenta para a prática de outras infrações penais. Esses crimes envolvem o uso da tecnologia da informação para facilitar a execução de atividades ilegais, como fraudes, lavagem de dinheiro, espionagem cibernética, entre outros[120].

Nas palavras de Damásio e Milagres, normalmente um crime informático é cometido como meio para a prática de um crime fim de ordem patrimonial. Ele exemplifica o caso do agente que captura dados bancários e usa para desfalcar a conta corrente da vítima. Pelo princípio da consumação, o agente só será punido pelo delito fim (furto)[121].

É importante observar que, conforme Vianna esclarece, é preciso evitar a confusão entre o delito informático mediato e o delito informático impróprio, uma vez que nos casos mediados ocorre a lesão ao bem jurídica inviolabilidade de dados informáticos, ainda que tal lesão não seja sancionada pela aplicação do princípio da consunção. Além disso, Vianna ressalta a distinção dos delitos informáticos mediatos dos delitos informáticos mistos, uma vez que no caso dos primeiros há dois tipos penais diversos, cada um deles visando a proteção de um bem jurídico específico[122].

Portanto, é possível observar que a mera utilização de um computador para a prática de um crime, como o estelionato, não deveria ser considerada, com precisão técnica, um crime informático. No entanto, tanto autores quanto a mídia em geral adotaram a convenção de denominar crimes informáticos qualquer delito cometido com o uso da tecnologia, seja como instrumento da conduta, seja como objeto ilícito. Embora essa classificação não seja a mais precisa do ponto de vista técnico, é impossível ignorá-la devido à sua popularidade acadêmica e, por consequência, social. A mídia em geral também passou a utilizar essa mesma terminologia[123].

[120] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 79.

[121] *Ibidem.*

[122] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 80.

[123] VIANNA. Op. Cit, pg. 55.

1.3.5 Sujeito Ativo

O sujeito ativo no contexto penal é definido como todo ser humano, dotado de certos atributos, como capacidade de compreensão e de determinação[124]. A identificação do sujeito ativo e a imputação objetiva nos crimes cibernéticos são tarefas extremamente desafiadoras, especialmente quando há ausência física do indivíduo em questão. Diante da importância de identificar o autor de um crime e das dificuldades associadas a essa tarefa, surgiu a necessidade de categorizar grupos que praticam crimes cibernéticos específicos.

No imaginário popular, possivelmente influenciado por representações cinematográficas e campanhas publicitárias, tradicionalmente se associa ao criminoso cibernético a uma imagem estereotipada de um indivíduo jovem, desleixado em sua aparência, porém excepcionalmente talentoso e conhecedor profundo da área de informática. No entanto, é importante ressaltar que essa construção do senso comum não se sustenta diante da realidade complexa e heterogênea dos atores envolvidos no cenário dos crimes cibernéticos[125].

Para Glenny[126], a maioria dos cibercriminosos é do sexo masculino, possuindo pouca habilidade em se comunicar, com idade entre 13, 14 ou 15 anos, ou seja, antes mesmo de ter valores morais consolidados, fazendo do mundo virtual seu palco de talentos, sem precisar se relacionar diretamente com as pessoas[127].

Atualmente, observou-se uma quebra desses estereótipos, uma vez que qualquer indivíduo pode se tornar um criminoso especializado. Essa possibilidade é ampliada pela própria internet, que disponibiliza informações e técnicas relacionadas a uma ampla gama de crimes, abrangendo desde a obtenção ilegal de senhas e identidades até a realização de grandes fraudes em sistemas[128].

No cenário virtual é importante ressaltar que, embora qualquer pessoa possa se envolver em atividades de cibercrime, é comumente atribuída aos hackers a autoria desses crimes. No entanto, o termo "*hacker*" não é o mais apropriado, uma vez que originalmente era utilizado para descrever indivíduos com habilidades avançadas em computação. Além disso, os autores afirmam que tanto especialistas da área quanto a doutrina preferem se referir aos criminosos

[124] GUEIROS, Artur; JAPIASSÚ, Carlos Eduardo. Direito penal: volume único. **São Paulo: Atlas**, 2018, pg.198.

[125] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 86.

[126] GLENNY, Misha. McMáfia: o crime organizado sem fronteiras. Porto: Civilização Editora, 2008.

[127] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 88.

[128] *Ibidem*

cibernéticos como "crackers", termo este que teria sido criado pelos próprios hackers para evitar confusões com outros indivíduos, pois esses possuem claramente intenções ilícita[129] .

De um lado, os *hackers*, muitas vezes apelidados de "fuçadores", encarnam a curiosidade inerente à exploração do potencial tecnológico, enquanto, do outro lado, os *crackers*, considerados os verdadeiros transgressores, imprimem suas marcas na rede por meio de invasões e destruições, muitas vezes com objetivos ilícitos. Essas definições, baseadas em uma compreensão refinada dos termos, estabelecem os pilares para a análise das interações entre esses agentes e a dimensão digital que habitam.

Para Crespo, existe uma série de denominação para identificar os responsáveis por condutas ilícitas[130]. Damásio e Jesus trazem as seguintes definições para os sujeitos ativos nos crimes cibernéticos [131]:

HACKER	Fuçador. Expressão que surgiu nos Laboratórios do *MIT(Massachusetts Institut of Technology*). Qualquer um que tenha grande conhecimento sobre tecnologia e que faça inovações.
CADERS	Estelionatários especializados em fraudes com cartões.
CRACKERS	Seriam os verdadeiros criminosos da rede. Utilizam seus conhecimentos de tecnologia para más finalidades.
PHEREAKER	São os “hackers da telefonia”, capazes de realizar interceptações, paralisar serviços e até mesmo utilizar a telefonia em nome de terceiros.

Tabela 04

Ainda sobre as classificações dos sujeitos ativos dos crimes cibernéticos existem os chamados de "*white hats"* (chapéu Branco)*, "gray hats"* (chapéu cinza) *e "black hats" (chapéu preto).* Os *"black hats"* representam os "c*rackers*", indivíduos com profundos conhecimentos tecnológicos que os aplicam em atividades de natureza criminosa. Por sua vez, os "*white hats*" correspondem aos "*hackers*", também conhecidos como “hackers éticos”, peritos que direcionam suas aptidões para o propósito benéfico de reforçar a segurança dos sistemas. Nessa

[129] ANANIAS, Ricardo A. R. e WANDERLEY, Lucas F. Delito Informático e a Lei 12.737/12(Lei Carolina dieckamnn). In: (Vários) Anais do IV Congresso De Ciências Jurídicas: Jurisdição, Estado e Cidadania e VII Encontro Científico do Curso de Direito. 2014.Disponível em: consensusjuridico.com.br/anais/ANAIS2014.pdf>. Acesso em 02 de ago. de2023

[130] CRESPO. Op. Cit, pg. 70.

[131] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 88.

configuração, os "gray hats" ocupam uma posição intermediária, situando-se entre as categorias "*black" e "white hats*"[132].

Também existe a classificação dos que não possuem conhecimento em informática, mas pensam que têm. São os chamados de *Lammer*s e os *Wannables*. Sob a visão de uma defesa criminal, demonstrar que o cliente e um *Lammer* tem significado, pois poderia provar e atestar a ausência de autoria de um cibercrime, como a invasão por exemplo[133].

Segundo Dias, é oportuno destacar que o sujeito ativo envolvido nesse tipo de crime, embora tenha o estereotipo de um gênio da informática, com habilidades acima da média, introvertido, antissocial e motivado pelo desejo de superar as máquinas, esse perfil evoluiu ao longo do tempo. Como resultado da constante evolução dessa realidade, surgem novas modalidades de criminosos cibernéticos, que não necessariamente são jovens, inteligentes e especialista em informática, motivados apenas pelo objetivo de extrair, utilizar ou vender informações[134].

1.3.6 Sujeito Passivo

O sujeito passivo, no contexto do Direito Penal, é aquele detentor do bem jurídico tutelado pela legislação, sobre o qual incide a conduta tipificada do sujeito ativo. É necessário, antes de tudo, estabelecer uma distinção entre o sujeito passivo ou vítima do delito, que corresponde à entidade afetada pela ação ou omissão do agente ativo. Nos casos dos delitos cibernéticos, as vítimas podem ser tanto indivíduos singulares quanto instituições, como entidades financeiras e órgãos governamentais, que fazem uso de sistemas automatizados de informação, frequentemente interligados a terceiros. Sob essa perspectiva, qualquer pessoa que utilize computadores ou esteja conectada à internet se torna passível de ser alvo de um crime cibernético, independentemente de ser uma pessoa física ou uma entidade jurídica[135].

1.3.7 Lugar do Crime

A determinação do local do crime encontra sua definição no Código de Processo Penal, que adota a perspectiva da Teoria da Ubiquidade, mediante a qual a competência territorial é estabelecida primordialmente pelo ponto em que se efetiva a consumação do delito, seja na

---

[132] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 88.

[133] *Ibidem*.

[134] DIAS, Vera Elisa M. A Problemática da Investigação do Cibercrime. 2010. Disponível em www.verbojuridico.net/doutrina/2011/veradias_investigacaocibercrime.pdf>. Acesso em 20 de maio de 2018

[135] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 90.

totalidade ou em parte, bem como no lugar em que se originou ou deveria ter ocorrido o resultado. Consequentemente, diante de uma situação em que um indivíduo situado no Estado do Rio de Janeiro invada o sistema computacional de terceiro localizado em São Paulo, a jurisdição competente para processar e julgar o cibercrime seria aquela vinculada à localidade do dispositivo alvo da invasão[136].

Naturalmente, a autoridade brasileira detém competência para a condução do processo em casos de delitos digitais perpetrados por agentes brasileiros no exterior, quando a vítima se encontra em território nacional. Entretanto, é condicionado ao fato de que esse agente adentre a fronteira nacional. Vale ressaltar que infrações cometidas por intermédio de proxies[137], redes virtuais privadas (*VPNs*)[138] e outras ferramentas empregadas para ocultar a origem da conexão, em que o agente está localizado no Brasil e apenas se utiliza de um vínculo exterior, podem ser submetidas a processamento neste país, desde que o delinquente seja devidamente identificado. Nesse contexto, surge uma nova complexidade, uma vez que provedores estrangeiros se mostram relutantes em fornecer informações de acesso a aplicações realizadas por cidadãos brasileiros, embora alojadas em servidores estrangeiros[139].

Esse fenômeno está intrinsecamente ligado à aplicação do Direito Penal no âmbito internacional, onde se trata da definição da jurisdição nacional para o julgamento do delito e da responsabilidade do Estado brasileiro na repressão da ação[140].

Nas palavras de Damásio e Milagres as condutas ilícitas praticadas em território estrangeiro, em tese, não se aplicariam as normas brasileiras, considerando a soberania do país, sendo que a questão deveria ser tratada pela extradição[141].

No ordenamento jurídico nacional o roteiro é taxativo para a fixação da competência do órgão jurisdicional e a aplicação da lei penal. No entanto, no contexto dos crimes cibernéticos,

---

[136] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 90

[137] Proxy é um serviço que age como um intermediário entre o usuário e a internet, recebe e repassa todas as suas requisições ao site que você está acessando. Disponível em: https://tecnoblog.net/responde/o-que-e-proxy-e-qual-a-diferenca-para-a-vpn/#:~:text=Um%20proxy%20%C3%A9%20um%20servi%C3%A7o,proxy%20e%20n%C3%A3o%20o%20seu.

[138] Rede privada virtual, do inglês virtual private network, é uma rede de comunicações privada construída sobre uma rede de comunicações pública. O tráfego de dados é levado pela rede pública utilizando protocolos padrões, não necessariamente seguros.

[139] JESUS, Damásio de. MILAGRE, José Antônio. *Op. Cit*, pg. 91.

[140] GRECO, R. Curso de direito penal: parte especial. 13. ed. Niterói: Impetus, 2016. v. 2.

[141] JESUS, Damásio de. MILAGRE, José Antônio. *Op. Cit*.

a possibilidade de conflitos entre jurisdições estrangeiras é uma realidade. Isso ocorre devido à diversidade de critérios que podem ser considerados para determinar a competência, como a nacionalidade da vítima ou do autor, a natureza do bem jurídico afetado e os efeitos do crime. Essa concorrência de jurisdições dificulta a persecução criminal por parte do Estado brasileiro, uma vez que os conflitos entre diferentes jurisdições nacionais não podem ser solucionados pelo direito doméstico, mas sim por normas de Direito Internacional expressas em tratados, convenções, acordos bilaterais, entre outros.

Embora a jurisdição brasileira seja competente para julgar os crimes cibernéticos, os atos processuais e de investigação necessários à persecução penal só podem ser determinados pela jurisdição do Estado em cujo território ocorrem, uma vez que o monopólio dessas ações pertence a ele. Assim, a obtenção da realização desses atos em território estrangeiro ocorre por meio do instituto da cooperação jurídica internacional, um procedimento que envolve autoridades centrais e diplomáticas, juntamente com normas de Direito Internacional, sem as quais a viabilização da persecução se torna extremamente difícil[142].

Todavia, a precisão quanto ao lugar de consumação de um crime cibernético revela-se extremamente complexa, sobretudo devido à ausência de fronteiras no ambiente digital. Com efeito, os crimes cibernéticos frequentemente manifestam-se como eventos plurilocais, onde vítima e o agente ocupam posições geográficas distintas, ou ainda, quando a execução do delito é iniciada em uma localidade e a consumação ocorre em outra, ainda que dentro do mesmo território nacional[143].

1.3.8 O Bem jurídico protegido no crime cibernético

O bem jurídico protegido nos crimes cibernéticos pode variar dependendo do tipo de crime em questão. Pode incluir a privacidade, a integridade dos dados, a propriedade intelectual, a segurança da informação, a confidencialidade, a reputação, entre outros.

Conforme Spinieli, os bens jurídicos afetados através da internet não se limitam ao sistema informático em si, mas se estendem para dados pessoais armazenados ou acessíveis através desse sistema. A legislação também considera delitos relacionados ao conteúdo

[142] BECHARA, Fábio Ramazzini; FLORES, Dímitri Molina. Crimes cibernéticos: qual é o lugar do crime para fins de aplicação da pena e determinação da competência jurisdicional. Revista Direito Mackenzie, v. 13, n. 2, p. 1-21, 2019.

[143] BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. Op. Cit. p. 3.

disseminado online, como publicidade enganosa e abusiva, além de pornografia infantil, reforçando a necessidade de tipificação penal para tais condutas[144].

Para Damásio e Milagres a abordagem dos crimes informáticos sempre representou um desafio, especialmente considerando que um código penal extremamente arcaico. A despeito de oferecer tutela a grande parte das transgressões ocorridas no meio virtual, o referido código demonstra omissão em questões onde a informática deveria ser o próprio bem resguardado pelo âmbito do Direito Penal[145].

Considerando que a atuação delitiva deve ser criteriosa ao preservar os bens mais relevantes e indispensáveis nas relações sociais, intervindo de forma minimamente intrusiva na vida dos cidadãos, não foi uma tarefa simples aprovar uma legislação que tipificasse os crimes cibernéticos. Nesse cenário, apesar da reconhecida salvaguarda conferida aos bens jurídicos tradicionais, tornou-se imperativo estabelecer proteção diante das infrações cometidas em relação aos bens jurídicos informáticos[146].

Dessa forma, no contexto dos crimes cibernéticos é indiscutível que onde há relevância econômica deve haver relevância jurídica, sendo está a proteção que se delineia. A resguarda da integridade das informações bancárias, financeiras, entre outras, geradas e manipuladas por indivíduos e entidades, é crucial. Os sistemas informáticos que processam e tratam dados eletrônicos produzem significados e informações, tornando-se alvo da tutela penal, uma vez que as informações também constituem bens de valor[147].

---

[144] SPINIELI, Andre Luiz Pereira. Crimes Informáticos: Comentários ao projeto de lei nº 5.555/2013**.** 3. ed. Brasília: Ministério Público Federal, 2018. (Crimes Cibernéticos - Coletânea de artigos). Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos. Acesso em: 14 ago. 2023.

[145] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg.92.

[146] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg.92.

[147] ALBUQUERQUE, Roberto Chacon de. A Criminalidade Informática**.** Sao Paulo: Juarez de Oliveira, 2006. Disponível em: https://core.ac.uk/download/pdf/185253434.pdf. Acesso em: 14 ago. 2023.

2 COOPERAÇÃO INTERNACIONAL E O CRIME CIBERNÉTICO

2.1 Cooperação penal internacional

Com a chegada da chamada era da informação[148] iniciou-se uma nova preocupação: a abordagem das condutas ilícitas perpetradas no ciberespaço. Essas atividades redefiniram as fronteiras tradicionais, transcenderam limites geográficos e alteraram o panorama jurídico. Com base nessa realidade, a delimitação de competência e jurisdição tornou-se um tema bastante complexo, especialmente no contexto dos crimes cibernéticos[149].

Nesse sentido, a criminalidade cibernética, como foi evidenciado nos capítulos anteriores, transcenderam as fronteiras nacionais, requerendo uma abordagem internacionalmente cooperativa na política criminal. Em casos em que a conduta criminosa, os resultados ou as evidências se estendem por múltiplas jurisdições, a colaboração entre os estados se torna essencial. As diligências que ultrapassam as fronteiras de um estado específico são muitas vezes necessárias para abordar eficazmente as complexidades introduzidas pela natureza transnacional desses crimes e para implementar a proteção penal efetiva. Para tanto, se faz essencial que existam instrumentos que viabilizem a cooperação jurisdicional internacional.

De acordo com Paulo Abrão Pires Júnior, a concretização eficaz da justiça em um mundo cada vez mais interconectado requer uma colaboração e proatividade intensificadas entre as entidades estatais. A complexidade e o alcance global das relações jurídicas, que frequentemente transcendem as fronteiras de estados soberanos, amplificam a necessidade de uma cooperação internacional robusta. Esse engajamento colaborativo entre nações é crucial para atender às demandas de justiça tanto dos indivíduos quanto da sociedade como um todo, garantindo que a justiça seja realizada de maneira compreensiva e eficiente[150].

Dessa forma, para uma efetiva persecução penal no decorrer de uma investigação de criminal cujas ações, resultados ou evidências podem abranger mais de uma jurisdição, pode ser necessário realizar diligências além de uma jurisdição. Nesse caso, a interação entre os Estados para resolver as consequências da multiplicidade de soberanias envolvidas se mostra essencial.

---

[148] A “Era da Informação” é um conceito chave desenvolvido pelo sociólogo espanhol Manuel Castells. Ele descreve essa era como um período caracterizado pela ascensão da tecnologia da informação e da comunicação como a força motriz da sociedade e da economia. CASTELLS, Manuel. A sociedade em rede. Op. Cit.

[149] GAVISON, R., & MINTCHEV, V. (2022). Transnational Cybercrime: Rethinking Global Cooperation. Boston University International Law Journal, 40(1), 1-32.

[150] JÚNIOR, Paulo Abrão Pires. Op. Cit.

Sendo assim, neste novo cenário de intensificação das relações entre as nações, seja no âmbito comercial, migratório ou informacional, se faz necessário cada vez mais que os Estados sejam proativos e colaborativos. As relações jurídicas não se limitam mais a um único Estado soberano, pelo contrário, é necessário estabelecer cooperação e solicitar a colaboração de outros Estados para atender às demandas dos indivíduos e da sociedade[151].

Nas palavras Júnior, para cumprir essa missão de assegurar a justiça, é imperativo que o Estado formule estratégias capazes de impactar ativos e indivíduos que possivelmente não estejam mais em sua jurisdição territorial. Este posicionamento estende-se até a atividades processuais, que são essenciais para o devido trâmite legal e podem ser alcançadas através de colaboração internacional. Nesse sentido, a cooperação internacional emerge como um requisito fundamental para a concretização dos direitos básicos do cidadão na era contemporânea[152].

Nesse sentido, é fundamental compreender a importância da cooperação jurídica em matéria penal, a necessidade de legislações harmonizadas, a aplicação coordenada da lei nos desafios enfrentados pela persecução penal dos crimes cibernéticos. Além disso, será demonstrada a importância dos acordos bilaterais e multilaterais entre países, que facilitam a cooperação diante desse contexto complexo dos crimes cibernéticos [153].

Todos estes pontos se mostrarão essenciais para uma melhor compreensão da importância da cooperação penal internacional no enfrentamento aos crimes cibernéticos, sobretudo quando forem analisados com mais profundidade no Capítulo IV dessa pesquisa, sobre a adesão do Brasil à convenção de Budapeste e seus reflexos no cenário internacional.

2.1.1 Conceito de cooperação penal internacional

Desde a Antiguidade, é possível identificar manifestações do que hoje é conhecido como Direito Penal Internacional. No entanto, o pleno desenvolvimento desse campo jurídico ocorreu de maneira efetiva ao longo do século XX, sendo impulsionado principalmente pelos impactos das duas grandes guerras mundiais e, sobretudo, pela queda do muro de Berlim e o fim da guerra fria. O aumento significativo na produção de normas internacionais relacionadas ao Direito Penal, que resultou na criação de sistemas globais de proibição, como no caso da

[151] JÚNIOR, Paulo Abrão Pires. Op. Cit.

[152] *Ibidem*.

[153] ARAÚJO, A. L., & SILVA, M. R. (2021). Cibercrime no Brasil: Uma análise das práticas ilegais e suas complexidades no ambiente digital. Revista Brasileira de Segurança Cibernética, 8(2), 45-62.

lavagem de dinheiro e do financiamento do terrorismo, contribuiu para a crescente atenção dedicada a esse domínio legal[154].

De acordo com Conte, ao abordarmos a aplicação da legislação penal no âmbito espacial, estamos, na verdade, adentrando no campo do Direito Penal Internacional. Nesse sentido, trata-se de uma questão interna, uma vez que está vinculada ao direito nacional de cada Estado. Por outro lado, temos o Direito Internacional Penal, que lida com a justiça penal em um contexto supranacional, visando combater crimes que afetam bens considerados da humanidade ou universais, tais como genocídio, crimes de guerra, tráfico de mulheres, entre outros. Portanto, na visão da autora o Direito Penal Internacional compreende um conjunto de princípios e normas que regulam conflitos de leis no espaço, ou seja, abrange situações em que um crime afeta bens jurídicos de dois ou mais países [155].

Nas palavras de Japiassu, o Direito Penal Internacional é a vertente jurídica que delimita os crimes internacionais e estabelece as respectivas sanções. Além disso, regula questões relativas à extraterritorialidade da aplicação das leis penais nacionais, imunidade de indivíduos internacionalmente protegidos, cooperação penal internacional em todas as suas esferas, transferência de processos e pessoas presas ou condenadas entre nações, extradição, definição dos critérios e limites de cumprimento de penas estrangeiras, bem como a instauração e funcionamento de tribunais penais de alcance internacional ou regional. Ademais, abarca qualquer outra problemática criminal relacionada a indivíduos que possa emergir no âmbito internacional[156].

Desse modo, o Direito Penal Internacional não apenas lida com questões de crimes transnacionais, tradicionalmente pertencentes ao âmbito do Direito Penal interno, mas também se ocupa de assuntos relacionados à cooperação penal internacional, frequentemente estudados no contexto do Direito Processual Penal. Adicionalmente, é responsável por tratar da extradição, um procedimento essencialmente vinculado à cooperação penal internacional[157].

Sendo assim, a cooperação penal internacional pode ser entendida como o conjunto de mecanismos que propiciam interação de Estados na efetivação da justiça penal, em atenção a

---

[154] JAPIASSÚ, Carlos Eduardo A. O direito penal internacional e os crimes internacionais. Revista Interdisciplinar do Direito-Faculdade de Direito de Valença, v. 9, n. 1, p. 69-90, 2012.

[155] CONTE, Christiany Pegorari; SANTOS, Coriolano Aurélio de Almeida Camargo. Desafios do direito penal no mundo globalizado: a aplicação da lei penal no espaço e os crimes informáticos. 2012.

[156] JAPIASSÚ, Carlos Eduardo A. O direito penal internacional e os crimes internacionais. *Op. cit*.

[157] JAPIASSÚ, Carlos Eduardo A. O direito penal internacional e os crimes internacionais. *Op. cit*.

procedimentos ou processos específicos. São equivalentes os termos jurisdicional, judiciária ou jurídica, empregados para qualificar a cooperação penal internacional, distinguindo-a da cooperação administrativa[158].

Para Abade, a cooperação internacional penal no âmbito jurídico consiste em um conjunto de medidas e mecanismos pelos quais os órgãos competentes dos Estados solicitam e prestam auxílio mútuo para realizar, em seus respectivos territórios, atos pré-processuais ou processuais que sejam relevantes para a jurisdição estrangeira. O propósito subjacente é facilitar o acesso à justiça[159].

Já para Souza, a melhor terminologia utilizada para designar o instituto de cooperação penal internacional, nos diversos instrumentos normativos existentes, assim como na literatura especializada, não é uniforme, e baseia-se na compreensão mais ou menos abrangente de seu âmbito de aplicação e é sempre influenciada pela tradição jurídica de cada país[160].

Nas palavras de Bechara, a cooperação jurídica penal internacional pode ser conceituada como o conjunto de medidas que estabelecem as diretrizes para a interação entre dois ou mais Estados, ou até mesmo entre Estados e tribunais internacionais, com o objetivo de suprir as restrições territoriais impostas pela soberania. Essa necessidade surge em decorrência das limitações inerentes à autonomia estatal[161].

Segundo Bechara, a expressão cooperação jurídica internacional engloba outros termos sinônimos, tais como assistência, ajuda ou auxílio mútuo internacional. Essa abrangência vai além do intercâmbio entre órgãos judiciais, incluindo também a colaboração entre órgãos administrativos. Dessa forma, a cooperação jurídica internacional se estende a diversas esferas de atuação, promovendo uma interação harmoniosa e inteligente entre os diferentes setores envolvidos[162].

Cervini define a cooperação penal internacional podendo ser descrita como o conjunto de atividades processuais que vão além das formas simples, regulares e concretas, realizadas por órgãos jurisdicionais competentes em matéria penal, pertencentes a diferentes Estados

---

[158]ABADE, Denise Neves. Análise da Coexistência entre Carta Rogatória e auxílio direto na assistência jurídica internacional. Temas de cooperação internacional, p. 7, 2015

[159] ABADE. *Op. cit*. pg,07.

[160] SOUZA, Solange Mendes de. Cooperação jurídica penal no Mercosul: novas possibilidades. Rio de Janeiro: Renovar, 2001. p. 133.

[161] BECHARA, Fábio Ramazzini. *Op. Cit*, pg 31

[162] BECHARA, Fábio Ramazzini. *Op. Cit*, pg 31

soberanos. Essas atividades convergem de forma funcional e necessária em âmbito internacional, visando alcançar um mesmo objetivo, que é o desenvolvimento e execução de um processo penal de natureza similar. Tudo isso ocorre dentro de um estrito marco de garantias, de acordo com o grau e a projeção intrínseca da assistência solicitada[163].

Souza emprega a terminologia cooperação penal internacional como uma expressão mais precisa, uma vez que engloba não somente a cooperação entre autoridades judiciais, mas também a colaboração entre autoridades policiais ou administrativas[164]. Por sua vez, Grinover utiliza o termo abrangente "cooperação internacional em matéria penal" para englobar todas as formas de colaboração entre Estados nessa área, como extradição e execução de sentenças penais estrangeiras[165].

Para Nádia de Araújo a cooperação jurídica internacional, que é a terminologia mais consagrada, representa de forma ampla o intercâmbio internacional para o cumprimento extraterritorial de medidas solicitadas pelo poder judiciário de outro país. Isso ocorre devido à limitação territorial da jurisdição do poder judiciário, que é um atributo fundamental da soberania do Estado. Assim, quando as necessidades do poder judiciário ultrapassam as fronteiras nacionais, é necessário solicitar a assistência do poder judiciário de outro Estado. Vale ressaltar que, embora tradicionalmente também se incluísse o problema da competência internacional nessa matéria, para os fins deste capítulo, não abordaremos esse assunto. Atualmente, existem novas possibilidades de atuação administrativa do Estado nessa área, por meio de modalidades de contato direto entre os órgãos estatais[166].

De maneira semelhante, a convenção do conselho da Europa sobre o cibercrime adota o critério de empregar a expressão genérica "cooperação internacional" para se referir às diferentes formas de colaboração entre Estados mencionadas em seu texto, como extradição e auxílio mútuo em matéria penal[167].

---

[163] CERVINI, Raul; TAVARES, Juarez. Princípios da cooperação judicial penal internacional no protocolo Mercosul. São Paulo: RT, 2000, p. 51

[164] SOUZA, Solange Mendes de. *Op. Cit*, p. 3.

[165] GRINOVER, Ada Pellegrini. As garantias processuais na cooperação internacional em matéria penal. In: Revista Forense, vol. 373, ano 100, Rio de Janeiro: Forense, maio/jun. 2004. p. 4-5

[166] ARAUJO, Nádia. A importância da cooperação jurídica internacional para a atuação do estado brasileiro no plano interno e internacional. In: Manual De Cooperação Jurídica Internacional E Recuperação De Ativos. Cooperação em matéria penal. Brasília. Secretária Nacional de Justiça, 2008, pg. 40.

[167] Convention on Cybercrime. Budapest, 23.XI.2001. Disponível em:http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. Acesso em: 14 ago 2023.

No Brasil a cooperação internacional é verificada desde os primeiros artigos da Constituição Federal. O inciso IX do artigo 4º da Carta de 1988, onde estipula a cooperação entre as nações como um dos princípios fundamentais que orientam as relações internacionais do Brasil[168]. Ainda que a ênfase na cooperação internacional seja evidente no texto constitucional, a abordagem adotada pelo país é caracterizada pelo voluntarismo, o que implica que a efetivação da cooperação deve estar respaldada por acordos prévios entre as partes ou pelo compromisso de reciprocidade[169].

Nesse contexto o Direito Penal Internacional desempenha um papel fundamental na busca pela harmonização entre os diferentes ordenamentos jurídicos. Sua função é estabelecer os crimes internacionais e suas respectivas penas, bem como definir regras referentes à aplicação extraterritorial do Direito Penal interno. Além disso, o Direito Penal Internacional abrange questões como a imunidade de pessoas internacionalmente protegidas, a cooperação penal internacional em todos os níveis, as transferências internacionais de processos e de pessoas presas ou condenadas, a extradição e a determinação da forma e dos limites de execução de sentenças penais. Para lidar com essas questões, existem tribunais penais internacionais ou regionais que desempenham um papel crucial na resolução de problemas criminais relacionados a indivíduos que surgem no âmbito internacional[170].

Segundo apontamentos de Trota e Ferreira, houve um crescimento significativo na cooperação jurídica internacional em matéria penal nos últimos anos. Esse crescimento é explicado, principalmente pela elaboração de tratados internacionais, pela criação de organismos internos e pelo surgimento de mecanismos importantes para a efetivação das medidas solicitadas. Essas iniciativas têm como principal objetivo auxiliar mutuamente os Estados-Membros envolvidos, especialmente diante do aumento das manifestações delitivas que ultrapassam as fronteiras nacionais, como é o caso dos crimes transnacionais, como o tráfico internacional de entorpecentes, pessoas ou armas, evasão de divisas e lavagem de dinheiro e nos crimes cibernéticos. É importante ressaltar que, diante da capacidade humana inesgotável de conceber e cometer novos atos lesivos, a lei sempre está em desvantagem em relação ao potencial criativo do ser humano para perpetrar condutas ainda não previstas em lei,

[168] BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 02/06/2022.

[169] ABADE, Denise Neves. Direitos fundamentais na cooperação jurídica internacional: Extradição, assistência jurídica, execução de sentença estrangeira e transferência de presos. Versão digital [kindle]. São Paulo: Saraiva, 2013.

[170] JAPIASSU, Carlos Eduardo Adriano. O direito penal internacional. Belo Horizonte: Del rey. 2009, p. 4-5.

sendo a cooperação penal internacional uma importante ferramenta no auxílio dos Estados para o enfrentamento desse tipo de criminalidade[171].

2.1.2 Instrumentos de efetivação da cooperação jurídica internacional

No cumprimento de sua obrigação de assegurar a justiça, o Estado necessita elaborar estratégias que viabilizem o alcance de bens e indivíduos que possam não mais se encontrar sob sua jurisdição. Mesmo nos procedimentos de natureza processual, porém indispensáveis para o devido andamento do caso, podem ser adquiridos por meio de assistência externa, o que confere à colaboração jurídica internacional um requisito essencial para a concretização dos direitos fundamentais[172]

Existe uma gama de instrumentos específicos conforme a natureza da assistência requerida, podendo ocorrer situações em que mais de um desses instrumentos seja apropriado. dentre os instrumentos disponíveis, destacam-se a cooperação jurídica internacional estabelecida por meio dos mecanismos como as cartas rogatórias, a homologação de sentença estrangeira, os pedidos de extradição, a transferência de pessoas condenadas, e ainda, o auxílio direto[173].

O instituto da extradição é o mais antigo instrumento de cooperação internacional e pode ser considerado também o de natureza mais gravosa, por envolver diretamente a liberdade do indivíduo. Desde os tempos da Antiguidade no Oriente, as civilizações caldeias, egípcias e chinesas já efetuavam a entrega de indivíduos em fuga através de uma obrigação mútua imposta por rituais religiosos realizados em nome de suas divindades respectivas. No contexto Ocidental, o ato de entregar pessoas também estava presente nesse período, representando um pacto significativo que demandava respeito e cumprimento[174].

Para Weber, a extradição é caracterizada como um processo legal no qual um Estado cede um indivíduo, seja acusado ou já condenado por um crime, à jurisdição de outro Estado habilitado para o seu julgamento e penalização. Esse procedimento é fundamentado na premissa

[171] TROTTA, Sandro Brescovit; FERREIRA, Luciano Vaz. Cooperação jurídica internacional em matéria penal: contornos históricos. Sistema Penal & Violência, v. 5, n. 1, 2013.

[172] CONCI, Luiz Guilherme Arcaro. O controle de convencionalidade como parte de um constitucionalismo transnacional fundado na pessoa humana. Revista de Processo. Vol. 232/2014, Jun/2014, p. 363.

[173] PIRES JÚNIOR, Paulo Abrão. O papel da cooperação jurídica internacional. In: Manual de cooperação jurídica internacional e recuperação de ativos. Secretaria Nacional da Justiça. 2. ed. Brasília, 2012, p. 17.

[174] BRASILEIRO, Anaís Eulálio. A cooperação jurídica internacional no terrorismo. 2018. Dissertação de Mestrado. Brasil.

de que o delito foi perpetrado no território do Estado solicitante ou que o indivíduo em questão está sujeito às suas leis penais. A implementação da extradição requer uma condenação final que resulte em privação de liberdade ou a declaração de prisão por uma autoridade competente do Estado requerente. A estrutura legal da extradição é delineada nos artigos 76 a 94 da Lei nº 6.815/1980, que foram substancialmente modificados pela Lei nº 6.964/1981[175].

A carta rogatória, de acordo com Marco Antônio Marques da Silva, é um instrumento de comunicação utilizado pelas autoridades judiciárias estrangeiras para solicitar a realização de uma diligência essencial à instrução criminal, tanto no território brasileiro quanto no exterior[176]. Trata-se do método convencional empregado por um Estado soberano, por meio de sua jurisdição, para requerer atos processuais em outro território soberano, com o objetivo de obter e reunir evidências ou realizar qualquer outro ato de instrução processual. A solicitação é sempre emitida por uma autoridade judicial a outra autoridade equivalente de um país estrangeiro e tem como finalidade, por exemplo, a citação de réu ou investigado domiciliado no exterior (com endereço conhecido), depoimentos e notificações[177].

A homologação de sentenças provenientes de outros países são questões relacionadas à circulação internacional das decisões judiciais, cuja efetividade é de interesse para o adequado funcionamento do sistema internacional. A homologação de sentença estrangeira desempenha um papel fundamental no reconhecimento e na execução de decisões judiciais de autoridades estrangeiras no território do Estado requerido, promovendo a eficácia dessas decisões e o respeito aos direitos adquiridos no exterior[178]. As decisões oriundas da justiça estrangeira eram homologadas pelo STF até 2004, sendo analisadas agora STJ e só então terão qualquer efeito no território nacional[179].

Nas palavras de Abade esse instituto de homologação de sentenças estrangeiras, constitui-se de um mecanismo de cooperação jurídica internacional no qual um determinado Estado efetua, em seu território, a execução de uma sentença penal proveniente de outro Estado.

---

[175] WEBER, Patrícia Maria Núñez. Cooperação internacional penal: conceitos básicos. Temas de Cooperação Internacional: Coleção MPF Internacional, Brasília, v. 2, n. 2, p. 1-248, 2015. Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/temas-de-cooperacao-internacional-1a-edicao. Acesso em: 14 ago. 2023

[176] SILVA, Marco Antonio Marques da; FREITAS, Jayme Walmer de. Código de Processo Penal comentado. São Paulo: Saraiva, 2012, p. 990

[177] WEBER, Patrícia Maria Núñez. Op.Cit.

[178] ARAUJO, Nádia. Op. Cit, pg 44.

[179] ARAUJO, Nádia. Op. Cit, pg 45.

Essa modalidade de cooperação está fundamentada no reconhecimento, por parte dos Estados, da existência de obstáculos gerais relacionados à nacionalidade ou residência habitual do condenado, que impedem a sua entrega a outro Estado para o cumprimento da sentença condenatória. Com o intuito de evitar que tais obstáculos à extradição resultem em impunidade absoluta, os Estados aceitam a implementação nacional de uma sentença penal condenatória estrangeira. Além disso, há também motivos de ordem humanitária, uma vez que os condenados poderiam cumprir a pena em seu país de origem[180].

Com o aumento das relações globais e a propagação dos crimes transnacionais, tornou-se evidente que os métodos tradicionais de cooperação jurídica internacional eram inadequados ou ineficientes em certas situações. Diante dessas novas demandas, os Estados se viram obrigados a desenvolver mecanismos mais avançados que permitissem a cooperação jurídica, ao mesmo tempo em que garantiam agilidade e segurança. Assim surgiu o que é conhecido como pedido de auxílio direto. O auxílio direto, no contexto brasileiro, é a colaboração fornecida pela autoridade nacional em resposta a uma solicitação externa encaminhada por meio da autoridade central brasileira. Nesse sentido o pedido é concebido e avaliado como uma diligência originalmente sob responsabilidade da jurisdição nacional [181].

É importante observar que no Brasil, é responsabilidade do Ministério da Justiça e segurança pública, por meio do seu departamento de recuperação de ativos e cooperação jurídica internacional (denominado "DRCI"), exercer a função de autoridade central para o processamento de pedidos de cooperação jurídica internacional ativa e passiva, incluindo cartas rogatórias. Essas atribuições estão descritas no artigo 14º, IV, Anexo I do Decreto n. 9.662/2019, que aprova a estrutura regimental do ministério, e, consequentemente, regulamenta as leis nacionais e os acordos internacionais em vigor relacionados à cooperação jurídica em matéria Penal[182].

2.2 Cooperação penal internacional no contexto dos crimes cibernéticos

2.1.1 Soberania, Território, jurisdição e competência

No contexto contemporâneo marcado por uma sociedade interconectada, o ciberespaço

[180] ABADE, Denise Neves. Direitos fundamentais e cooperação jurídica internacional. Saraiva Educação SA, 2017.

[181] ARAUJO, Nádia de. Cooperação jurídica internacional no Superior Tribunal de Justiça: Comentários à Resolução n. 9/2005. Rio de Janeiro: Renovar, 2010, p. 94.

[182] BRASIL. Ministério da Justiça. Cartilha de Cooperação Jurídica Internacional em Matéria Penal. Op. Cit, pg21.

e a expansão da internet, o Estado é compelido a confrontar desafios inéditos no cenário de cooperação internacional em matéria Penal. Estes desafios são amplificados pela fluidez das fronteiras geográficas na prática criminosa e pelo crescimento acentuado da criminalidade de natureza transnacional. Inclusive, atos processuais que, à primeira vista, podem parecer menos significativos, são cruciais para a eficácia dos procedimentos judiciais e frequentemente requerem colaboração internacional. As autoridades encarregadas da persecução penal têm notado uma crescente necessidade de obter diligências e elementos probatórios fora de suas próprias jurisdições, visando esclarecer tanto a autoria quanto a materialidade de delitos que ultrapassam suas fronteiras legais[183].

No contexto da soberania estatal, a manutenção, proteção, fiscalização e monitoramento de limites territoriais, quer sejam terrestres ou marítimos, surgem como preocupações centrais para os países. Este zelo é motivado pela compreensão de que o território físico constitui um elemento indissociável da própria condição de Estado soberano. Contudo, é crucial reconhecer que essas medidas, frequentemente, mostram-se insuficientes para coibir a prática dos crimes cibernéticos, que frequentemente transcendem as fronteiras geográficas naturais. Tal cenário ressalta a complexidade intrínseca na governança e segurança territorial em uma era cada vez mais globalizada e interconectada[184].

Essa constatação se torna ainda mais evidente no contexto dos crimes cibernéticos que frequentemente envolvem infratores que podem estar dispersos em múltiplos Estados ou, ainda que localizados em uma única jurisdição, gerar impactos, seja diretamente ou indiretamente, em territórios distintos. Esta dinâmica gera à necessidade de os Estado envolvidos empreenderem esforços de cooperação nas medidas investigativas, persecutórias e judiciais, visando à aplicação mais efetiva e justa da lei[185].

De acordo com Pergorari, a globalização juntamente com o surgimento da criminalidade que ultrapassa fronteiras nacionais tem trazido novos questionamentos acerca do conceito tradicional de soberania estatal. Nesse sentido quando se fala em jurisdição, está-se fazendo referência, justamente ao poder de legislar e governar, à manifestação da soberania de um

---

[183]MINISTÉRIO DA JUSTIÇA. Manual de Cooperação Jurídica Internacional. Matéria Penal e Recuperação de Ativos, 4. ed. Brasília, 2019. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-protecao/lavagem-dedinheiro/institucional-2/publicacoes/manuais/cooperacao-juridica-internacional-em-materia-penal/manual-penalonline-final-2.pdf. Acesso em: 27 abr. 2023, p. 10

[184]*Ibidem.*

[185] MINISTÉRIO DA JUSTIÇA. Manual de Cooperação Jurídica Internacional. Matéria Penal e Recuperação de Ativos. Op. Cit.

Estado. Já a noção de competência, nesse cenário, serve para demarcar o alcance específico da autoridade exercida por cada entidade jurisdicional, estabelecendo assim um regime de colaboração e especialização dentro do corpo estatal.[186].

Desse modo, o conceito de território pode ser entendido como o espaço onde é reconhecida à aplicação de uma ordem jurídica estatal, sendo, portanto, um dos pilares essenciais do Estado, uma vez que representa o local onde sua soberania é exercida. Do ponto de vista geográfico, o território corresponde ao espaço físico delimitado por fronteiras.[187].

Em geral, a jurisdição refere-se à autoridade legal que um estado tem para fazer cumprir suas leis, e a competência refere-se ao escopo dessa autoridade, o que dificulta a integração com outros países de acordo com Guidi e Rezek:

> Nosso Direito é contido, como o são também nossas instituições e procedimentos; nossa maneira de endereçar a realidade com um comando legal está intrinsecamente ligada ao território. Estados dividem-se em suas fronteiras, jurisdições se pretendem universais, mas são limitadas por outras igualmente vocacionadas, a "comunidade" internacional, conglomerado de Estados e Organizações aferradas a suas soberanias, tem um largo caminho a percorrer até atingir a mesma integração mundial que a Internet nos deu em pouco mais de duas décadas[188].

Segundo Celso Ribeiro Bastos, ao abordar o assunto, nos esclarece que cada Estado possui sua própria ordem jurídica em vigor. Em outras palavras, nenhum país estrangeiro tem permissão para realizar atos coercitivos dentro do território nacional. Esse fenômeno é conhecido como impenetrabilidade da ordem jurídica estatal. Portanto, o território desempenha um papel crucial na configuração do Estado, pois é uma porção de terra na qual apenas o poder do Estado é reconhecido e permite que ele seja soberano[189].

Ryngaert e Zoetekouw enfatizam que os princípios que regem os limites territoriais não surgiram isoladamente e não têm uma origem inata. Pelo contrário, eles emergiram a partir de noções materiais, políticas e epistemológicas que foram evoluindo desde o século XIV. Contudo, a expansão das fronteiras por meio dos avanços tecnológicos tem contribuído para o

---

[186] CONTE, Christiany Pegorari. Jurisdição e competência nos crimes informáticos. Revista Brasileira de Meio Ambiente Digital e Sociedade da Informação, v. 1, 2014, p. 13.

[187] CONTE, Op. Cit. p. 49.

[188] GUIDI, Guilherme Berti de Campos; REZEK. Op. Cit. p.276-288, p. 278.

[189] BASTOS, Celso Ribeiro. Curso de Teoria do Estado e Ciência Política. São Paulo: Saraiva: 1999, p.58.

aumento e progresso dos crimes cibernéticos, evidenciando assim novos conceitos de territorialidade e soberania[190].

No Brasil a aplicação da lei penal nacional dentro dos limites do território é uma questão de exercício da soberania estatal, constituindo-se está, portanto, a regra. Nesse sentido, a lei penal é aplicada dentro do território que a promulgou. No entanto, em situações excepcionais, é permitida a aplicação de legislação estrangeira, desde que estabelecida por algum tratado ou convenção internacional. Essa possibilidade de aplicação de leis estrangeiras modifica o princípio da territorialidade, tornando-o uma territorialidade temperada. O artigo 5º do Código Penal estabelece que a lei brasileira é aplicada aos crimes cometidos no território nacional, sem prejuízo de convenções, tratados e regras de Direito Internacional.[191]

Segundo Hungria, em relação a esse tema, o código penal estabeleceu uma resistência à inacessibilidade do direito interno ou à supremacia exclusiva da ordem jurídica do Estado sobre seu território, possibilitando e reconhecendo, em certos casos, a validade da legislação de outro Estado. Isso ocorre em prol de uma convivência internacional harmoniosa e, na maioria das vezes, mediante a condição de reciprocidade, permitindo que o território de um Estado seja acessível pelo exercício de uma soberania estrangeira[192].

No ordenamento jurídico brasileiro, a competência também está fundamentada na Constituição Federal, no artigo 109º, inciso IV[193], que estabelece a competência dos juízes federais em relação à matéria, ou seja, à natureza dos delitos cometidos. Ele determina que os crimes políticos e as infrações penais praticadas em prejuízo dos interesses da União, de suas entidades autárquicas ou empresas públicas (exceto as contravenções), são de competência exclusiva da justiça federal. No entanto, é importante ressaltar que a justiça militar e a justiça eleitoral possuem competências específicas, que não são abrangidas por essa regra[194].

Se o sistema computacional estiver localizado no Brasil, a competência será do juízo deste local. No entanto, se o comando partir de um sistema computacional brasileiro e resultar

---

[190] GUIDI, Guilherme Berti de Campos; Op. Cit. p.276-288, p. 278.

[191] CONTE, Christiany Pegorari. Jurisdição e competência nos crimes informáticos. Op. Cit. Pg 18.

[192] HUNGRIA, Nelson. Comentários ao Código Penal. 4º ed. Rio de Janeiro: Forense, 1958, Vol. 1. Tomo I, p. 149.

[193] BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 de ago de 2023.

[194] BRASIL. Constituição da República Federativa do Brasil. Op. Cit.

em acesso não autorizado a computadores em outro país, a competência será determinada pelo juízo do local onde o comando foi dado. Isso está de acordo com o disposto no parágrafo um do artigo 70º do Código De Processo Penal, que estabelece que, se a execução do crime começar no território nacional e se confirmar fora dele, a competência será determinada pelo lugar onde o último ato da execução foi praticado no Brasil[195]. A competência nos casos de tentativa será fixada no mesmo sentido quando, mesmo tendo sido dado o comando no território brasileiro, não se consumar no estrangeiro por motivos alheios à vontade do agente. Nesse caso, a competência também será do juízo do local em que foi praticado o último ato de execução, conforme estabelecido no caput do artigo 70º do código de processo penal[196].

No entanto, se o delito for um atentado em um país estrangeiro e seus resultados forem produzidos no Brasil, deve-se aplicar o disposto no segundo parágrafo do mesmo artigo do diploma legal. Esse parágrafo estabelece que, quando o último ato de execução for praticado fora do território nacional, será competente o juiz do lugar do crime, mesmo que parcialmente tenha produzido ou deveria produzir resultados. Nesses casos, a competência será do juízo onde estiver localizado o sistema computacional ameaçado pela tentativa proveniente de países estrangeiros[197].

Em suma, com o surgimento da internet e, consequentemente, do ciberespaço, houve uma transformação na concepção tradicional de soberania, território e competência. Isso se deve ao fato de que a internet possibilitou a rápida e eficiente circulação de informações, bem como a interação em um espaço que não reconhece as fronteiras físicas. Na rede, não há distinção de localização. O conceito de lugar passa a ser qualquer ponto de acesso à informação na rede[198].

O ciberespaço permite escapar das limitações do mundo real. O conceito de território está agora intimamente ligado à ideia de rede. A rede, assim como um território, é caracterizada pela localização da informação. Portanto, a informação na rede se torna um elemento identificador do território no ciberespaço. Essas características tornam a internet mais desafiadora para estabelecer um "centro de comando" como na versão tradicional de um território físico delimitado[199].

---

[195] VIANA, Túlio Lima. Op. Cit, pg 104.

[196] BRASIL. Decreto-Lei 2.848 de 7 de dezembro de 1940. Código Penal.

[197] VIANA, Túlio Lima. Op. Cit, pg 105.

[198] CONTE, Op. Cit. p. 49.

[199] CONTE, Op. Cit. p. 50.

Além da dificuldade em identificar um território no âmbito do ciberespaço, surge outra questão problemática: um indivíduo pode estar simultaneamente em diversos espaços utilizando a internet. Isso significa que uma pessoa pode possuir uma identidade no mundo físico e várias identidades distintas na internet, o que, em última análise, pode resultar em conflitos de competência entre os Estados e dificuldades na localização do próprio agente do crime.[200]

Dessa maneira, a principal problemática acerca da territorialidade nos casos de crimes cibernéticos surge quando um indivíduo pode se encontrar no Chile e realizar uma invasão no sistema de uma empresa sediada no Canadá, por meio de um provedor brasileiro, resultando em danos ocorrendo no Japão. Nesse contexto, surge a questão sobre a jurisdição do crime e qual Estado seria competente para processar e julgar o infrator. Caso um país não criminalize determinada atividade cibernética prejudicial, o país afetado pode utilizar o poder coercitivo de sua legislação para deter um indivíduo que esteja além dos limites de sua soberania[201].

Para Valin, o grande desafio ao lidar com o conceito de jurisdição e territorialidade na internet reside na natureza internacional da rede. No ambiente digital, não há fronteiras e, portanto, qualquer conteúdo publicado nela está disponível em todo o mundo. Dessa forma, surge a questão de como determinar a autoridade competente para analisar um caso relacionado a um crime ocorrido na rede[202].

Para Pegorari, é importante ressaltar que, apesar da natureza global do ciberespaço, cada nação possui sua própria soberania, embora essa soberania tenha sido relativizada nos últimos anos com o surgimento dos crimes cibernéticos. Além disso, embora haja uma corrente contemporânea que busca mitigar a soberania nacional em favor de uma soberania internacional, visando uma participação comunitária dos Estados na resolução de problemas globais por meio de acordos internacionais, especialmente impulsionados pela globalização, é importante destacar que esses acordos ainda são ineficazes quando se trata da aplicação efetiva do Direito Penal, uma vez que são subsidiários em relação à jurisdição interna dos países. Portanto, estamos diante de um desafio complexo que requer uma análise mais aprofundada por parte dos estudiosos do Direito e a comunidade jurídica internacional[203].

---

[200] CONTE, Op. Cit. p. 50.

[201] *Ibidem*

[202] VALIN, Celso. A questão da jurisdição e da territorialidade nos crimes praticados pela Internet. In Direito, sociedade e informática: limites e perspectivas da vida digital. Florianópolis: Fundação Boiteux, 2000, p. 115

[203] CONTE, Op. Cit. p. 49.

2.2.2 Natureza Transnacional dos crimes cibernéticos

A transnacionalidade, sem dúvida, é a característica preeminente dos crimes cibernéticos. Barreiras como a distância, as fronteiras de controle ou até mesmo a exigência de presença física do agente perdem a relevância diante das operações conduzidas pelas redes internacionais de transmissão de dados informáticos, com destaque para a Internet[204].

Ao abordar a questão dos crimes cibernéticos, torna-se evidente que soluções efetivas não podem ser articuladas apenas em âmbito nacional, uma vez que esse fenômeno está intrinsecamente ligado à sociedade em rede, impulsionado pela presença da internet. A ampla mobilidade de dados e sua livre circulação por meio de sistemas informáticos e redes de telecomunicações permitem que atividades ilícitas dessa natureza sejam praticadas à distância. O cibercrime é caracterizado principalmente pela interdependência de ações, uma vez que, em muitos casos, os atos executórios são realizados em um determinado país, enquanto os resultados são produzidos em outro, sujeito a diferentes ordenamentos jurídicos, ultrapassando, assim, as fronteiras nacionais[205].

Conforme apontado por Bednar, Katos e Hennel, a natureza global dos crimes cibernéticos intensificou a demanda por investigadores engajados em uma comunicação complexa entre grupos e em uma base multinacional. Tanto os investigadores quanto os próprios criminosos se beneficiam dessas tecnologias interconectadas. Além disso, a necessidade de navegar entre diferentes sistemas judiciais ao redor do mundo cria um ambiente desafiador para a persecução penal desses crimes[206].

Dada a complexidade da questão e a natureza global dos crimes cibernéticos, a existência de diversas leis nacionais destinadas a prevenir tais crimes poderia potencialmente levar à criação de paraísos criminosos, locais onde os prestadores de serviços possam estabelecer-se e beneficiar de uma legislação branda que não pune adequadamente os crimes cibernéticos. Essa analogia remete aos conhecidos paraísos fiscais, nos quais empresas internacionais buscam reduzir seus custos por meio de benefícios fiscais e tributários. A

[204] APPADURAI, A. (1996). Modernidade em Dispersão: Ensaios sobre as Artes e a Identidade Global. Editora UFMG.

[205] BEDNAR, P.M.; KATOS, V.; HENNEL, C. Cyber-Crime Investigations: Complex Collaborative Decision Making. In: Third International Annual Workshop on Digital Forensics and Incident Analysis. WDFIA 2008. Malaga, Spain. 9 p. Disponível em : https://lucris.lub.lu.se/ws/files/5676843/5045156.pdf

[206] BEDNAR, P.M.; KATOS, V.; HENNEL. Op. Cit.

existência de leis nacionais divergentes no combate aos delitos informáticos poderia, portanto, fomentar a criação desses paraísos criminais[207].

Cabe ressaltar que os crimes cibernéticos são um fenômeno que se manifestam de maneira semelhante em todos os países, especialmente devido às facilidades proporcionadas pelos avanços tecnológicos, em especial a internet. Essas facilidades permitem que uma conduta criminosa se origine em um país e se espalhe para outros, o que justifica a denominação de criminalidade transnacional para os delitos cometidos em ambiente virtual.

Diante desse contexto, o futuro do Direito Penal requer, no mínimo, uma maior colaboração entre os Estados para uma investigação e punição eficazes dos delitos transfronteiriços. Apesar das diferenças nas leis penais de cada país, é essencial estabelecer uma cooperação mais estreita entre as nações para enfrentar esse desafio[208].

A característica transnacional dos crimes informáticos é uma realidade inegável e desafiadora. A natureza globalizada da internet e a facilidade de comunicação e troca de informações entre diferentes países e regiões criam um ambiente propício para a prática desses delitos além das fronteiras nacionais. A existência de leis nacionais divergentes e a falta de cooperação internacional efetiva podem resultar na criação de paraísos criminais, onde os criminosos se beneficiam de legislações mais brandas ou da falta de regulamentação adequada.

Diante desse cenário, a necessidade de instrumentos internacionais de assistência mútua e de harmonização das legislações se torna cada vez mais premente. A convenção de Budapeste, como um exemplo de tratado internacional, busca justamente promover a cooperação entre os países e a uniformização das leis para enfrentar de forma mais eficaz os desafios transnacionais dos crimes cibernéticos. No próximo capítulo, exploraremos as principais medidas e estratégias adotadas para combater essa nova forma de criminalidade que cresce de forma exponencial e requerer cada vez mais ajuda mútua dos estados internacionais para seu enfrentamento.

2.2.3 Desafios na persecução penal

Para Tavora, o processo de persecução criminal, encarregado de apurar infrações penais e identificar os respectivos autores, é estruturado em duas fases distintas e bem articuladas. A etapa inicial, de caráter inquisitivo, é conhecida como inquérito policial. A subsequente, caracterizada pela observância do princípio do contraditório e da garantia de ampla defesa, é

[207] BOITEUX, L. Crimes Informáticos: reflexões sobre política criminal inseridas no contexto internacional atual. Revista Brasileira de Ciências Criminais, São Paulo, n. 47. RT, 2004 pg 202.

[208] CONTE. Op. Cit. Pg 06.

designada como fase processual[209].

Uma vez que um suposto ato delituoso desencadeia o dever estatal de punir, o Estado tem, como norma, a responsabilidade de iniciar a persecução criminal com o objetivo de investigar, processar e, por fim, exercer seu direito de punir, resolvendo conflitos e aplicando a lei ao caso específico. Em síntese, a persecução penal compreende duas fases interdependentes: (1) a investigação preliminar, da qual o inquérito policial é uma modalidade específica, destinada à construção de um conjunto mínimo de provas que viabilize a iniciação da fase subsequente; e (2) o processo penal, instaurado mediante a apresentação de uma ação penal perante o judiciário[210].

Nesse sentido a investigação de crimes cibernéticos apresenta desafios intrínsecos devido a várias razões. Inicialmente, muitas vítimas podem estar alheias à ocorrência do delito, enquanto outras, particularmente no âmbito empresarial, podem optar por não denunciar a infração para preservar sua imagem pública e a confiança de seus clientes. Além disso, a anonimidade dos perpetradores e a complexidade em rastreá-los amplificam as barreiras à efetivação da justiça[211].

Mesmo quando localizado o dispositivo de origem do ataque, a responsabilidade pode ser contestada pelo proprietário do equipamento. Adicionalmente, a sofisticação tecnológica, como o uso de criptografia, complica ainda mais a coleta de provas[212]. Outros desafios encontrados na investigação dos crimes cibernéticos são os resultados diretos do nosso sistema jurídico, uma vez que a imposição de sanções penais só é possível quando há certeza da prática do crime. É essencial comprovar tanto a autoria quanto a materialidade do delito, além da existência de indícios sólidos de que o indivíduo em questão cometeu o crime. Caso não sejam comprovados a materialidade e a autoria, o juiz tem deverá absolver o réu[213].

Nesse contexto, a persecução penal pode se fragmentar em diversos pontos, abrangendo diversos países. Um exemplo é um simples e-mail contendo conteúdo ofensivo ou pornografia

---

[209] TÁVORA, Nestor; ROCHA JR, Francisco Monteiro; PACHECO FILHO, Vilmar Velho**.** Direito Processual Penal. IESDE BRASIL SA, 2012, pg27.

[210] *Ibidem*.

[211] HERMAN, Susan N. et al. Os desafios do crime cibernético. Revista Eletrônica de Direito Penal e Política Criminal, v. 1, n. 1, p. 47-56, 2013.

[212] *Ibidem.*

[213] DOMINGOS, Fernanda Teixeira Souza; RODER, Priscila Costa Shreiner. Obtenção de provas digitais e jurisdição na internet. São Paulo: EMAG, 2017, pg 62.

infantil, que pode percorrer diversos servidores localizados em países distintos antes de atingir seu destino. Da mesma forma, um vírus de computador disseminado pela internet pode afetar inúmeros sistemas informáticos ao redor do globo. Assim nos procedimentos de investigação criminal conduzidos por um Estado afetado, pode surgir a necessidade de obter evidências na forma de dados armazenados em sistemas informáticos situados no exterior[214].

No entanto, as atividades das instâncias judiciais e policiais de cada nação possuem limites jurisdicionais que dificultam na persecução penal. Isso acarreta problemas específicos tanto no âmbito factual quanto no jurídico, sempre que se requer a execução de atos investigativos ou diligências para a obtenção de provas em redes de computadores globais especialmente a internet. Isso ocorre porque a autoridade policial e judicial encontra sua jurisdição delimitada pelas fronteiras do Estado em que atua, e qualquer intervenção para além desses limites é rejeitada devido à necessidade de respeito ao princípio de soberania territorial dos Estados. O acesso direto na rede e a coleta de dados em sistemas informáticos de outros países pode ser interpretado como uma violação da soberania territorial do país em que os dados estão armazenados, visto que infringe a prerrogativa exclusiva das autoridades locais de conduzir investigações em seu próprio território[215].

Manter limites rígidos e intransigentes pode acarretar dificuldade de localizar suspeitos ou estabelecer sua culpabilidade em relação a atos criminosos. A natureza inflexível dos elementos essenciais desses princípios pode contribuir para a violação de dois valores fundamentais no âmbito do Direito Penal Internacional: a busca pela justiça universal, através da eliminação da impunidade; e o reconhecimento dos valores da ordem comunitária internacional. Essa rigidez pode até mesmo desencorajar os Estados a se engajarem em cooperação, onde agilidade e rapidez são essenciais para desfecho como nos casos dos crimes cibernéticos [216] .

Nesse sentido, apesar da internet aparentar ser uma rede intangível, seu funcionamento está intrinsecamente ligado à existência de uma infraestrutura física. Para que um usuário possa se conectar, é necessário contar com diversos provedores de conexão de rede, os quais atribuem

[214] DOMINGOS , Fernanda Teixeira Souza; RODER, Priscila Costa Shreiner. Op. Cit pg 61

[215] DOMINGOS, Fernanda Teixeira Souza; RODER, Priscila Costa Shreiner. Op. Cit pg 62

[216] ALLE, Saulo Stefanone. Cooperação jurídica internacional e auxílio direto ativo em matéria penal. Belo Horizonte: Arraes Editores, 2017. 189 p. P. 110. *E-book kindle.*

ao usuário um número de IP (*Internet Protocol*)[217], utilizado para acessar o ambiente virtual. O acesso ao conteúdo disponível nessa plataforma, como serviços de *e-mail*, redes sociais e outras formas de comunicação *online*, depende justamente dessa estrutura fornecida pelos provedores, os quais passam a armazenar informações sobre as atividades dos usuários na rede, como histórico de navegação, postagens e comunicações[218].

As empresas provedoras de internet possuem informações que são essenciais para desvendar um crime cibernético ou obter provas relacionadas a um crime no mundo físico. Isso tem levado os usuários e o poder judiciário a fazerem diversos pedidos para que essas informações sejam disponibilizadas durante uma investigação criminal. No entanto, surge a dificuldade de determinar qual local teria jurisdição para decidir sobre o fornecimento dessas informações, uma vez que as empresas podem ter sede física em um país, mas armazenar seus dados em qualquer lugar do mundo[219].

Além disso, cada sistema jurídico tem sua própria visão sobre a proteção da privacidade, o que resulta em diferenças legislativas em relação aos requisitos para o fornecimento legal de dados e informações dos usuários. Adicionalmente, a prova no meio digital é volátil, devido à enorme quantidade de conteúdo transmitido pela internet, o que faz com que os provedores tenham o mínimo de armazenamento possível, devido aos altos custos envolvidos[220].

Segundo La Chapelle e Fehlinger, existem quatro critérios fundamentais para determinar a lei aplicável na obtenção de dados digitais. Além do local onde o usuário está e onde os servidores que armazenam os dados estão localizados, também devemos considerar a lei do país onde a empresa que presta o serviço está incorporada e a lei do país onde os registros foram feitos. No entanto, todas as possíveis soluções apresentam obstáculos e podem entrar em conflito com as regras de aplicação da lei penal em cada sistema jurídico[221].

A primeira opção, que exigiria que os provedores de internet fornecessem informações de acordo com a lei do país onde o usuário está, pode se deparar com uma situação complexa.

---

[217] Endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais. MARCEL Leonardi. Op. Cit. Pg 19.

[218] DOMINGOS, Fernanda Teixeira Souza; RODER, Priscila Costa Shreiner. Op. Cit pg 63.

[219] DE ARAÚJO ALVES, Matheus. Op. Cit, pg 23.

[220] DOMINGOS, Fernanda Teixeira Souza; RODER, Priscila Costa Shreiner.Op. Cit,pg 63.

[221] LA CHAPELLE, Bertrand; FEHLINGER, Paul. Jurisdiction on the internet: from legal Arms race to to transnational cooperation. Internet & jurisdiction. Paper series, n 28, April 2016. Disponível em: www.internetjurisdiction.net. Acesso em 14 ago 2023.

Por exemplo, se um usuário estiver em um determinado país cometendo uma infração pela internet e produzindo um resultado típico no país que precisa dos seus dados para investigação, mas estiver usando um provedor de internet sediado em um terceiro país[222].

O segundo critério que pretende utilizar as leis locais onde estão os servidores que armazenam os dados tem gerado diversas discussões entre os provedores de internet. Eles alegam a necessidade de cumprir as leis de proteção de dados e privacidade. Essa questão tem sido uma difícil tarefa para os operadores do direito, que precisam da prova digital. Isso ocorre devido à possibilidade de as informações estarem duplicadas em vários servidores simultaneamente, ou até mesmo fragmentadas. Essa dispersão dos dados torna inviável estabelecer precisamente o local em que determinado dado, imprescindível para uma investigação criminal, está armazenado[223].

A terceira opção, que aborda o uso da legislação da região onde a empresa foi incorporada, enfrenta obstáculos quando o local de prestação de serviços difere daquele de incorporação. Isso ocorre porque leis estrangeiras estariam sendo aplicadas no território nacional, o que acarreta consequências semelhantes à adoção da quarta opção. Esta última envolve a aplicação da legislação do país de origem do registrador, resultando também em implicações estrangeiras que afetam o território nacional[224].

Nas palavras de Damásio e Milagres, com o avanço tecnológico e a interconexão global proporcionada pela internet uma série de condutas delitivas que transcendem fronteiras nacionais surgem todos os dias, e a tradicional noção de territorialidade tem se tornado confusa pela natureza virtual das infrações cometidas por meio de sistemas informáticos e redes de telecomunicação. Os autores afirmam que diante da possibilidade de um mesmo ato criminoso ser cometido em um país, enquanto seus efeitos reverberam em vários outros simultaneamente tornando a aplicação da lei penal complexa em virtude das diferentes jurisdições existentes, bem como da dificuldade de estabelecer qual lei deve ser aplicada em situações que envolvem múltiplos locais para o mesmo fato criminoso, gerando uma complexidade na persecução penal quando se trata de crimes cometidos no ambiente virtual[225].

---

[222] DOMINGOS, Fernanda Teixeira; RODER, Priscila Costa Shreiner.Op. Cit,pg 65.

[223] DOMINGOS, Fernanda Teixeira; RODER, Priscila Costa Shreiner.Op. Cit,pg 66.

[224] DOMINGOS, Fernanda Teixeira; RODER, Priscila Costa Shreiner.Op. Cit,pg 66.

[225] JESUS, Damásio Evangelista de; MILAGRE, José Antônio. Op. Cit, p. 71.

2.3 Principais tratados e convenções internacionais relacionados aos crimes cibernéticos

Considerando que a justiça de cada país não possui alcance global, a colaboração por meio de acordos e tratados internacionais é fundamental para enfrentar situações em que crimes permanecem impunes devido a característica transnacional das infrações, resultando em uma sensação de incapacidade[226]. A compreensão dessas limitações envolve a criação de mecanismos que permitam a um Estado superar suas limitações no exterior, isto é, além das vias convencionais de cooperação internacional, que também são analisadas neste estudo. Após essa consideração, é relevante dar destaque à abordagem consensual proporcionada pelos tratados internacionais de assistência judicial mútua, os quais desempenham um papel significativo no cenário atual ao facilitar e padronizar a colaboração entre diferentes jurisdições para fins de comunicação e orientação judiciária[227].

No contexto das convenções e tratados internacionais que em que o tema crimes cibernéticos já vem sendo objeto de debates, merecem destaque o Protocolo de assistência jurídica mútua em assuntos penais do Mercosul, a Convenção Interamericana sobre assistência mútua em matéria penal (Convenção da OEA) e, de forma mais significativa, a Convenção sobre Cibercrime, também conhecida como Convenção de Budapeste, que será minuciosamente abordada no capítulo VI desta pesquisa.

O Protocolo de assistência jurídica mútua em assuntos penais do Mercosul, firmado na cidade argentina de São Luís em 13/6/1996, aprovado pelo conselho do mercado comum (Decisão 02/96) e promulgado no Brasil por meio do Decreto 3.468, de 17/5/2000, tem como objetivo principal a integração econômica e jurídica dos Estados-Partes do Mercosul, em conformidade com o tratado de Assunção. Esse protocolo foi elaborado com o intuito de harmonizar a legislação dos países membros do bloco econômico, visando alcançar os objetivos comuns estabelecidos. Com foco nas atividades criminosas de natureza transnacional, a cooperação jurídica em matéria penal é considerada fundamental para aprofundar os interesses mútuos dos Estados-Partes no processo de integração[228].

O documento em questão tem como objetivo principal a eliminação das barreiras burocráticas decorrentes das prerrogativas soberanas, visando estabelecer um mecanismo de

---

[226] GUIDI, Guilherme Berti de Campos; REZEK, Op. Cit. p.276-288, p. 279.

[227] JESUS, Damásio Evangelista de; MILAGRE, José Antônio. Op. Cit, p. 55.

[228] TROTTA, Sandro Brescovit; FERREIRA, Luciano Vaz. Op. Cit. pg 12.

cooperação penal direta no âmbito do Mercosul, reconhecendo que diversas atividades criminosas representam uma séria ameaça e se manifestam por meio de modalidades transnacionais, nas quais as evidências frequentemente estão localizadas em diferentes Estados[229].

A convenção Interamericana sobre assistência mútua em matéria penal (convenção da OEA), firmada durante a assembleia geral da OEA em maio de 1992, em Nassau, nas Bahamas, e promulgada no Brasil pelo Decreto nº 6.340/08, os Estados americanos, incluindo os componentes do Mercosul, com exceção do Uruguai, têm como propósito essencial buscar a solução de problemas políticos, jurídicos e econômicos que possam surgir entre eles. A convenção estabelece a obrigação dos Estados-Partes de prestar assistência mútua em matéria penal, abrangendo investigações, processos e procedimentos referentes a delitos de competência do Estado requerente no momento da solicitação. No entanto, o Estado-Parte não possui a faculdade de exercer jurisdição ou desempenhar funções reservadas às autoridades do outro Estado-Parte, de acordo com sua legislação interna. Além disso, os particulares não têm o direito de obter ou excluir provas, nem de impedir o cumprimento de pedidos de assistência (Convenção Interamericana sobre Assistência Mútua em Matéria Penal, art. 1º e 2º)[230].

Outro importante Acordo de Assistência Judiciária em Matéria Penal é entre o Brasil e os Estados Unidos da América, chamado de MLAT, que é um instrumento cooperativo, e sua função no contexto da relação entre dois Estados é padronizar procedimentos e reduzir embaraços ao trânsito internacional de pessoas, bens, provas no contexto de investigações e procedimentos criminais.[231]O Acordo firmado em 14 de outubro de 1997, que entrou em vigor em 2001, possui como principal objetivo facilitar a execução das tarefas das autoridades responsáveis pelo cumprimento da lei em ambos os países, abrangendo áreas como investigação, inquérito, ação penal e prevenção do crime, por meio da cooperação e assistência judiciária mútua[232].

Ainda nesse contexto de ajuda mútua entre estados, outras organizações, como o

---

[229] TROTTA, Sandro Brescovit; FERREIRA, Luciano Vaz. Op. Cit. pg 12.

[230] TROTTA, Sandro Brescovit; FERREIRA, Luciano Vaz. Op. Cit. pg 12.

[231] GUIDI, Guilherme Berti de Campos; REZEK, Francisco. Op. Cit. p. 284.

[232] BRASIL. Decreto N° 3.810, de 2 de maio de 2001, Acordo de Assistência Judiciária em Matéria Penal entre Brasil e Estados Unidos. Disponível em http://www.planalto.gov.br/ccivil_03/decreto/2001/D3810.htm Acesso em: 28/05/2021

Conselho da Europa[233], a Interpol[234], a OCDE[235] e o G8[236], sempre demonstraram certa preocupação com o aumento dos casos de crimes cibernéticos. Essas entidades sempre reconheceram a necessidade de uma abordagem global e coordenada para combater efetivamente essa nova forma de criminalidade. Através de iniciativas conjuntas, como a troca de informações, o desenvolvimento de diretrizes e a promoção da cooperação internacional, essas organizações sempre buscaram fortalecer as capacidades dos países membros no combate aos crimes cibernéticos e na proteção da segurança no ambiente virtual. Além disso, desempenham um papel importante na sensibilização e conscientização sobre os riscos e impactos dos crimes cibernéticos no mundo, incentivando a adoção de medidas preventivas e aprimorando a legislação e as políticas relacionadas a esse tema[237].

Em suma, a análise realizada neste capítulo evidencia a importância dos tratados e convenções internacionais no contexto penal dos crimes cibernéticos. A natureza transnacional dessas condutas delitivas exige uma abordagem global e coordenada para enfrentar os desafios que surgem nesse cenário. Os tratados e convenções internacionais desempenham um papel fundamental ao estabelecerem normas e diretrizes comuns, promovendo a cooperação entre os Estados e facilitando a persecução penal efetiva desses crimes. Além disso, esses instrumentos internacionais contribuem para a harmonização das legislações nacionais, preenchendo lacunas e garantindo uma resposta adequada diante das constantes evoluções tecnológicas. Através da cooperação internacional e do fortalecimento dos mecanismos de assistência mútua, é possível enfrentar de forma mais eficaz os desafios impostos pelos crimes cibernéticos.

---

[233]VERONESE, Alexandre. Cooperação jurídica e proteção de dados pessoais – A necessidade de inserção do Brasil nos tratos do Conselho da Europa. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/judiciario-e-sociedade/cooperacao-juridica-e-protecao-de-dados-pessoais-12042019

[234]FREITAS, Sérgio Henrique; Reis, Cristianne, et.al. A INTERPOL E O COMBATE AOS CRIMES TRANSNACIONAIS. Disponível em: https://www.defesa.gov.br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/XV_cadn/a_interpol_e_o_combate_aos_crimes_transnacionais.pdf

[235]BRASIL, Ministério da Economia. Organização para a Cooperação e Desenvolvimento Econômico – OCDE. Disponível em: http://www.fazenda.gov.br/assuntos/atuacao-internacional/cooperacao-internacional/ocde

[236]NASCIMENTO, Samir de Paula. Cibercrime: Conceitos, modalidades e aspectos jurídico-penais. Revista Âmbito Jurídico, 3 set. 2019. Internet e Informática. Disponível em: https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime

[237] NASCIMENTO, Samir de Paula. Op. Cit.

3 LEGISLAÇÃO PENAL BRASILEIRA E OS CRIMES CIBERNETICOS

3.1 Análise da legislação pertinente

A Constituição Federal Brasileira de 1988 estabelece princípios constitucionais fundamentais que regem o sistema jurídico do país. Dentre esses princípios, destacam-se a reserva legal e a legalidade, os quais são fundamentados no artigo 5º. Esses princípios foram estabelecidos pelo legislador com o objetivo de determinar que condutas que não estejam expressamente previstas em lei e aquelas que não tenham sido formuladas em conformidade com o devido processo legislativo não pode ser considerado como crimes[238].

Para Silva, o princípio da legalidade ou reserva legal é caracterizado como um limite tanto ao poder punitivo quanto ao poder normativo do Estado, uma vez que impede a criação de tipos penais. Segundo o autor, esse princípio é uma "consequência direta do fundamento da dignidade da pessoa humana, pois remonta à ideia de proteção e desenvolvimento da pessoa que o tem como referencial[239]. Essa previsão é confirmada pelo Código Penal Brasileiro em seu artigo 1º, que estabelece que "Não há crime sem lei anterior que o defina e não há pena sem prévia cominação legal"[240].

Nesse sentido, a ausência de previsão legal para uma conduta que cause danos a terceiros, mesmo que moralmente reprováveis, não configura crime no Brasil, uma vez que o sistema adotado é o da reserva legal[241]. Portanto, sem uma lei prévia que defina uma determinada conduta como crime, não é possível impor punição uma clara aplicação do princípio da legalidade. No âmbito da legislação sobre crimes cibernéticos, Jesus e Milagre propõem uma sistematização relevante a ser considerada. Essa sistematização, denominada

---

[238] BRASIL, Constituição Federal, 1988. Op. Cit.

[239] SILVA, Marco Antônio Marques da Silva. Acesso à Justiça Penal e Estado Democrático de Direito. São Paulo: Ed. J. de Oliveira, 2001, p. 07

[240] BRASIL. Código Penal. Brasília. Op. Cit.

[241] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 26.

TCC, abrange os elementos essenciais para a compreensão e análise desses crimes: técnica, comportamento e crime[242].

A Técnica refere-se ao método, procedimento, software ou processo informático utilizado, que pode caracterizar um determinado comportamento. Essa técnica pode ser executada manualmente ou por meio de subtécnicas, métodos automatizados ou ferramentas. Por exemplo, um agente que obtém acesso a dados de um repositório pode estar utilizando a técnica de SQL (*Structured Query Language) injection*[243].

O Comportamento, por sua vez, consiste em uma ação realizada por meio de uma ou mais técnicas, cometida por um ou mais agentes, seja por ação ou omissão, em relação a redes de computadores, dispositivos informáticos ou sistemas informatizados. No exemplo mencionado anteriormente, o agente que utilizou a técnica de SQL injection praticou o comportamento de "invasão de sistema informático"[244]. Por fim, o Crime engloba um ou vários comportamentos que utilizam uma ou mais técnicas e que ofendem um ou mais bens ou objetos jurídicos protegidos pelo Direito. É importante ressaltar que a classificação de um comportamento como crime pode variar de acordo com o país em que é praticado[245].

Essa sistematização proposta por Jesus e Milagre contribui para uma melhor compreensão e análise dos crimes cibernéticos, permitindo uma abordagem mais precisa e abrangente dessas condutas no contexto jurídico, devido as particularidades de cada legislação nacional para determinar se um determinado comportamento é considerado crime ou não[246]. Ao abordar a sistematização proposta por Jesus e Milagre, é importante observar não se trata de legislar especificamente sobre a técnica utilizada ou a vulnerabilidade existente, uma vez que esses elementos tendem a se tornar obsoletos rapidamente. O foco deve estar na identificação do comportamento que merece ser considerado crime pelo Direito Penal, levando em consideração o bem jurídico afetado[247].

---

[242] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 26

[243] É um tipo de ameaça de segurança que se aproveita de falhas em sistemas que interagem com bases de dados via SQL. A injeção de SQl ocorre quando o atacante consegue inserir uma série de instruções através de manipulação das entradas de dados de uma aplicação. JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 366.

[244] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 26.

[245] *Ibidem*

[246] *Ibidem*

[247] *Ibidem*

No entanto, é crucial encontrar um equilíbrio na definição desse comportamento, evitando tanto uma especificação excessiva que possa limitar sua aplicação a casos particulares, quanto uma abertura excessiva que possa abranger comportamentos triviais e não ofensivos. É necessário estabelecer critérios claros e objetivos para determinar quais condutas devem ser consideradas criminosas, levando em conta a proteção dos direitos individuais e a preservação da ordem social[248].

Dessa forma, a sistematização proposta busca fornece uma base para a compreensão e a abordagem dos crimes cibernéticos, considerando tanto a dinamicidade das técnicas utilizadas quanto a necessidade de proteção dos bens jurídicos envolvidos. No entanto, é fundamental que essa sistematização seja constantemente revisada e atualizada, a fim de acompanhar as transformações tecnológicas e sociais e garantir uma resposta efetiva aos desafios apresentados pela criminalidade digital[249].

Ainda nessa abordagem da sistemática dos crimes cibernéticos, os autores esclarecem a importância em diferenciar os termos "comportamento" e "técnica" utilizados pelos criminosos digitais. Ao legislar sobre crimes cibernéticos, não se deve começar pela análise de uma técnica específica ou pela definição de tipos penais, mas sim pela análise de condutas que possam ser realizadas de diversas formas (técnicas) e que mereçam a consideração do Direito Penal[250].

Uma técnica, como o "cavalo de Troia"[251], por exemplo, pode ser utilizada tanto para invasão de sistemas quanto para causar danos ou comportamentos inesperados em um sistema informático. No entanto, nem toda técnica se enquadra em uma conduta incriminável. Um dos principais erros cometidos por doutrinadores e legisladores é confundir técnica com conduta. A falta de apoio técnico, como especialistas em tecnologia e segurança da informação, nos setores legislativos, leva o legislador brasileiro a criar tipos penais incoerentes. Por exemplo, vírus de computador, pode não ser uma conduta ilegal, dependendo da técnica empregada[252].

---

[248] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 26.

[249] *Ibidem.*

[250] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 27.

[251] O cavalo de Tróia tem este nome porque, tal como na lenda mitológica, o “presente” recebido aparentemente não oferece nenhum perigo. Ou seja, à primeira vista o programa que contém um cavalo de Tróia parece útil, no entanto uma vez instalado ele causará estragos no computador. GASPARY, Luciano Paschoal et al. Minicursos do V Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais. Sociedade Brasileira de Computação, 2005.pg13.

[252] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 26.

A abordagem adotada em relação à análise das técnicas utilizadas nas ações criminosas, ressaltam que uma mesma ação pode ser realizada por meio de diversos formas gerando inúmeros resultados. Além disso, é possível que certas técnicas, quando praticadas de forma fragmentada, não se enquadrem em um tipo penal específico.[253]

Nesse sentido uma das questões que merece destaque é a necessidade de uma maior precisão na definição dos tipos penais relacionados aos crimes cibernéticos para sua correta tipificação. A falta de clareza e especificidade em algumas descrições legais pode gerar interpretações divergentes e dificultar a aplicação efetiva da lei. Além disso, é importante considerar a dinamicidade do cenário tecnológico e a constante evolução das técnicas utilizadas pelos criminosos digitais. A legislação precisa ser flexível o suficiente para abranger novas formas de crimes cibernéticos que possam surgir no futuro[254].

O Brasil ainda não possuía uma legislação abrangente e específica para tratar dos crimes cibernéticos, e até o ano de 2012 não havia nenhuma disposição legal no ordenamento jurídico brasileiro que tratasse especificamente da punição dos crimes cibernéticos próprios, sendo as legislações existentes focadas principalmente nos cibercrimes impróprios[255].

No entanto no decorrer das últimas décadas, houve uma sequência de projetos de lei no Congresso Nacional buscando estabelecer uma legislação adequada para os crimes cibernéticos. A primeira iniciativa legislativa foi o Projeto de lei nº84/99[256], 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[257], 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 dos crimes cibernéticos.

---

[253] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 26.

[254] *Ibidem*

[255] *Ibidem*

[256] Câmara dos Deputados da República Federativa do Brasil (1999), "Projeto de Lei nº 84/1999", http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028, acesso em set, 2023.

[257] CARNEIRO, Lucas Vitor Vitório; SANTOS, Jackson Novaes; EDLER, Gabriel Octacilio Bohn. O direito cibernético: o impacto gerado pela lei carolina dieckmann no combate aos crimes virtuais realizados contra as crianças e adolescentes. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 8, n. 11, p. 2061-2080, 2022.

Em 2012, em decorrência dos ataques à divulgação de imagens íntimas da atriz Carolina Dieckmann, duas leis foram promulgadas com urgência para preencher algumas lacunas legislativas sobre o tema. Estas leis ficaram conhecidas como Lei 12.735/2012[258], denominada Lei Azeredo, e Lei 12.737/2012[259], Lei Carolina Dieckmann. No mesmo ano também foi sancionada a Lei 12.965/2014, oficialmente intitulada Marco Civil da Internet, a qual estabelece a regulação da internet no Brasil e define princípios, garantias, direitos e deveres para seu uso[260].

Além dessas legislações, que têm sido objeto de extensa análise no contexto dos crimes cibernéticos, é importante mencionar outras normas que também desempenham um papel importante na promoção da segurança jurídica no ambiente virtual, como a Lei Geral de Proteção de Dados Pessoais Lei 13.709/2018[261], que estabelece diretrizes essenciais para o tratamento de informações pessoais na internet e impactou diretamente a forma como as empresas e organizações lidam com dados dos usuários. Mais recentemente, a Lei de Combate ao *Stalking*, Lei 14.132/2021[262], que aborda questões de assédio virtual, reforçando a proteção em especial da mulher, contra práticas criminosas no ambiente digital.

Nesse sentido a constante evolução do cenário cibernético e o surgimento de novas modalidades de crimes cibernéticos impõem a necessidade de uma atualização legislativa contínua e uma ampla discussão acerca da melhor abordagem para proteger os direitos dos cidadãos e coibir atividades ilícitas no espaço digital. E muito embora o arcabouço jurídico brasileiro tem evoluído ao longo dos anos para lidar com os desafios emergentes dos crimes cibernéticos, buscando proporcionar maior segurança jurídica e proteção aos cidadãos no mundo virtual ainda se faz necessário uma maior celeridade legislativa ante a velocidade com que novas condutas surgem no ciberespaço.

---

[258] BRASIL. Lei nº 12.735, de 30 de novembro de 2012. Brasília. Disponível em:<http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em: 22 ago. 2023.

[259] 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

[260] BRASIL. Lei n. 12.965, de 23 de abril de 2014. Brasília, 2014. Disponível em: <http://www.planalto.gov.br/ccivel_03/_ato2011-2014/2014/Lei/L12965.htm. Acesso em 23ago.2023.

[261] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República. Acesso em ago 2023

[262] BRASIL, Lei n. 14.132, de 31 de março de 2021. Disponível em: http://planalto.gov.br/ccivel_03/_Ato2019-20233/2021/Lei/L14132.htm.Acesso em ago. 2023.

Dessa forma após uma breve análise das esferas doutrinária e processual, o presente capítulo pretende examinar o panorama atual da legislação brasileira referente aos crimes cibernéticos. Em seguida, proceder-se-á à análise da tipificação dos principais ataques cibernéticos no ordenamento jurídico nacional, identificando quais medidas legislativas ainda se fazem necessárias para a plena adequação das leis brasileiras aos requisitos estabelecidos pela recente adesão do Brasil na convenção de Budapeste.

3.1.1 Lei Azeredo (Lei 12.735/12)

Primeiramente é importante ressaltar a distinção entre o Projeto de Lei (PL) 84/99 e a Lei 12.735/12, ambas são popularmente conhecidas como "Lei Azeredo". A PL 84/99, inicialmente apresentada pelo Ex deputado federal Piauhulino (PSDB-PE), foi posteriormente alterada pelo então senado Eduardo Azeredo, o que levou o projeto a ser conhecido como Lei Azeredo. O projeto dispunha sobre os crimes, penas e outras providências quanto ao meio virtual. Embora seja o mais antigo, é também o mais criticado desde sua criação. Importa frisar que a proposta em discussão costumeiramente é comparada ao Ato Institucional nº 5, que remota ao período da ditadura militar brasileira, que suspendia as garantias constitucionais. Isso ocorreu em função do estado de vigilância constante pretendido pelo projeto que acabaria com uma das principais característica do meio virtual, a privacidade[263].

Seu objetivo primordial era estabelecer um arcabouço legal para crimes cibernéticos, tornando determinadas ações no ambiente digital sujeitas a penalidades como prisão e multa. Essa iniciativa legislativa, contudo, foi duramente criticada, dada a abrangência e a severidade de suas disposições. No Projeto, constava que não se podia permitir que pela falta de lei, que regule os crimes de informática, pessoas inescrupulosas continuassem a usar computadores e suas redes para propósitos escusos e criminosos, daí a necessidade de uma lei que definisse de forma mais incisiva os crimes cometidos na rede e a imposição de severas penas[264].

A Lei 12.735, sancionada em 30 de novembro de 2012, originada da PL 84/99 sofreu diversas modificações em sua trajetória parlamentar. Embora o texto inicial contasse com 18 artigos, o número cresceu para mais de 20 após as emendas na relatoria. No entanto, apenas cinco destes artigos foram aprovados pelo congresso em 2012. Dos aprovados, dois, que versavam sobre

[263] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 110.

[264] *Ibidem.*

a falsificação de cartões de crédito e a disseminação de informações estratégicas militares, foram vetados pelo Poder Executivo[265].

A legislação em questão teve como objetivo principal estabelecer normas para condutas realizadas por meio de sistemas eletrônicos digitais, bem como aquelas praticadas contra sistemas informatizados e seus equivalentes, e já nos seus primeiros artigos abordam a tipificação de crimes cometidos no ambiente virtual[266].

Uma importante alteração trazida pela Lei 12.735 diz respeito ao inciso II do parágrafo 3º da Lei 7.716, de 5 de janeiro de 1989, que aborda crimes por preconceito de raça e cor. A atualização prevê a possibilidade de interromper transmissões eletrônicas ou publicações em qualquer meio quando houver fabricação, venda, distribuição ou veiculação de elementos que utilizem a cruz suástica ou gamada com o propósito de promover o nazismo, especialmente por meios de comunicação ou publicações de qualquer natureza[267].

Já as condutas relacionadas à falsificação de cartão de crédito e ao delito em favor do inimigo, que já eram previstas no Código Penal e no Código Penal Militar, respectivamente, foram inicialmente contempladas nos artigos 2º e 3º, mas foram excluídas na versão final da lei. Além disso, a legislação também abrangia aspectos processuais e penais no combate aos crimes digitais, conforme estabelecido no artigo 4º, que fundamentava a criação de órgãos especializados nesse combate. Isso se deve ao fato de que a investigação desses delitos geralmente começa com a localização e manipulação de equipamentos informáticos e dos dados armazenados neles, exigindo profissionais tecnicamente capacitados. Por sua vez, o artigo 5º alterou a redação do §3º do Art. 20 da Lei n.º 7.716/1989[268], que tratava dos crimes resultantes de preconceito de raça ou cor, com o objetivo de coibir a disseminação do preconceito e da intolerância racial por meio das novas tecnologias[269].

Embora a Lei Azeredo tenha sido criada especificamente para tipificar crimes cibernéticos, este papel acabou sendo delegado à Lei N.º12.737 de 201236 , promulgada no mesmo ano. Dessa

---

[265] PAGANOTTI, Ivan. Pressão virtual e regulamentação digital brasileira: análise comparativa entre o marco civil da internet e a lei azeredo. Revista Eptic Online, v. 16, n. 2, 2014.

[266] BRASIL. Lei nº 12.735. Op. Cit.

[267] *Ibidem.*

[268] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 110

[269] *Ibidem.*

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[270].

3.1.2 Lei Carolina Dieckmann (Lei N. 12.737/12)

A Lei 12.737/2012[271], conhecida como Lei Carolina Dieckmann, recebeu esse nome devido ao vazamento das fotos íntimas da atriz. Esse incidente trouxe certa notoriedade ao projeto em questão, que havia sido proposto no ano anterior e aprovado pela Câmara dos Deputados duas semanas após o referido episódio. A lei, de autoria conjunta do então deputado federal Paulo Teixeira, resgatou o que a PL 84/99, porém sem as controvérsias da época. A lei trata de delitos informáticos, tipificando condutas que não eram previstas de forma específica como infrações penais[272].

Popularmente ficou conhecida como "Lei Carolina Dieckmann", em virtude do incidente amplamente divulgado na mídia, no qual *crackers* (criminosos digitais) invadiram os arquivos da atriz brasileira, e acessaram seus dados de forma não autorizada. A atriz recusou-se a ceder a chantagens financeiras para evitar a divulgação ilícita de suas imagens íntimas em sites de pornografia, dando notoriedade e celeridade ao projeto que já estava em andamento e versava sobre a tipificação de invasão de dispositivos informáticos[273].

Importante ressaltar que a Lei nº 12.737/2012 representou um marco normativo fundamental ao estabelecer a tipificação desse tipo penal. Essa iniciativa demonstrou a intenção explícita de modernizar o arcabouço jurídico da época, evitando a introdução de legislação penal fragmentada no ordenamento jurídico nacional. Consequentemente, contribui para a sistematização e a unificação das normas que criminalizam tais condutas, o que, por sua vez, facilita a compreensão do cidadão comum quanto à função pedagógica da legislação penal repressiva. Além disso, promove uma base sólida para a tarefa hermenêutica e a aplicação das leis por parte do Poder Judiciário[274].

---

[270] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 110

[271] BRASIL. Lei 12.737, de 30 nov. 2012. Op. Cit.

[272] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 110

[273] Carolina Dieckmann fala pela 1ª vez sobre fotos e diz que espera “justiça”. G1, São Paulo. 14 maio 2012. Disponível em: Acesso em: 30 jul. 2017

[274] KUNRATH, Josefa Cristina Tomaz Martins. A expansão da criminalidade no ciberespaço: desafios de uma política criminal de prevenção. 2014, pg 66.

Nesse sentido, a Lei nº 12.737/2012 trouxe inovações ao ordenamento jurídico brasileiro ao estabelecer novos tipos de delitos, ampliando a legislação sobre crime cibernético no Brasil. Essa lei introduziu no Código Penal artigos que tratam da invasão de dispositivo informático, interrupção ou perturbação de serviço telemático ou de informação de utilidade pública, bem como a falsificação de cartão[275].

Um aspecto notável dessa Lei é o seu artigo 2º, que tipifica as condutas relacionadas à "invasão de dispositivo informático". Esse artigo expandiu o Código Penal brasileiro, incluindo os artigos 154-A e 154-B[276], que têm como objetivo penalizar aqueles que invadem, adulteram ou destroem a privacidade digital de terceiros, violando mecanismos de segurança.

No que diz respeito ao crime previsto no artigo 154-A, que trata da invasão de dispositivo informático, seu objetivo é proteger a inviolabilidade dos dados informáticos, que está relacionada ao direito à privacidade e à intimidade, garantidos pelo artigo 5º da Constituição Federal[277]. Além disso, busca-se assegurar a integridade dos dados, protegendo-os contra destruição e alteração. Essa proteção abrange tanto os programas computacionais quanto os dados armazenados neles[278].

O tipo penal denominada invasão de dispositivo informático, de acordo com o disposto no artigo 154-A do Código Penal, delineia uma conduta delituosa específica. Esta consiste na invasão de dispositivo informático pertencente a outrem, independentemente de estar conectado à rede de computadores, por meio da indevida violação de mecanismos de segurança, com a finalidade de adquirir, adulterar ou eliminar dados ou informações sem a expressa ou tácita autorização do titular do dispositivo, ou ainda, para instalar vulnerabilidades com o propósito de obter vantagem ilícita[279].

A pena prevista para a modalidade simples do crime em questão é de detenção, com pena variando de três meses a um ano, além da imposição de multa. No que tange à forma qualificada, conforme estipulado pelo § 2º, a pena é acrescida em um sexto a um terço quando a invasão resulta em prejuízo econômico para a vítima. No cenário previsto pelo § 3º, a penalidade é aumentada de um a dois terços caso haja divulgação, comercialização ou transmissão dos dados ou informações obtidas a terceiros, independentemente da finalidade. Adicionalmente, a punição é agravada em

---

[275] BRASIL. Lei 12.737, de 30 nov. 2012. Op. Cit

[276] BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Op. Cit.

[277] *Ibidem.*

[278] VIANA, Túlio Lima. Op. Cit, p.93

[279] KUNRATH. Op. Cit. Pg. 66.

um terço a metade quando o crime for cometido contra autoridades de alto escalão, como Presidente da República, Governadores, Prefeitos, Presidente do Supremo Tribunal Federal, Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal, ou dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal[280].

Este tipo penal foi inserido no capítulo que aborda os crimes contra a liberdade individual (artigos 146 a 154 do Código Penal), mais especificamente, em sua Seção IV - Dos Crimes contra a Inviolabilidade dos Segredos (artigos 153 a 154-B do Código Penal). Consequentemente, o bem jurídico sob proteção legal engloba a salvaguarda da liberdade individual, a privacidade e a intimidade de pessoas físicas e jurídicas, direitos já resguardados pelo inciso X do artigo 5º da Constituição Federal[281].

De acordo com Cabette, o crime de invasão de dispositivo informático configura-se com a mera invasão ou instalação de vulnerabilidade. O acesso a dados, sua adulteração ou mesmo a obtenção de vantagens ilícitas são consideradas extensões desse crime. A sua forma qualificada é identificada quando, efetivamente, se obtêm dados após a invasão. É um crime formal, consumando-se apenas com a invasão ou introdução de vulnerabilidades, como códigos maliciosos para captura de senhas. Contudo, ele admite tentativa. O autor pode ser qualquer indivíduo ou entidade, e as motivações para tal conduta variam desde o desejo de superar barreiras de segurança até intenções econômico-financeiras[282].

Nas palavras de Kunrath, nos crimes de invasão de dispositivo informático, é necessário o elemento subjetivo do dolo específico, excluindo-se a modalidade culposa. Esse dolo é caracterizado pela intenção de "obter, adulterar ou destruir dados" ou pela instalação de vulnerabilidades com propósito de vantagem ilícita. A simples invasão do sistema ou dispositivo já se enquadra no tipo penal, independentemente de conseguir vantagem ou adulteração. Dispositivo informático, nesse contexto, engloba computadores, dispositivos móveis como *notebooks, tablets e smartphones*, entre outros equipamentos com capacidade de armazenamento, estejam eles conectados à internet ou não, e futuras inovações tecnológicas[283].

---

[280] BRASIL. Lei 12.737, de 30 nov. 2012. Op. Cit

[281] KUNRATH. Op. Cit. Pg. 66.

[282] CABETTE, Eduardo L. S. O novo crime de Invasão de Dispositivo Informático. Consultor Jurídico, São Paulo. Disponível em: <http://www.conjur.com.br/2013-fev-04/eduardo-cabette-crime-invasao-dispositivo-informatico>. Acesso em: 20 set 2023.

[283] KUNRATH. Op. Cit. Pg. 68.

Importante ressaltar que o elemento normativo do tipo é que o dispositivo informático alheio esteja protegido por mecanismos de segurança, com um antivírus, *firewall* ou senhas. Neste sentido Cabette explica que, se um dispositivo estiver sem essas proteções não se enquadra na conduta criminalizada, exigindo-se a violação indevida de mecanismo de segurança. Tal abordagem legislativa parece incongruente, pois sugere que a ausência de proteção em um sistema torna sua invasão atípica. Analogicamente, seria como entender que uma casa com portas abertas permite sua invasão, ignorando o consentimento do proprietário. O autor argumenta ainda que a legislação poderia ser mais inclusiva e justa ao enfocar apenas a invasão ou instalação indevidas, desvinculando-se da menção específica a mecanismos de segurança[284].

Os apontamentos de Milagres e Damásio, no tipo penal estabelecido pela Lei 12.737/2012, referente à invasão de dispositivo informático, configura-se como um perigo abstrato, isto é, um tipo penal que não demanda a concretização de um dano efetivo. O autor destaca que, embora os perigos contemporâneos não sejam necessariamente superiores aos enfrentados por gerações passadas, a percepção destes riscos sofreu alterações. Esta mudança é impulsionada tanto pelas incertezas científicas inerentes às novas tecnologias quanto pela ampla cobertura midiática de eventos adversos. Este contexto gera uma atmosfera de insegurança palpável, levando a sociedade a uma postura menos tolerante a comportamentos arriscados, mesmo que estes não resultem em danos concretos. Assim, percebe-se uma tendência legislativa voltada à proibição de condutas potencialmente perigosas em resposta ao desejo social por maior segurança e estabilidade diante dos desafios contemporâneos[285].

Assim, na sociedade da informação, observa-se um crescente movimento de proteger direitos supraindividuais, adotando-se uma abordagem preventiva por parte do Estado em resposta a potenciais riscos, ao invés de ameaças concretas ao bem jurídico. Contudo, é importante lembrar que o princípio constitucional da presunção de inocência se contrapõe a qualquer presunção em desfavor do agente[286].

Sob essa perspectiva, os autores argumentam que os delitos de perigo abstrato não deveriam ser contemplados na legislação penal. No entanto, dada a realidade permeada por incertezas e riscos, o legislador, em seu esforço de antecipar e mitigar a criminalidade digital, tem

[284] CABETTE. Op. Cit.

[285] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 137.

[286] *Ibidem.*

frequentemente recorrido a essa categoria de delitos, buscando prevenir eventualidades antes que um dano efetivo ocorra[287].

Nesse sentido, muito embora a Lei 12.737/2012 tenha trazido avanços para o arcabouço jurídico brasileiro em relação aos crimes cibernéticos, a legislação ainda está longe de apaziguar a questão da efetiva punição dos criminosos. Isso porque a punição é para invasão (com finalidade dolosa), pouco importando o resultado da atividade ilícita autorizada[288].

O artigo 154-B, trazido pela Lei 12.737/2012 estabelece ainda que a ação penal para o crime de invasão de dispositivo informático será pública, condicionada à representação da vítima, exceto nos casos em que o delito for cometido contra a administração pública direta ou indireta da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos, nestes casos a ação penal será incondicionada[289].

Além disso, a Lei nº 12.737/2012 modificou os delitos tipificados nos artigos 266 e 298 do Código Penal[290], que não era expresso ao tratar da possibilidade de sistemas informáticos serem objeto do ataque envolvendo a interrupção. Tal lacuna foi suprimida com a alteração da redação incluindo o serviço informático, telemático ou de informação de utilidade pública, bem como impedir ou dificultar-lhe o restabelecimento, estipulando penas que variam de um a três anos de reclusão e multa, que são aplicadas em dobro em caso de calamidade pública. Trata-se de um crime formal, podendo ser comissiva ou omissiva[291].

Milagres e Damásio definem serviços de utilidade pública como aqueles que objetivam facilitar a vida do indivíduo na sociedade, colocando à disposição deste utilidades que lhe proporcionam mais conforto e bem-estar. Já a telemática é caracterizada como um conjunto de tecnologias voltadas à transmissão de dados, fruto da integração entre telecomunicações e informática, otimizando o processamento, armazenamento e comunicação de informações. Nesse contexto, os serviços telemáticos resultam na junção entre informática e telecomunicações, potencializando o manejo da informação de forma mais interativa e produtiva. Ademais, os autores ressaltam que o foco do dispositivo é o funcionamento do serviço de comunicação, voltado ao interesse coletivo. Dessa forma, para que se aplique o referido dispositivo em situações de

---

[287] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 298.

[288] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 299.

[289] BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Op. Cit.

[290] *Ibidem.*

[291] BRASIL. Lei 12.737, de 30 nov. 2012. Op. Cit

interrupção de um serviço específico, é crucial avaliar se tal interrupção prejudicou de fato o bem-estar coletivo ou se apresentou um risco compartilhado[292].

O artigo 298º do código penal, já previa o delito de falsificação de documento particular ou alteração de documento particular verdadeiro, o que a lei n 12.737/2012 trouxe foi a inserção do parágrafo onde equipara o documento particular o cartão de crédito ou débito. Nesse sentido bem jurídico que buscou proteger foi a fé pública, no que tange aos documentos particulares, sendo a intenção maior do legislador atender as constantes fraudes bancárias envolvendo clonagem de cartões. Porém, o artigo não se aplica às fraudes financeiras praticadas pela internet[293].

Na interpretação de Milagres e Damásio sobre a Lei 12.737/2012, ao estabelecer uma equiparação do cartão de crédito ou débito a um documento particular, ficou notório que esses cartões, predominantemente confeccionados em plástico e que servem como instrumentos de autenticação em transações comerciais, encontram-se em uma trajetória de evolução constante, com uma tendência à obsolescência acelerada. Os autores argumentam que essa legislação, possivelmente impulsionada por eventos notáveis, não contemplou adequadamente as implicações futuras do dispositivo. A equiparação à categoria de documentos particulares poderia ser mais abrangente, considerando que, atualmente, documentos são armazenados em *CDs, pendrives, memory sticks, chips*, entre outros dispositivos passíveis de falsificação[294]. Dessa forma, esses formatos não seriam abarcados pela Lei 12.737/2012, que se mostrou específica ao definir quais tecnologias se assemelham a documentos particulares. Isso aponta para uma legislação que apresenta limitações desde sua criação diante dos avanços tecnológicos[295].

Nesse sentido ao analisar a lei 12.737/2012, Peck ressalta que aqueles que instalam vulnerabilidades em sistemas de informação com o intuito de obter vantagem indevida, como *backdoors*[296] ou configurações que deixam portas de comunicação abertas, estarão sujeitos às mesmas penalidades aplicadas aos invasores. Essa medida visa proteger os usuários comuns de dispositivos eletrônicos contra *hackers* e indivíduos mal-intencionados que abusam da confiança alheia ou buscam intencionalmente invadir dispositivos para roubar dados ou prejudicar seus

[292] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 205.

[293] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 206.

[294] *Ibidem*

[295] *Ibidem*

[296] Tipo de código malicioso. Programa que permite o retorno de um invasor a um computador comprometido, por meio de inclusão de serviços criados ou modificados para este fim. Normalmente esse programa é colocado de forma a não ser notado. JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 354.

proprietários[297]. Essas ações podem incluir exclusão ou alteração de dados, tornando-os inutilizáveis, bem como o acesso a informações íntimas e privadas, como fotos, documentos e vídeos. Além disso, a nova legislação também oferece maior proteção jurídica às empresas contra a espionagem digital, uma vez que a obtenção de segredos comerciais e informações sigilosas, conforme definido por lei, agora também se enquadra como crimes cibernéticos[298].

Em suma, a criação da Lei Carolina Dieckmann teve como objetivo preencher lacunas legislativas existentes no ordenamento jurídico interno, buscando uma repressão e punição mais efetivas dos ilícitos praticados no ambiente virtual. Assim, representou um grande avanço na modernização da legislação brasileira para lidar com a crescente ameaça dos crimes cibernéticos. No entanto, apesar das melhorias trazidas por essa lei, a tipificação das condutas relacionadas a esse tema ainda está longe de solucionar todos os problemas relativos aos crimes cibernéticos no Brasil. Nas palavras de Milagres e Damásio a solução não é fácil de ser encontrada, mas com certeza não resolve tão somente com a edição de leis e mais leis criminais. Envolve educação digital, políticas criminais e estrutura investigativa[299].

3.1.3 Marco civil da internet (Lei N. 12.965/14)

Antes da implementação do Marco Civil da Internet, o Brasil carecia de uma legislação abrangente que tratasse das questões relacionadas especificamente das ações realizadas na internet. Nesse sentido, apenas resoluções emitidas pelo Poder Executivo tentavam suprir a lacuna legislativa referente a questões jurídicas emergentes no ambiente virtual e no uso de suas plataformas[300].

Com o objetivo de promover a participação popular, a matéria foi disponibilizada à comunidade em geral, a fim de obter opiniões sobre a minuta de anteprojeto. Esse ato foi considerado como uma estratégia para garantir a aprovação do projeto por parte da população. Nessa ocasião, foi criado um blog no qual os internautas puderam expressar suas opiniões,

---

[297] PINHEIRO, Patrícia Peck; HAIKAL, Victor Auilo. A nova lei de crimes digitais. 2013. Disponível em: <www.pppadvogados.com.br/Publicacoes.aspx?v=1&nid=1432>. Acessado em:14/05/2023.

[298] PINHEIRO, Patrícia Peck; HAIKAL, Victor Auil, Op. Cit.

[299] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 298.

[300]BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. Manual de investigação cibernética: à luz do Marco Civil da Internet. Brasport, 2016. Pg28

interesses e situações que desejavam regulamentar, fato esse inovador no contexto do processo legislativo brasileiro[301].

A participação popular foi efetiva na definição inicial do projeto de lei, demonstrando que este não foi moldado exclusivamente pelo poder legislativo, mas sim derivado de uma iniciativa efetiva da sociedade. Após o período de recebimento de sugestões, a secretaria de assuntos legislativos do Ministério da Justiça, em conjunto com a escola da Fundação Getúlio Vargas do Rio de Janeiro, que possui um grupo de pesquisa sobre Direito e Sociedade, elaboraram a minuta consolidada. Posteriormente, o projeto foi novamente aberto à sociedade para que esta pudesse opinar sobre seu conteúdo[302].

O marco civil da internet surgiu com o conceito de "constituição da internet, de forma que garantisse os direitos e deveres de todos os usuários da internet, nesse sentindo trouxe em seus artigos o respeito à liberdade de expressão como seu fundamento, o que é reforçado pelo artigo 19, que busca assegurar a liberdade de expressão e evitar a censura[303]. Além disso, o artigo 3º, I, define os princípios do uso da internet no Brasil, de acordo com a Constituição Federal, garantindo a liberdade de expressão, comunicação e manifestação do pensamento. Um cuidado especial foi dado ao direito à privacidade, conforme os incisos I, II, III, VII e VIII do artigo 7º, que estabelecem os direitos dos usuários, como a inviolabilidade da intimidade e vida privada, a preservação do sigilo das comunicações transmitidas ou armazenadas, a proibição do fornecimento de dados coletados pela internet sem o consentimento prévio do usuário, bem como a obrigação de informar o usuário sobre a coleta de dados sobre si, desde que haja justificativa para tal[304].

Da mesma forma, o artigo 10º determina que a guarda e disponibilização dos registros de conexão e acesso a aplicações de internet devem ser realizadas com respeito à intimidade, vida privada, honra e imagem das pessoas envolvidas direta ou indiretamente. O artigo 14º estabelece que os provedores de internet não podem armazenar registros de acesso sem o consentimento prévio do usuário. Outro aspecto que recebeu atenção do legislador foi o combate às atividades ilícitas civis e criminais praticadas na internet sob o pretexto da privacidade. Assim, o artigo 13º

[301] BRANT, Cássio Augusto Barros. O microssistema do direito tecnodigital. Belo Horizonte, 2016, pg 131.

[302] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 298.

[303] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 299.

[304] BRANT, Cássio Augusto Barros. Op. Cit. Pg 136.

estabelece a obrigação de manter os registros de acesso dos usuários por, pelo menos, um ano, sendo que, no caso das redes sociais, esse período é de seis meses[305].

O legislador também abordou a responsabilidade civil dos provedores de internet por violações aos direitos da personalidade, como honra, imagem, vida privada e intimidade das pessoas. Ou seja, os provedores podem ser responsabilizados por danos decorrentes de conteúdo postado caso não o removam após ordem judicial[306]. Além disso, são previstas medidas preventivas, como a possibilidade de os provedores retirarem do ar notícias que possam causar danos a determinados usuários sem a necessidade de uma ordem judicial (por exemplo, vítimas de "vingança pornô"). Também existem ações repressivas contra crimes como pedofilia, racismo ou divulgação não autorizada de imagens íntimas. Por fim, o artigo 29º, juntamente com seu parágrafo único, garante o direito do usuário de instalar em seu computador pessoal programas de controle parental, ou seja, programas destinados a filtrar conteúdos considerados impróprios para crianças menores[307].

No contexto brasileiro, apesar da promulgação do Marco Civil da internet ser concebida para estabelecer diretrizes e obrigações relacionadas à utilização da rede de computadores, a sua efetivação no âmbito penal ainda não se materializou. Apesar de ser instituída baseada na Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD)[308], não supriu a proteção de dados pessoais nos contextos de segurança pública, defesa nacional e nas atividades de investigação e repressão de infrações penais, conforme estipulado no seu artigo 4º. Tal limitação acarreta desafios significativos para os órgãos de inteligência e de persecução penal, impondo restrições que merecem análise e discussão mais aprofundadas no cenário jurídico brasileiro[309].

Nesse contexto, o Marco Civil da Internet se revela como uma lei pioneira nas questões específicas de condutas praticadas no ambiente virtual, buscando harmonizar a liberdade de expressão com a preservação dos direitos de privacidade dos internautas, ao mesmo tempo em que procura regulamentar o uso da internet e salvaguardar os direitos individuais. É importante

---

[305] BRANT, Cássio Augusto Barros. Op. Cit. Pg 136.

[306] *Ibidem.*

[307] BRANT, Cássio Augusto Barros. Op. Cit. Pg 136.

[308] 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.

[309] FIGUEIREDO, Alani Caroline Osowski; RIOS, Rodrigo Sánchez. Proteção de dados pessoais e direitos fundamentais: desafios frente à cooperação jurídica internacional em matéria penal. Revista Científica do CPJM, v. 2, n. 07, p. 114-129, 2023.

ressaltar que seu impacto integral ainda está sob avaliação, e sua plena efetivação continua sendo um desafio[310].

3.1.4 Lei Geral de Proteção de dados Pessoais – (Lei 13709/2018)

A proteção de dados ganha cada vez mais relevância à medida que o mundo se torna mais digitalizado, e os dados pessoais que trafegam nesse ambiente emergem como ativos de valor inestimável para diversas empresas e organizações. Tanto em âmbito nacional quanto global, a implementação de leis e regulamentos buscam preservar a privacidade dos cidadãos, estabelecendo diretrizes claras para as entidades responsáveis pela manipulação dessas informações. A ascensão dessa nova configuração social, impulsionada principalmente pela internet, tem remodelado nossas interações, economias e a maneira como nos relacionamos com o conhecimento e a informação. No entanto, com as inúmeras oportunidades de crescimento e transformação, a sociedade conectada também se torna um ambiente propício para o surgimento e a disseminação do cibercrime e a proteção dos dados se torna essencial diante dos desafios impostos pelos crimes cibernéticos.

No Brasil, a Lei 13.709/2018 conhecida como Lei Geral de Proteção de Dados (LGPD)[311] representa uma inovação no país, estabelecendo princípios e conceitos orientadores para o uso seguro de dados. Seu objetivo principal é alcançar um equilíbrio entre a proteção efetiva dos direitos dos titulares desses dados e a possibilidade de processamento de dados pessoais e sensíveis para fins específicos, incluindo a pesquisa científica. A LGPD introduziu, pela primeira vez no sistema jurídico brasileiro, um conjunto de normas e princípios voltados para a regulamentação do tratamento de dados pessoais em todas as atividades cotidianas dos cidadãos, abrangendo diversos setores[312].

Na análise de Mendes e Doneda, a Lei Geral de Proteção de Dados (LGPD) se estrutura em torno de cinco pilares fundamentais: a generalidade e unidade em sua aplicação; as bases autorizadas para tratamento de dados; os princípios e direitos do titular dos dados; as obrigações dos agentes de tratamento; e a responsabilização desses mesmos agentes. Ao examinar estes

[310] BRASIL. Marco civil da internet: Lei n. 12.965.Op. Cit.

[311] 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.

[312] PINHEIRO, Patrícia Peck. Proteção de dados pessoais: Comentários à lei n. 13.709/2018-lgpd. Saraiva Educação SA, 2020. pg 1488.

pilares, torna-se evidente que a LGPD visa uma aplicação abrangente e uniforme, sugerindo uma possível aplicabilidade no contexto da jurisdição penal[313].

O artigo 2º da Lei Geral de Proteção de Dados estabelece os princípios fundamentais da proteção de dados pessoais. Esses princípios incluem o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, a inviolabilidade da intimidade, honra e imagem, bem como o desenvolvimento econômico, tecnológico e a inovação, entre outros. Essa complexa intersecção entre privacidade, direitos humanos, liberdade, dignidade e desenvolvimento econômico destaca a dualidade da legislação: ao mesmo tempo em que protege a privacidade do indivíduo, também promove o crescimento econômico e tecnológico[314].

No artigo 3º da LGPD, é estabelecido que a lei será aplicada independentemente do meio, do país de origem ou da localização dos dados. 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 de extrema importância para a privacidade, pois uma violação desses dados pode resultar em consequências graves. Portanto, é concedida uma proteção adicional a esses dados, uma vez que está o intrinsecamente ligados à liberdade e à dignidade do indivíduo[315].

Já no artigo 4º, a Lei Geral de Proteção de Dados (LGPD) são estabelecidas algumas exceções quanto à sua aplicabilidade. Não se aplica, por exemplo, a dados tratados por indivíduos para propósitos estritamente pessoais e sem fins econômicos. Também estão isentos os dados processados com objetivos exclusivamente jornalísticos, artísticos ou acadêmicos, sendo que, para o contexto acadêmico, certos artigos da LGPD são especificamente aplicáveis. A lei também se abstém em casos que envolvam segurança pública, defesa nacional, segurança do Estado ou investigações e repressões de infrações penais. Adicionalmente, não se aplica a dados oriundos de fora do Brasil, a menos que esses dados sejam compartilhados com agentes

[313] MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. Revista de Direito do Consumidor, 2020.

[314] BRASIL. Lei 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD

[315] PINHEIRO, Patricia Peck. Proteção de dados pessoais: Comentários à lei n. 13.709/2018-lgpd. Op. Cit. pg1488.

nacionais ou transferidos para outro país, exigindo que o país de origem ofereça um nível de proteção de dados equivalente ao estipulado pela Lei[316].

Nesse sentindo, A LGPD traz uma dualidade intrigante em seus dispositivos. Enquanto artigo 4º da legislação estabelece claramente a não aplicabilidade da mesma nas atividades de investigação e repressão de infrações penais no território nacional, o artigo 33º, III, delineia condições específicas para a transferência internacional de dados pessoais. Este último destaca que tal transferência é permitida unicamente quando necessária para a cooperação jurídica internacional entre órgãos de inteligência, investigação e persecução. Essa cooperação deve estar alinhada com os instrumentos de Direito Internacional[317].

Essa aparente dicotomia na legislação indica que, enquanto se abstém de regular a investigação criminal no âmbito nacional, a LGPD aborda explicitamente a necessidade cooperação internacional no âmbito da persecução penal. Esta disposição sugere que, embora a LGPD se distancie de questões penais internas, reconhece a relevância e a necessidade de normatizar as interações no cenário internacional, garantindo uma segurança jurídica nas relações entre autoridades brasileiras e estrangeiras[318].

No contexto da Lei Geral de Proteção de Dados (LGPD), é pertinente enfatizar que as sanções delineadas estão circunscritas ao âmbito administrativo. No entanto, a manipulação imprópria de dados pessoais pode ter implicações que ultrapassam essa esfera, culminando em consequências penais para aqueles que os gerenciam, sejam operadores ou controladores de dados. Neste cenário, podem ser invocados dispositivos legais como o artigo 307º do Código Penal, que aborda a falsa identidade, e o artigo 21º da Lei n. 7.429/1976, relacionado à falsidade ideológica em operações de câmbio. Adicionalmente, para os servidores públicos, o artigo 313-B, que trata da modificação ou alteração não autorizada de sistemas de informações, pode ser particularmente relevante[319].

Embora a legislação não mencione explicitamente investigações ou repressão de infrações penais, há debates no meio jurídico sobre a necessidade de mecanismos de responsabilização criminal. A LGPD não introduz novos delitos penais, porém, é possível

[316] BRASIL. Lei 13.709. Op. Cit.

[317] MENDES, Laura Schertel; DONEDA. Op. Cit.

[318] MENDES, Laura Schertel; DONEDA. Op. Cit.

[319] MALDONADO, Laura Braga; SOTERO, Andrea Luiza Escarabelo. Aplicabilidade da Lei Geral de Proteção de Dados Pessoais Lei 13.709/18—sanções administrativas e criminais. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, v. 7, n. 3, p. 221-229, 2021.

recorrer ao Código Penal, à Lei do Sistema Financeiro Nacional, ao CDC e a outras normativas relacionadas à proteção de dados para entender possíveis implicações criminais[320].

A implementação da Lei Geral de Proteção de Dados (LGPD) no Brasil tem sido um desafio tanto para as organizações quanto para os órgãos de fiscalização. As empresas tiveram que se adaptar às exigências da lei, reavaliando suas práticas de coleta, armazenamento e tratamento de dados. A adequação à LGPD requer 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[321].

Nesse sentido, vale lembrar que a regulamentação sobre proteção de dados sofreu várias modificações significativas desde sua promulgação, como a Medida Provisória n. 869/2018, que posteriormente instituiu a Autoridade Nacional de Proteção de Dados (ANPD), órgão crucial que garante a uniformidade, aderência e execução das normativas elencadas na lei[322].

A ANPD, enquanto entidade da administração pública, tem como missão primordial assegurar os direitos fundamentais relacionados à liberdade e privacidade, bem como supervisionar, orientar e garantir a aplicação da LGPD, intervindo com sanções quando identificadas violações na gestão de dados. A configuração organizacional da ANPD foi delineada pelo Decreto n. 10.474, de 26 de agosto de 2020, posicionando-a sob a alçada da Presidência da República, especificamente vinculada à Casa Civil. Ademais, ressalta-se que a maior parte das nomeações no órgão, seja no Conselho Diretor ou no Conselho Consultivo, é prerrogativa do presidente da República[323]. Recentemente houve nova alteração por meio da Lei 14.460/2022 que transformou a ANPD em autarquia de natureza especial[324].

No âmbito internacional, é importante ressaltar que a Lei Geral de Proteção de Dados (LGPD) foi amplamente influenciada pelo Regulamento Geral de Proteção de Dados (GDPR)[325] da União Europeia, com o objetivo de consolidar em um único regulamento geral a

---

[320] MALDONADO e SOTERO. Op. Cit.

[321] *Ibidem.*

[322] PINHEIRO, Patrícia Peck. Direito digital. Saraiva Educação SA, 2021, pg.285.

[323] PINHEIRO, Patrícia Peck. Direito digital. Op. Cit pg 285.

[324] PINHEIRO, Patricia Peck. Proteção de dados pessoais: Comentários à lei n. 13.709/2018-lgpd. Op. Cit. Pg815.

[325] 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-

regra de 28 Estados-Membros. Há hoje leis nacionais sobre a matéria nos países membros que fizeram com que as instituições dependendo do tipo de operação dos seus negócios tivessem que construir uma matriz de análise comparativa (direito comparado) para analisar qual a regra aplicável em determinado caso concreto que envolva dados de um determinado titular[326].

A proteção de dados no contexto digital, tanto no Brasil quanto no mundo, é uma questão de extrema importância, considerando o crescente volume de coleta e processamento de dados pessoais. Apesar dos avanços significativos proporcionados pela Lei Geral de Proteção de Dados (LGPD), a proteção de dados no Brasil ainda enfrenta desafios. A efetiva implementação da lei depende não apenas 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[327].

Como exemplo, patrícia Peck ilustra que uma instituição brasileira que colete dados no território nacional, mas que possua um aplicativo aberto a clientes de diversas nacionalidades, residências e cidadanias, pode se deparar com questões relacionadas à aplicação de leis e jurisdições. Por exemplo, um cidadão europeu que esteja temporariamente trabalhando no Brasil, utilizando um cartão de crédito internacional, pode ser considerado o titular dos dados e, portanto, estar sujeito tanto à regulamentação nacional (Lei Geral de Proteção de Dados - LGPD) quanto à regulamentação europeia (Regulamento Geral de Proteção de Dados - GDPR)[328].

Além disso, caso essa instituição brasileira utilize recursos de armazenamento em nuvem e opte por guardar os dados pessoais em outro país, poderá estar sujeita a outras regulamentações, como o *Cloud Ac*t dos Estados Unidos. Essa legislação americana estabelece que as autoridades dos EUA podem solicitar acesso a dados armazenados em servidores localizados fora do país, desde que esses servidores sejam controlados por empresas americanas[329].

---

eu_pt#:~:text=O%20Regulamento%20(UE)%202018%2F,Dados%20na%20Aplica%C3%A7%C3%A3o%20da%20Lei. Acesso:28 mai.2023.

[326]PINHEIRO, Patricia Peck. Proteção de dados pessoais: Comentários à lei n. 13.709/2018-lgpd.pg1302.

[327] PINHEIRO, Patricia Peck. Proteção de dados pessoais: Comentários à lei n. 13.709/2018-lgpd.pg1302.

[328] PINHEIRO, Patrícia Peck. Proteção de dados pessoais: Comentários à lei n. 13.709/2018-lgpd. Op.Cit. pg.1302.

[329] GUIDI, GUILHERME BERTI DE CAMPOS. provas no estrangeiro Cloud Act and the reflections on the systematics of evidence collection abroad. Revista de Direito, v. 2019, p. 07-08.

No contexto atual, é de suma importância que as instituições brasileiras estejam plenamente conscientes das implicações legais e regulatórias relacionadas à coleta, armazenamento e processamento de dados pessoais, especialmente quando há a possibilidade de envolvimento de diferentes jurisdições. A harmonização dessas regulamentações e a adoção de medidas adequadas de proteção de dados são elementos essenciais para assegurar a conformidade legal e a segurança dos dados dos usuários.

Portanto, é imprescindível acompanhar regularmente as novas regulamentações internacionais, bem como as aplicações de penalidades e os guias de entendimento, a fim de aprimorar a compreensão da Lei Geral de Proteção de Dados (LGPD) em áreas que ainda apresentam lacunas. Dessa forma, será possível garantir uma abordagem mais coesa e inteligente no tratamento dos dados pessoais, promovendo a efetiva proteção dos direitos dos indivíduos e a conformidade com as normas vigentes.

3.1.5 Lei *Stalking* (Lei N. 14.132/2021)

A terminologia "*stalking*", originária do inglês, refere-se ao ato de perseguir ou aproximar-se de forma furtiva e intencional. Este delito caracteriza-se pela invasão contínua e deliberada da privacidade de um indivíduo, manifestando-se através de coações, monitorizações, ameaças e outras formas de interferência. A natureza persistente dessas ações pode culminar em significativos impactos psicológicos para a vítima, desencadeando sentimentos de medo e constante apreensão[330].

Nas palavras de Jesus, *stalking* refere-se a uma manifestação de violência em que o agressor consistentemente infringe a privacidade da vítima, utilizando uma gama variada de táticas e meios. Estes incluem, mas não se limitam a ligações frequentes, mensagens não desejadas, envio de presentes e flores sem solicitação, subscrições não autorizadas e a presença contínua em locais frequentados pela vítima. O agressor, ou *stalker*, pode ainda difundir rumores sobre a integridade profissional ou moral da vítima, exercendo um controle psicológico sobre ela e ditando suas ações e movimentos[331].

---

[330] WERMUTH, Maiquel Ângelo Dezordi. STALKING E CYBERSTALKING: CONSIDERAÇÕES CRÍTICAS SOBRE O DELITO TIPIFICADO NO ART. 147-A DO CÓDIGO PENAL BRASILEIRO. Revista Brasileira de Ciências Criminais, v. 186, n. 2021, p. 105-126, 2021.

[331] JESUS, Damásio E. de. Stalking. Revista Jus Navigandi, Teresina, ano 13, n. 1655, 12 jan. 2008. Disponível em: https://jus.com.br/artigos/10846. Acesso em: 21 set. 2023.

O *stalking* é conceitualmente categorizado como um crime habitual[332], onde a persistência da conduta é essencial para caracterizar a violação à liberdade individual da vítima. A perpetração deste crime pode manifestar-se através de meios variados, como virtualmente, fisicamente e psicologicamente, de maneiras diretas ou indiretas. O elemento chave é a presença do dolo, ou seja, a consciência e intenção do *stalker* de que suas ações persistentes causam desconforto à vítima. Ao se analisar a natureza dessas ocorrências, é possível segmentar o *stalking* em dois tipos principais: aquele direcionado a pessoas desconhecidas, frequentemente observado com celebridades, e o dirigido a indivíduos conhecidos, como é o caso entre parentes ou vizinhos[333].

Para Aras o *stalking* pode ser categorizado de diversas maneiras, de acordo com a relação entre o *stalker* e sua vítima. Quando oriundo de vínculos familiares ou sentimentais, passados ou atuais, denomina-se afetivo. Já o funcional advém de relações profissionais, comerciais ou acadêmicas. Há ainda a forma idólatra, decorrente de uma admiração obsessiva, típica de fãs em relação a celebridades, líderes políticos e outras figuras públicas. A perseguição pode manifestar-se de forma presencial ou à distância. Enquanto a motivação pode ser por sentimentos como ódio, vingança, inveja, admiração excessiva ou paixão doentia[334].

No Brasil, a Lei nº 14.132/21, que inclui o artigo 147-A no Código Penal Brasileiro que criminaliza a conduta de perseguir alguém, "*stalking"* foi publicada em 21 março de 2021. A lei entrou em vigor no dia 1º de abril de 2021 e, após a sua publicação no Diário Oficial da União e revogou a contravenção penal de perturbação à tranquilidade que estava prevista no artigo 65º do Decreto-Lei nº 3.688/41, que era bastante utilizado até então para punir condutas similares no país[335].

Antes da promulgação da Lei n°14.132/2021, a perseguição era considerada apenas uma contravenção penal e a penalidade para essa infração era relativamente branda. O artigo 65 da

---

[332] O crime habitual é aquele que materializa o modo de vida do infrator, exigindo, para a consumação, a reiteração de condutas, que por sua repetição, caracterizam a ocorrência da infração. TÁVORA, Nestor; ALENCAR, Rodrigues. Curso de Direito Processual Penal. 8 ed. rev. amp. e atual.: Salvador: JusPodivm, 2013.pg569.

[333] SILVA, Nathália Sueli Meneguetti; FLORINDO, Susam Carla Oliveira Dionizio; SACRAMENTO, Karina Adriana. DA (IN) EFETIVIDADE DA APLICAÇÃO DA LEI N° 14.132/2021 NO BRASIL. Facit Business and Technology Journal, v. 2, n. 42, 2023.

[334] ARAS, Vladimir. Blog do Vlad. O crime de stalking do art. 147-A do Código Penal. [2021]. Disponível em: https://vladimiraras.blog/2021/04/01/o-crime-de-stalking-doart- 147-a-do-codigo-penal.

[335] COIADO, Renata; SANI, Ana Isabel. Criminalização do stalking no Brasil. Revista LEX de Criminologia & Vitimologia, v. 3, n. 1, p. 73-102, 2021.

Lei de Contravenções Penais estabelecia apenas que molestar alguém ou perturbar lhe a tranquilidade, intencionalmente ou por motivo reprovável, a pena seria de prisão simples, com duração de quinze dias a dois meses cumulada com multa[336], na legislação vigente a pena varia de 06 meses a 02 anos e multa[337]. O legislador incluiu a figura do *stalking* na Seção I do capítulo VI do Código Penal, que aborda os crimes contra a liberdade pessoal. O bem jurídico protegido por esse crime é a liberdade individual, que engloba o direito de ir, vir e agir. A pessoa perseguida é o objeto material do crime, sendo que o *stalking*, caracterizado como uma perseguição ameaçadora, tem como objetivo atingir um indivíduo específico[338].

Vale observar que a perseguição reiterada pode ocorrer de diversas formas, e no contexto digital geralmente são perpetradas envolvendo redes sociais. Assim, surge o termo "*cyberstalking*" como uma vertente digital do crime de *stalking*, intensificado pela evolução tecnológica e pela utilização massiva da internet[339]. Nesse sentido o *ciberstalking* se caracteriza como um crime cibernético praticado no ambiente digital, frequentemente se materializa através de mensagens via SMS, aplicativos como *WhatsApp e Telegram*, e interações em plataformas sociais como *Instagram e Facebook*[340].

Por ter a característica habitual, para a tipificação do delito de *stalking,* é essencial comprovar a perseguição reiterada por parte do *stalker.* Isso implica que devem existir ações contínuas que restrinjam ou causem desconforto à liberdade ou privacidade da vítima. Se essas ações contínuas não forem verificadas, e não se adequar a outro tipo penal, o ato será considerado atípico[341].

Nesse sentido o delito de *stalking* levanta questionamentos conceituais complexos quanto à distinção entre condutas consideradas normais" e aquelas que caracterizam o crime. Essa demarcação é sutil e depende, em muitos casos, da percepção individual da vítima. Comportamentos potencialmente classificados como *stalking* podem, em certos contextos, serem vistos como normais[342].

---

[336] COIADO, Renata; SANI, Ana Isabel. Op. Cit.

[337] BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Op. Cit.

[338] GENNARINI, Juliana Caramigo. A criminalização do Stalking. Direito Penal e Processo Penal**.** Op. Cit.

[339] GENNARINI, Juliana Caramigo. A criminalização do Stalking. Direito Penal e Processo Penal**.** Op. Cit

[340] *Ibidem*

[341] WERMUTH, Maiquel Ângelo Dezordi. Op. Cit.

[342] SILVA; FLORINDO; SACRAMENTO, Op. Cit.

Entretanto, quando alguns comportamentos reiterados e rejeitados pela vítima, podem configurar intimidação penalmente sancionável. Isso levanta questões sobre quais características definem uma ação como perseguição e se essa avaliação deveria ser baseada em critérios subjetivos, centrados na experiência da vítima. O art. 147-A do Código Penal brasileiro estabelece a reiteração como elemento do crime, gerando debates sobre, por exemplo, quantas mensagens reiteradas seriam necessárias para se enquadrar no tipo penal, e como diferenciar o *stalking* de outros delitos, como o de ameaça previsto no art. 147 do mesmo Código[343].

Nota-se que existem uma série de dificuldades na aplicação da lei de stalking, há também a necessidade de representação da vítima, conforme estipulado no § 3º do artigo 147º do Código Penal. Assim, para que o Ministério Público inicie uma ação, é imprescindível o consentimento da vítima, sob risco de rejeição da denúncia, conforme o artigo 395º, II, do Código de Processo Penal. Em relação aos delitos cibernéticos, a investigação se torna ainda mais complexa, dada a natureza intangível das evidências e desafios na localização do autor do crime[344].

Um estudo do *Bureau of Justice Statistics* dos Estados Unidos, conduzido por Truman e Morgan, revelou que, em 2016, 3,8 milhões de indivíduos com 16 anos ou mais foram vítimas de *stalking*, com tecnologia sendo frequentemente utilizada como meio. O levantamento mostrou que mulheres foram vítimas mais que o dobro em relação aos homens, sendo mais propensas a serem perseguidas por ex-parceiros. Além disso, 24% das vítimas relataram perseguições durando dois anos ou mais, com 10% indicando ocorrências tão frequentes que não puderam ser quantificadas[345].

No Brasil, de acordo com o anuário da Segurança Pública Brasileira, só em 2022, foram mais de 27,7 mil ocorrências registradas de *stalking.* Após a oficialização desta tipificação criminal, houve um notório aumento desses casos, concentrados majoritariamente nas

---

[343] *Ibidem.*

[344] SILVA; FLORINDO; SACRAMENTO, Op. Cit.

[345] TRUMAN, Jennifer L.; MORGAN, Rachel E. Stalking Victimization, 2016. U.S. Departmentof Justice, 2021. Disponível em: [https://www.bjs.gov/content/pub/pdf/sv16.pdf].STALKING E CYBERSTALKING: CONSIDERAÇÕES CRÍTICAS SOBRE O DELITO TIPIFICADO NO ART. 147-A DO CÓDIGO PENAL BRASILEIRO. Pg. 14 Acesso em: 21.09.23.

principais capitais. Entretanto, o Fórum de Segurança Pública enfatiza que, devido à ausência de levantamentos em alguns Estados, o número real pode superar os registros disponíveis[346].

Esses dados foram coletados a partir de um estudo empírico nas instâncias judiciais brasileiras, abrangendo o período de 2015 a 2020, antecedente à criminalização do *stalking* no país, revelou que 84,22% dos casos estão relacionados ao contexto doméstico, frequentemente associados a desavenças por términos de relacionamentos. Nesse cenário, destaca-se a prevalência de vítimas femininas enfrentando formas específicas de violência, majoritariamente decorrentes da não aceitação do fim do relacionamento. Adicionalmente, observou-se uma perspectiva de gênero, já reconhecida socialmente, na qual tais comportamentos de perseguição frequentemente envolvem ex-parceiros [347].

Vale observar ainda a análise feita por Aras sobre o art. 7º da Lei Maria da Penha que fornece uma interpretação essencial para a compreensão da recente tipificação delitiva sobre a majorante delineada no inciso II do §1º do art. 147-A do CP, estabelecendo que a agravante se aplica especialmente em contextos em que o crime ocorre em virtude da condição de gênero da vítima, sobretudo em cenários de violência doméstica e familiar. Esta majorante é especialmente relevante quando o *stalker* possui relações prévias com a vítima, como ex-cônjuge ou ex-companheiro(a), ou em situações que refletem atitudes de menosprezo ou discriminação baseadas no gênero feminino, configurando misoginia[348].

Muito embora o a lei de *stalking* seja um avanço legislativo, ainda há a necessidade de aprimoramentos para garantir uma proteção mais severa às vítimas e proporcionar medidas educativas aos infratores, conscientizando-os sobre a seriedade de suas ações. Além disso, ao analisar a proteção concedida às vítimas, observa-se a ausência de disposições sobre medidas protetivas imediatas durante o trâmite processual, um diferencial presente em legislações internacionais, como a de Portugal[349], e na própria Lei Maria da Penha no contexto de violência

---

[346] FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. Anuário Brasileiro de Segurança Pública. Dados estatísticos. Atualizado em: 22/08/2022. Disponível em: https://forumseguranca.org.br/anuario-brasileiro-seguranca-publica/ Acesso em 22 set 2023.

[347] COIADO, Renata; SANI, Ana Isabel. Op. Cit.

[348] ARAS, Vladimir. Op. Cit.

[349] Em Portugal, a criminalização ocorreu em 2015. Comete o delito de perseguição quem, "de modo reiterado, perseguir ou assediar outra pessoa, por qualquer meio, direta ou indiretamente, de forma adequada a provocar-lhe medo ou inquietação ou a prejudicar a sua liberdade de determinação". O agente é punido com pena de prisão até 3 anos ou pena de multa, "se pena mais grave não lhe couber por força de outra disposição legal". Diz a lei portuguesa que pode ser aplicada ao réu as penas acessórias de proibição de contato com a vítima pelo período de 6 meses a 3 anos e de obrigação de frequência a programas específicos de prevenção de condutas típicas da perseguição. Esta medida "deve incluir o afastamento da residência ou do local de trabalho" da vítima e o seu

doméstica. Embora a legislação tenha intensificado a esfera punitiva, equiparando-se a normativas internacionais, é importante refletir sobre possíveis revisões que enfatizem tanto aspectos protetivos quanto educativos para assegurar uma efetividade mais abrangente[350].

Nos casos de perseguição no ambiente virtual, os desafios são ainda maiores devido às barreiras geográficas que transcendem as fronteiras nacionais, exigindo esforços acrescidos no compartilhamento de informações e na cooperação internacional. Além disso, é fundamental reconhecer as habilidades dos cibercriminosos, que parecem estar sempre um passo à frente da lei, prejudicando qualquer tentativa de os identificar. Neste contexto, destaca-se a importância da adesão do Brasil à convenção de Budapeste, que será analisada no próximo capítulo, que se mostra acertada sendo uma medida essencial para reforçar a resposta jurídica ao c*yberstalking* e garantir a segurança no ambiente virtual em especial para as mulheres que são as maiores vítimas dessa modalidade de crime cibernético.

3.1.6 Lei 14.155/2021

A Lei 12.737 analisada anteriormente, introduziu no Código Penal brasileiro a tipificação da conduta de invasão de dispositivos informáticos com o intuito de acessar, alterar ou destruir dados sem autorização do usuário. Nesse contexto, no dia 27 de maio de 2021, o presidente da república sancionou a Lei 14.155/2021[351] que altera o Código Penal tornando mais rigorosa a punição para os crimes de violação de dispositivo informático, furto e estelionato cometidos pela internet ou por meio de dispositivos eletrônicos. Enquanto anteriormente a pena prevista era de detenção de 3 meses a 1 ano, além de multa, a nova legislação estabelece uma pena mais rigorosa de 1 a 4 anos de reclusão, acrescida da aplicação de multa[352].

Art 154-A Código Penal Anteriormente[353]	Art. 154-A após alteração promovida pela Lei 14.155/2021[354]

cumprimento “deve ser fiscalizado por meios técnicos de controle à distância. ARAS, Vladimir. Blog do Vlad. O crime de stalking do art. 147-A do Código Penal. [2021]. Disponível em: https://vladimiraras.blog/2021/04/01/o-crime-de-stalking-doart- 147-a-do-codigo-penal.

[350] COIADO, Renata; SANI, Ana Isabel. Op. Cit.

[351] BRASI. 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.

[352] BRASI. Lei 14.155.*Op. cit.*

[353] BRASIL. Código Penal. Op. Cit.

[354] BRASI. Lei 14.155, de 27 de maio de 2021. Op. Cit.

Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: **Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.**	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.**
§ 1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.	§ 1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
§ 2o Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.	§ 2o Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.
§ 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.	§ 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.
§ 4o Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.	§ 4o Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
§ 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra: I – Presidente da República, governadores e prefeitos; II – Presidente do Supremo Tribunal Federal; III – Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV – Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.	§ 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra: I – Presidente da República, governadores e prefeitos; II – Presidente do Supremo Tribunal Federal; III – Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV – Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Tabela 05

Segundo a legislação vigente, é considerado invasão de dispositivo informático o ato de acessar um dispositivo alheio, conectado ou não à rede de computadores, com o objetivo de obter, adulterar ou destruir dados ou informações sem a autorização expressa ou tácita do usuário do dispositivo, ou de instalar vulnerabilidades visando obter vantagem ilícita. O objeto jurídico do crime, como se percebe, é a privacidade individual e profissional que contêm dados armazenados em dispositivos informáticos[355]. A tipificação do crime é mais uma forma de assegurar o direito fundamental previsto na Constituição Federal, no art. 5º, inciso X, que prevê a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas, assegurando-se o direito de indenização pelo dano decorrente de sua violação[356].

A descrição inicial da conduta do art. 154-A, antes da promulgação da nova lei, foi alvo de críticas por parte de juristas devido à sua falta de completude na tipificação do crime. Para Rogério Sanches Cunha, a falta de previsão para casos de excesso na prática do crime, ou seja, quando o agente ultrapassa os limites da autorização concedida para acessar o dispositivo. Um exemplo seria quando o proprietário do dispositivo autoriza um técnico a acessar uma pasta com fotografias, mas o técnico vai além e obtém outras informações armazenadas no dispositivo. Nesses casos, não há configuração do crime, uma vez que essa conduta não está abrangida no tipo penal, que pressupõe a violação do dispositivo[357].

Nesse sentido, embora a nova redação tenha solucionado um dos principais problemas de interpretação, ainda persistem algumas questões em aberto. Uma dessas críticas diz respeito ao fato de que o legislador estabeleceu a conduta criminosa como sendo a invasão não autorizada do dispositivo, mas não abordou especificamente as informações contidas nele. Dessa forma, em situações em que mais de uma pessoa utiliza o dispositivo, por exemplo, os dados ali presentes ficam sujeitos à autorização do verdadeiro proprietário do aparelho[358].

Ademais, antes da modificação do texto normativo, os dispositivos informáticos desprovidos de mecanismos de segurança não podiam ser objeto material das condutas criminosas descritas, uma vez que o delito exigia a "violação indevida de mecanismo de segurança". Dessa forma, invadir ou instalar vulnerabilidades em dispositivos que não possuíam mecanismos de segurança, como senhas, por exemplo, não configuraria o crime previsto no art.

---

[355] BRASIL. Constituição Federal, 1988. Op. Cit.

[356] BRASIL. Código Penal. Op. Cit.

[357] CUNHA, Rogério Sanches, Manual de Direito Penal: Parte Especial. Op. Cit. Pg. 136.

[358] CUNHA, Rogério Sanches, Manual de Direito Penal: Parte Especial (arts. 121 ao 361). 11. ed. Salvador: JusPODIVM, 2019. Pg. 136.

154-A[359]. Essa situação e interpretação da norma abriram precedentes para que criminosos pudessem invadir dispositivos desprotegidos por senha e obter, adulterar ou destruir dados sem sofrer punição estatal. Felizmente, com a recente alteração trazida pela Lei nº 14.155/2021, o trecho que exigia a presença de mecanismos de segurança para a configuração do crime foi removido, permitindo que dispositivos desprotegidos por senha também sejam abarcados pela norma legal[360].

Outra alteração feita pela Lei diz respeito ao artigo 155º do Código Penal, introduzindo o parágrafo 4º-B a redação de furto mediante fraude quando cometido por meio de dispositivo eletrônico ou informático conectado ou não a uma rede de computadores, com ou sem a violação de mecanismos de segurança, utilização de programa malicioso ou qualquer outro meio fraudulento semelhante, a pena é de reclusão de 4 (quatro) a 8 (oito) anos e multa[361].

Para Cunha, dispositivo eletrônico ou informático refere-se a qualquer equipamento capaz de armazenar e processar informações, como computadores e smartphones. O dispositivo legal ressalta que não importa se o aparelho está conectado a redes, como intranet ou internet. Independentemente da técnica utilizada na fraude - seja violação de segurança, uso de arquivos maliciosos ou obtenção de senha - qualquer ação fraudulenta que resulte em subtração mediante dispositivo eletrônico é qualificada. É crucial diferenciar que o foco aqui é a distração da vítima para facilitar a subtração, e não induzir alguém a entregar um bem voluntariamente, o que configura estelionato[362].

Ainda nas alterações feitas no artigo 155º Código Penal, foi inserido o parágrafo 4º-C que dispõe de situações que aumentam a pena se o crime utilizar servidor estrangeiro ou se é dirigido contra idosos, definidos como indivíduos com 60 anos ou mais, segundo o que dispõe o art. 1º da Lei 10.741/03, ou vulneráveis no contexto do furto, considera-se a definição presente no art. 217-A, incluindo menores de 14 anos ou indivíduos com limitações mentais[363].

É fundamental destacar que a elevação da pena, conforme descrito no parágrafo 4º-C, exige que o autor esteja ciente das circunstâncias específicas de sua ação. Assim, para que haja

---

[359] CAPEZ, Fernando; PRADO, Stela. Código Penal Comentado. 5. ed. São Paulo: Saraiva, p. 347, 2014.

[360] CAPEZ, Fernando; PRADO, Stela. Código Penal Comentado. 5. ed. São Paulo: Saraiva, p. 347, 2014.

[361] CUNHA. Op. Cit.

[362] CUNHA. Op. Cit.

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

a majoração, o infrator precisa ter conhecimento da conexão internacional empregada ou estar ciente de que sua vítima é idosa ou vulnerável. No contexto dos crimes cibernéticos, essa consciência nem sempre é evidente, visto que, em diversas situações, o criminoso não mantém qualquer forma de contato com a vítima[364].

O artigo 171º do Código Penal, passou a contar com a qualificadora semelhante à inserida no crime de furto. Diferentemente do furto, onde a subtração ocorre frequentemente de maneira imperceptível à vítima através da invasão de um dispositivo eletrônico, no estelionato, a questão central é a indução ao erro. Neste último delito, a legislação ressalta o agravamento da conduta nas situações em que a vantagem é obtida por meio de: a) Anúncios em redes sociais, frequentemente fraudulentos; b) Contatos telefônicos, como o envio de mensagens em que o fraudador se passa por conhecido da vítima solicitando transferências bancárias; c) Correios eletrônicos enganosos, que simulam comunicações de entidades reconhecidas, levando a vítima a inserir informações sensíveis; d) Quaisquer outros mecanismos fraudulentos análogos em ambientes digitais, incluindo websites simulados.

Cunha exemplifica a primeira situação (furto) no caso de um hacker que intercepta dados em uma rede pública para efetuar transferências bancárias sem o consentimento da vítima. No segundo (estelionato), uma pessoa poderia ser induzida a comprar um produto em uma página falsa, que imita um varejista confiável, efetuando um pagamento por um item que nunca será entregue. Neste contexto, o que distingue ambos os crimes é a participação ativa da vítima no estelionato, fornecendo informações sob a influência de um ardil, enquanto no furto, a vítima geralmente é despojada de seus bens sem perceber[365].

A Lei nº 14.555/2021 traz à tona debates sobre a proporcionalidade das penas em crimes digitais, visto que, em algumas situações, as punições são mais rigorosas do que para delitos que impactam diretamente a vida ou saúde. Essa complexidade evidencia o desafio legislativo de equilibrar a punição de infrações digitais com a coerência do sistema penal[366].

Em suma, a Lei nº 14.555/2021 representa um importante avanço na legislação penal e processual penal brasileira, uma vez que estabelece penalidades mais severas e esclarece a jurisdição para crimes cometidos eletronicamente. Além disso, a lei amplia o escopo de certos

---

[364] *Ibidem.*

[365] CUNHA, Rogério Sanches. Lei 14.155/21 e os crimes de fraude digital: primeiras impressões e reflexos no CP e no CPP.Op. Cit.

[366] 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.

crimes, como invasão de dispositivos informáticos e estelionato eletrônico, em resposta às mudanças tecnológicas e sociais que aumentaram a ocorrência desses delitos.

No entanto, ainda há discussões em torno de certos aspectos da lei, como a determinação da jurisdição com base no domicílio da vítima, o que pode dificultar a eficiência das investigações e do processo penal. Portanto, é crucial continuar revisando e aprimorando a legislação para garantir uma resposta adequada e justa aos crimes cibernéticos e suas condutas, levando em consideração as complexidades inerentes a esses tipos de delitos[367].

3.2 Desafios e lacunas na legislação penal

3.2.1Deficiência da Lei tipificadora

O Avanço do processo de informatização e da sociedade em rede já analisados nessa pesquisa trouxe profundas evoluções no campo jurídico, acelerando transformações e exigindo adaptações. Entretanto, apesar desses vários progressos a revolução informática também exerceu forte influência no campo do Direito Penal, mudando não só a forma de cometimento dos crimes já previsto na legislação como também inaugurando novas figuras delitivas e novos bens jurídicos ameaçados.

De acordo com Damásio e Milagres, existe a corrente doutrinária que defende o direito penal mínimo que justifica a não necessidade de legislação adicional, argumentando que 95% dos crimes cibernéticos já estão contemplados no Código Penal Brasileiro[368]. Para Daoun, a ênfase principal é a desnecessidade de uma nova legislação penal, considerando que o Direito Penal para as relações virtuais deve ser mínimo. Recomenda-se utilizar o Direito Penal apenas em situações extremas, enquanto outras áreas do direito devem ser empregadas para coibir práticas no ambiente virtual[369].

Dessa forma o Direito Penal seria uma medida mais drástica, usando como analogia a situação fática em que pagar uma indenização é diferente de perder a liberdade. Portanto, para preservar a liberdade, é necessário adotar um direito penal mínimo, visto que no panorama virtual, 95% das relações já são regulamentadas, o que torna desnecessária a criação excessiva de legislação penal específica[370].

---

[367] *Ibidem.*

[368] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 92.

[369] DAOUN, Alexandre Jean. Crimes informáticos. In: Blum, Renato M. S. Opice (coord). Direito Eletrônico: a internet e os tribunais. Baruru: Edirpo, 2001. Pg. 21.

[370] JESUS, Damásio de. MILAGRE, José Antônio. Op. Cit, pg. 94.

Nota-se que é evidente que a cibercriminalidade trouxe novas formas de cometer crimes já conhecidos. A ameaça continua e continuará sendo ameaça e a difamação continuará sendo difamação, independentemente de serem praticadas por meio de dispositivos informáticos ou não. No entanto, é igualmente inegável que os crimes cibernéticos atualmente afetam bens jurídicos que não são protegidos pelo Direito Penal. A necessidade de enquadramento sempre foi objeto de debate entre os profissionais do Direito Penal, especialmente no que diz respeito à criação de leis específicas ou à adaptação da legislação existente[371]

Por outro lado, Alves argumenta que embora muitos ainda considerem a internet como um território livre e impune, isso não é a realidade brasileira. Diariamente, o sistema judiciário tem buscado combater a sensação de impunidade no meio digital e enfrentar a criminalidade por meio da aplicação das leis penais e de legislações específicas. Embora nem todas as condutas estejam devidamente codificadas, elas estão sendo adaptadas de forma pontual à legislação existente. As questões jurídicas decorrentes do aumento do uso da tecnologia da informação são claramente complexas e não podem ser abordadas apenas por meio da criminalização de determinados comportamentos. É necessário revisar a legislação nacional não apenas no âmbito penal, mas de forma conjunta e colaborativa[372].

Além disso, é possível observar que o Estado tem avançado ao prever algumas condutas criminosas, embora ainda haja muito a ser feito em relação à efetiva proteção penal no ambiente digital. A falta de disposições claras no ordenamento jurídico acaba agravando as dificuldades já existentes para a investigação dos crimes digitais, especialmente no que diz respeito aos sujeitos, às provas, ao tempo e ao local do crime, que se tornam ainda mais complexos quando se trata dessa modalidade delitiva[373].

Nesse contexto, é evidente que o Código Penal brasileiro, estabelecido em 1940, revela-se inadequado para lidar com os diversos comportamentos criminosos contemporâneos, especialmente os relacionados à cibercriminalidade. Os crimes cometidos por meio da internet, embora já estejam tipificados, são perpetrados de maneiras inovadoras e prejudiciais, o que dificulta a aplicação efetiva da legislação atual[374].

---

[371] Ibidem.

[372] DE ARAÚJO ALVES, Matheus.Crimes Digitais: análise da criminalidade digital sob a perspectiva do Direito Processual Penal e do Instituto da Prova. Editora Dialética, 2020. pg 1824.

[373] *Ibidem.*

[374] *Ibidem.*

Um exemplo dessa deficiência no ordenamento jurídico são os ataques distribuídos de negação de serviço, ou simplesmente *DDoS*, uma técnica maliciosa pela qual o agente utiliza equipamentos conectados à rede, de forma coordenada e distribuída, para deixar um serviço computador ou rede inoperante, o objetivo direto do *DDoS* não é invadir nem coletar informações, mas sim de exaurir recursos e causar indisponibilidade do alvo[375].

Nota-se que esses ataques revelam uma falha na legislação pois não há tipificação que enquadre a conduta descrita. A lei 12.737/2012, em seu artigo 3º descreve que incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. Contudo, o dispositivo se mostra insuficiente uma vez que faltam elementos normativos do tipo: Serviço telemático e informação de utilidade pública" pois não alcança o ataque a um website privado pois assim não é definido[376].

Em suma o ordenamento jurídico brasileiro em relação aos crimes cibernéticos no país está longe de ser satisfatória, o Código Penal brasileiro, estabelecido em 1940, revela-se inadequado para lidar com os diversos comportamentos criminosos contemporâneos, especialmente os relacionados à cibercriminalidade. Os crimes cometidos por meio da internet, embora alguns já estejam tipificados, são perpetrados de maneiras inovadoras e prejudiciais, o que dificulta a aplicação efetiva da legislação atual.

Diante dessa realidade, é imprescindível que o Brasil adote de forma mais célere uma legislação sólida e especializada, voltada especificamente para a cibercriminalidade, levando em consideração a singularidade desses delitos e adaptando-se às suas características em constante evolução.

3.2.2 Necessidade de perícias especializadas

Todo esse cenário da sociedade em rede e a revolução tecnológica trouxe o aumento da utilização de computadores para a prática de crimes, o que ensejou a necessidade de apuração das provas nesses dispositivos. Nesse sentindo surge a importância da comutação forense, cujo

---

[375] CERT.BR, Centro de estudos, resposta e tratamentos de incidentes de segurança no brasil, cartilha de segurança para internet: Ransomware. Disponível em: https://www.cert.br/

[376] BORTOT, Jessica Fagundes. Crimes cibernéticos: aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional. **Virtuajus**, v. 2, n. 2, p. 338-362, 2017.

objetivo é a investigação e coleta de evidências das condutas ilícitas praticadas por meio de dispositivos eletrônicos[377].

Toda investigação tem seu início fundamentado em evidências e informações coletadas, e esse princípio se aplica tanto ao meio físico quanto ao virtual. No contexto dos crimes cibernéticos, as evidências podem ser obtidas a partir de dispositivos eletrônicos, como celulares e discos rígidos. Nesse sentido, a evidência digital pode ser definida como qualquer informação extraída de um repositório eletrônico, seja por intervenção humana ou não, e que esteja em um formato compreensível para os seres humano[378].

Nas investigações relacionadas aos crimes cibernéticos, devido à natureza volátil dos dados e à facilidade de adulteração, é necessário realizar perícias técnicas rigorosas nas provas eletrônicas para que sejam aceitas em processos legais, a fim de assegurar a validade e integridade dos resultados. O objetivo da computação forense é fornecer evidências claras e irrefutáveis dos eventos ocorridos[379].

A computação forense é uma disciplina científica que tem como objetivo esclarecer os fatos por meio da aplicação de métodos científicos na coleta, validação e identificação de evidências digitais, visando a punição dos infratores. Seu propósito é extrair o máximo de informações durante a análise dos vestígios relacionados ao delito cometido, a fim de formular conclusões sólidas. Seu objetivo principal é coletar evidências digitais para chegar a conclusões sobre casos investigados. Por meio da reconstituição dos eventos encontrados, é possível determinar se o computador em análise foi utilizado para a realização de condutas ilícitas ou não autorizadas[380].

Nesse sentido a computação forense se demonstra essencial para a investigação dos crimes cibernéticos, pois são caracterizados por desafios significativos em relação à sua comprovação. Embora a prática desses delitos por meio de computadores seja relativamente

---

[377] RODRIGUES, Thalita Scharr; FOLTRAN JUNIOR, Dierone César. Análise de ferramentas forenses nainvestigação digital. 2010. Disponível em: <http://www.revistaret.com.br/ojs2.2.3/index.php/ret/article/viewFile/64/93>. Acesso em: 20 ago. 2023

[378] PINHEIRO, Patrícia Peck. Direito Digital. São Paulo: Editora Saraiva, 2013, p. 216.

[379] PEREIRA, Evandro della Vecchia. Investigação Digital: conceitos, ferramentas e estudos de caso. 2010.Disponível em: <http://www.infobrasil.inf.br/userfiles/26-05-S5-2-68766-Investigacao Digital.pdf>. Acesso em:20 ago. 2023

[380] RODRIGUES, Thalita Scharr; FOLTRAN JUNIOR, Dierone César. Análise de ferramentas forenses nainvestigação digital. 2010. Disponível em: <http://www.revistaret.com.br/ojs2.2.3/index.php/ret/article/viewFile/64/93>. Acesso em: 20 ago. 2023.

fácil, a verificação dos vestígios deixados exige uma qualificação técnica específica, que nem sempre está disponível em todos os locais onde os crimes são cometidos[381].

A vulnerabilidade da modificação de documentos digitais requer a designação de um perito tecnicamente qualificado para atestar a autenticidade do documento. Embora a computação forense seja precisa, a coleta de evidências pode se tornar frágil. Quando realizada de forma incorreta, violando disposições legais ou princípios constitucionais, isso pode tornar a prova ilícita ou inválida[382].

A produção de prova ilícita pode acarretar sérios prejuízos ao processo, uma vez que esse tipo de prova contamina todas as demais provas decorrentes dela. De acordo com a teoria dos frutos da árvore envenenada, os efeitos da ilicitude podem se estender além da prova viciada, contaminando todo o material subsequente. Portanto, todas as provas que derivam de uma prova ilícita devem ser excluídas do processo, conforme estabelecido no artigo 157º do Código de Processo Penal[383], que determina a inadmissibilidade e a necessidade de desentranhamento das provas ilícitas, entendidas como aquelas obtidas em violação a normas constitucionais ou legais[384].

Devido à minuciosidade exigida pela perícia nos crimes cibernéticos, um dos principais desafios jurídicos relacionados à produção de provas é a falta de preparo da polícia investigativa e dos peritos. Há uma escassez de profissionais capacitados nesse tipo de investigação, o que ressalta a necessidade de especialização e treinamento rigoroso para lidar com a perícia voltada para crimes digitais. Essa capacitação é fundamental para atender às exigências técnicas de coleta e preservação de evidências, a fim de evitar questionamentos futuros sobre a autenticidade da prova e a legalidade de sua obtenção[385].

No contexto da investigação policial e elaboração do laudo pericial, a competência do investigador ou perito desempenha um papel crucial na obtenção de provas bem-sucedidas. É fundamental que esses profissionais estejam devidamente capacitados e treinados para utilizar

---

[381] LIMA, Paulo Marco Ferreira. Crimes de Computador e Segurança Computacional. São Paulo: Editora Atlas,2011. p. 15.

[382] PINHEIRO, Patrícia Peck. Direito Digital. São Paulo: Editora Saraiva, 2013, p. 234.

[383] BRASIL. Decreto-Lei no 3.689, de 3 de outubro de 1941. Código de Processo Penal. Op. Cit.

[384] TAVORA, Nestor; ALENCAR, Rosmar Rodrigues. Curso de Direito Processual Penal. Salvador: Jus Podivm, 2012. p. 383

[385] COLLI, Maciel. Cibercrimes. Limites e perspectivas à investigação policial de crimes cibernéticos. Curitiba: Juruá Editora, 2010. P. 160

as tecnologias mais avançadas, a fim de identificar os indícios que permitirão a coleta de provas, bem como a preservação adequada do local e dos instrumentos e objetos utilizados na prática do ato ilícito[386].

Com o objetivo de conferir legitimidade às provas obtidas em casos de crimes virtuais, a investigação criminal e a instrução processual requerem a adoção de procedimentos técnicos. Especialistas em hardware, software, tráfego e segurança de rede desempenham exames periciais para determinar a veracidade dos fatos. A eficácia da investigação criminal depende da atuação desses peritos na análise do ambiente onde o crime foi cometido e na confirmação dos fatos.

Ao analisar o ambiente em que o delito ocorreu, os profissionais podem identificar vestígios das atividades criminosas. Roberto Antônio Malaquias, ao considerar o envio de um e-mail não autorizado, exemplifica vestígios que podem indicar a prática do crime, como a identificação da origem do e-mail, sua autoria, destinatário, adulteração, rota utilizada para chegar ao destino, endereços virtuais e protocolos de comunicação envolvidos, que permitem rastrear o percurso da mensagem na rede de computadores. Nesse exemplo, a identificação do e-mail, objeto da investigação criminal e produção de provas, juntamente com todos os seus componentes, funciona como um rastreador para identificar a máquina que originou a mensagem, servindo como prova documental[387].

A complexidade de produzir provas no cenário virtual se mostra ainda mais difícil quando necessária a identificação do computador de origem de uma conduta ilícita. De acordo com Peck, no âmbito do Direito Digital, a identificação de um computador é realizada por meio do endereço IP (Protocolo de Internet). Cada usuário ou internauta recebe um número IP sempre que estabelece uma conexão com a rede mundial de computadores. Além de possibilitar a identificação virtual, o IP registra todo o tráfego de rede e os acessos realizados pelo usuário. Uma vez identificado o IP, são analisadas possíveis evidências da prática do delito. Essa análise, conduzida por peritos especializados, é uma atividade extremamente complexa, especialmente considerando a existência de programas de computador que visam ocultar a verdadeira identidade do autor, principalmente quando os computadores estão localizados em locais e redes públicas[388].

---

[386] MALAQUIAS, Roberto Antônio Darós. Crime Cibernético e Prova – A investigação criminal em busca da verdade. Curitiba: Juruá Editora, 2012. p. 65.

[387] MALAQUIAS, Roberto Antônio Darós. Op. Cit. Pg80.

[388] PINHEIRO, Patrícia Peck. Direito Digital. Op. Cit 242.

Este cenário demonstra a necessidade de especialização dos profissionais envolvidos na investigação de crimes digitais, Colli sugere que uma possível solução para a resolução de questões relacionadas aos crimes cibernéticos seria a criação de divisões especializadas em computadores, mídias e meios de comunicação. Isso se deve à velocidade e constante evolução desses crimes, bem como à violação de um bem jurídico especial, a informação, o que requer conhecimento específico para identificar os indícios de autoria e materialidade da infração penal[389].

No contexto atual, em que a tecnologia permeia o cotidiano das pessoas e é utilizada para a prática dos crimes cibernéticos é essencial que as delegacias estejam preparadas. Para tanto, têm sido criadas núcleos especializados e profissionais estão sendo treinados para investigar tais crimes. No entanto, a quantidade de especialistas nessa área ainda é insuficiente para lidar com a quantidade de condutas ilícitas que ocorrem diariamente na internet[390].

No Brasil, no âmbito da polícia civil, existem 18 estados que possuem delegacias especializadas na investigação dos crimes cibernéticos [391]. Já no âmbito da polícia federal, atualmente o combate aos crimes cibernéticos é responsabilidade da Unidade Especial de investigação de crimes cibernéticos (UEICC)[392].

Considerando que a sociedade contemporânea depende cada vez mais da tecnologia em seu dia a dia, é imprescindível que haja um número adequado de peritos computacionais capacitados para lidar com os desafios impostos pelos crimes virtuais. Somente assim será possível garantir a efetividade das investigações e a punição dos responsáveis por condutas ilícitas na rede mundial de computadores[393].

3.3.3 Importância da cooperação penal internacional

No âmbito das análises apresentadas até o momento, é possível concluir que o atual momento vivenciado pela maioria das sociedades contemporâneas é caracterizado por uma

---

[389] COLLI, Maciel. Op. Cit. Pg167.

[390] QUEIROZ, Claudemir; VARGAS, Raffael. Investigação e perícia forense computacional. Certificações, Leis processuais e estudos de caso. São Paulo: Brasfort, 2010. p. 10.

[391] DELEGACIAS CIBERCRIMES: crimes na web. CRIMES NA WEB. 2021. Disponível em: https://new.safernet.org.br/content/delegacias-cibercrimes. Acesso em: 02 ago. 2023.

[392] FEDERAL, Polícia. PF lança unidade especial para reprimir crimes cibernéticos: ministério da justiça. Ministério da Justiça. 2022. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2022/06/pf-lanca-unidade-especial-para-reprimir-crimes-ciberneticos. Acesso em: 28 ago. 2023.

[393] QUEIROZ, Claudemir; VARGAS, Raffael. Op. Cit. pg 10.

delicada e significativa transição, resultante principalmente da revolução tecnológica que se manifesta na Sociedade da Informação. Com a ampla disseminação da internet, tornou-se evidente a criação de um novo território, no qual as interações humanas ocorrem de maneiras até então inimagináveis. Essas mudanças ocorreram de forma abrupta e repentina, levando a constatação de que os Estados, em sua maioria, enfrentam imensas dificuldades para exercer sua autoridade jurisdicional e regular as condutas ocorridas no ambiente virtual[394].

Nesse sentido fica clara a importância da cooperação internacional no enfrentamento dos crimes cibernéticos. Este instituto se estabelece como uma ferramenta fundamental para atenuar as complexidades que o ordenamento jurídico brasileiro enfrenta. À medida que a persecução penal desses delitos ultrapassa as fronteiras nacionais e assume uma característica transnacional, a colaboração entre países se torna imperativa. A troca de informações, o compartilhamento de provas e a harmonização das legislações desempenham papéis cruciais na capacitação do Brasil para investigar, processar e punir eficazmente os cibercriminosos.

Observa-se que o ciberespaço é amplamente utilizado por agentes delituosos como um meio vantajoso para a prática de crimes, alguns já previstos na legislação penal, afetando toda a sociedade. Nesse sentido, o ordenamento jurídico brasileiro com a Lei 12.737/2012, LGPD e o Marco civil da Internet, inovam o cenário jurídico penal, atendendo em parte às demandas da comunidade jurídica e da sociedade em geral, que presenciam certas condutas na internet consideradas prejudiciais aos indivíduos, mas que não são devidamente punidas devido à falta de tipificação penal[395].

No entanto, é importante ressaltar que as referidas leis não têm o poder de eliminar completamente os crimes cometidos na internet. Isso ocorre porque vivemos em um mundo em constante evolução tecnológica, e o Código Penal consegue acompanhar prontamente o surgimento de novas condutas prejudiciais aos bens considerados relevantes para uma sociedade moderna, isso se deve principalmente pela velocidade com que as condutas surgem e a morosidade do legislador.

Além disso, a tipificação dos crimes cibernéticos deve ser tratada em nível internacional, visando uma abordagem unificada e coesa em relação a esses crimes. Nesse contexto, a pesquisa até aqui demonstrou a necessidade premente de o Brasil estabelecer parcerias sólidas com

[394] COLTRO, Rafael Khalil; WALDMAN, Ricardo Libel. Criminalidade digital no Brasil: A problemática e a aplicabilidade da convenção de budapeste. Revista Em Tempo, v. 21, n. 1, p. 104-123, 2021.

[395] ROCHA, Carolina Borges. A evolução criminológica do Direito Penal: Aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012. Jus Navigandi, Teresina, ano, v. 18, 2013.

outros países e organismos internacionais, fortalecendo, assim, sua capacidade de resposta diante dos desafios crescentes apresentados pelos crimes cibernéticos em um mundo cada vez mais interconectado e digitalizado. À luz dessas considerações, o próximo capítulo se concentrará na análise da recente adesão do Brasil na convecção de Budapeste, ocorrida em dezembro de 2021, como uma das soluções proposta para o enfrentamento dos crimes cibernéticos no âmbito da cooperação penal internacional.

4 CONVENÇÃO DE BUDAPESTE E COOPERAÇÃO PENAL INTERNACIONAL

4.1 Visão geral da convenção de Budapeste

O Conselho da Europa, composto por 46 países, é a principal organização de defesa dos direitos humanos no continente[396]. Sua larga experiência e tradição na celebração de instrumentos multilaterais sobre cooperação internacional desempenhou um papel fundamental na promoção da modernização da legislação penal e processual penal dos Estados-membros, com o objetivo de combater a cibercriminalidade. Através do Conselho da Europa, foram realizados conferências, debates e estudos sobre o tema, visando encontrar soluções legais para as atividades potencialmente criminosas que surgiram com o avanço das tecnologias de informática, telecomunicações e telemática[397].

Cientes da realidade da cibercriminalidade, o conselho da Europa criou algumas recomendações acerca dos perigos da criminalidade no ambiente digital, bem como medidas legais para investigação desses delitos. Essas Recomendações abordavam aspectos normativos e forneciam orientações para a criação de crimes específicos, instrumentos legais de investigação e mecanismos genéricos de cooperação. Nota-se que no ordenamento jurídico

[396] EUROPE, Council Of. CONSELHO DA EUROPA: quem somos. QUEM SOMOS. 2023. Disponível em: https://www.coe.int/pt/web/about-us/who-we-are. Acesso em: 28 ago. 2023.

[397] BARBAGALO, Fernando Brandini. Cibercriminalidade e crimes informáticos: uma aproximação entre a legislação italiana e brasileira. Pg05.

comunitário da União Europeia as recomendações não possuem eficácia vinculativa para os países membros, que podem ou não aceitar suas orientações[398].

Nesse sentido a recomendação R-93-13, de 11 de setembro de 1995, adotada pelo Conselho da Europa, apresentava um caráter meramente sugestivo e apresentava uma lista mínima de delitos cometidos no ambiente virtual. Nessa lista, destacava-se a importância da criminalização de condutas como fraude e sabotagem, bem como danos em programas ou dados informáticos. Além disso, a recomendação também mencionava a necessidade de intervenção administrativa em casos de condutas menos graves[399].

A recomendação era que o ato vinculasse todos os países dos integrantes do conselho da Europa e permitisse uma padronização das legislações internas. Nota-se que desde então o Conselho da Europa já demonstrava preocupação com as questões de Direito Penal e processual penal no cenário da virtual, demonstrado pelo seu preâmbulo:

> "ante o notável desenvolvimento da tecnologia da informação e sua aplicação em praticamente todos os setores da sociedade contemporânea, enfatizando os riscos de sua utilização para a prática de crimes e a dificuldade de encontrar e manter as evidências de tais crimes em razão de estarem armazenadas ou mesmo terem sido transmitidas por meios dos sistemas de informação e telemática[400].

Nesse contexto, cientes da potencialidade dos crimes cibernéticos, o Conselho da Europa se dedicou à temática e empreendeu esforços com o objetivo de estabelecer uma política criminal comum voltada para a proteção da sociedade contra a criminalidade digital, por meio da adoção de legislação adequada e do fomento à cooperação internacional. O objetivo era definir um ambiente compartilhado, utilizado por todos aqueles que acessam a internet e se conectam aos serviços de comunicação e informação, buscando conciliar a proteção jurídica com a soberania dos países membros.[401]

Os primeiros trabalhos para a formulação do texto da convenção de Budapeste foram realizados pelo Comitê de Peritos em Crimes no Ciberespaço. O comitê foi criado pelos Ministros do Conselho da Europa em 4 de fevereiro de 1997, num esforço conjunto de 04 anos,

---

[398] *Ibidem*

[399] *Ibidem*

[400] Disponível em < https://rm.coe.int/16804f6e76 > Acesso em 10 de fevereiro de 2022.

[401] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. Revista Brasileira de Ciências Criminais. São Paulo: Revista dos Tribunais, 2004. p. 170.

até sua finalização em 2001. Após a realização de diversas sessões, reuniões e encontros adicionais, o projeto de lei foi apresentado aos ministros que solicitaram sua elaboração. Após a revisão da versão final, o projeto foi submetido ao comitê de especialistas em ciberespaço, em seguida foi encaminhado ao comitê de ministros para adoção e posteriormente enviado aos países membros para que firmassem o pacto[402].

Com a participação de Estados-membros do Conselho da Europa e de Estados não-membros, como Estados Unidos, Canadá, Japão e África do Sul, na qualidade de observadores externos, o texto final da convenção e o seu relatório explicativo foram aprovados e adotados pelo comitê de ministros do Conselho da Europa em sua 109ª Sessão, em 8 de novembro de 2001, e a convenção foi aberta à assinatura na cidade de Budapeste, em 23 de novembro de 2001, entrando em vigor em 01 julho de 2004[403].

No Hungria assinaram o Tratado, os países: Albânia, Armênia, Áustria, Bélgica, Bulgária, Croácia, Ilha de Chipre, Estônia, Finlândia, França, Alemanha, Grécia, Hungria, Itália, Letônia, Moldova, Holanda, Noruega, Polônia, Portugal, Romênia, Espanha, Suíça, República Iugoslava da Macedônia, Ucrânia e Inglaterra. De países não-membros do Conselho Europeu, houve a adesão do Canadá, Japão, África do Sul e dos Estados Unidos[404].

Dessa forma, nascia o mais abrangente e avançado instrumento jurídico de cooperação internacional em matéria de crimes cibernéticos, com o propósito de desenvolver uma política criminal unificada para salvaguardar a sociedade diante da criminalidade no ciberespaço. Esse marco enfatiza a importância de uma legislação atualizada e compatível com o constante avanço tecnológico. A convenção de Budapeste é o primeiro acordo internacional a tratar especificamente dos crimes cibernéticos. Seu escopo abrange a segurança de redes de computadores, violações de direitos autorais, fraude por meio de computadores e pornografia infantil[405].

Atualmente a convenção conta com mais 66 países que já assinaram e outros 11 que foram convidados a aderir. Vale ressaltar que até 30 de junho de 2021, 158 Estados utilizaram-

---

[402] BARBAGALO, Fernando. Op. Cit. Pg05

[403] CIBERCRIME, NA CONVENÇÃO SOBRE O. Vladimir Chaves Delgado. 2007. Tese de Doutorado. Centro Universitario de Brasília, pg. 154.

[404] 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: 03 set.2023.

[405] BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. Revista Brasileira de Ciências Criminais. São Paulo: Revista dos Tribunais, 2004, p.167.

no como orientação ou fonte para a sua legislação interna, e até 30 de junho de 2021, cerca de 185 Estados em todo o mundo (96% dos membros da ONU) tinham participado, de uma forma ou de outra, nas atividades do Conselho da Europa sobre o cibercrime[406].

4.1.1 Principais objetivos

No preâmbulo da convenção de Budapeste, o texto já define sua principal característica que é a harmonização das legislações penais, definições das terminologias e outras disposições relacionadas aos crimes cibernéticos. Além disso, as necessárias alterações nas legislações processuais nacionais, a fim de conferir poderes de investigação e persecução criminais adequadas para combater os delitos cometidos por meio de sistemas de computador e outros tipos de delitos nos quais as provas devem ser obtidas por meios eletrônicos, bem como estabelecer um regime de cooperação internacional rápido e efetivo[407].

Sua organização é clara e estratégica, compreendendo quatro capítulos que tratam de maneiras distintas assuntos relacionados a criminalidade virtual. O primeiro capítulo estabelece os significados dos termos utilizados de forma a evitar dúvidas no que se refere a interpretação das suas normas[408].

O segundo capítulo, se divide em três seções, sendo a primeira sobre Direito penal material, subdividindo em quartas subseções. No título I define uma lista de condutas a serem tipificas pelos estados-membros e sus ordenamentos jurídicos internos. O título II define infrações associadas à informática e a aborda os crimes que já estão tipificados nas legislações penais comuns, mas que também podem ser cometidos utilizando-se de computadores. Já no título III trata das infrações relacionadas ao conteúdo, e o título IV sobre as infrações relacionadas com a violação do direito do autor e direitos conexos. Por sua vez o título V versa sobre responsabilidades e sanções [409]. Na seção II, o texto trata do Direito Processual a serem implementados pelos estados-membros com a finalidade de conferir maior eficiência à persecução penal no contexto das investigações e procedimentos internos relativos não apenas as condutas expressas na convenção como também outras relacionadas com sistemas e dados

[406] CONVENÇÃO DE BUDAPESTE. Op. Cit.

[407] CONVENÇÃO DE BUDAPESTE. Op. Cit.

[408] CONVENÇAÕ DE BUDAPESTE. Op. Cit.

[409] CONVENÇÃO DE BUDAPESTE. Op. Cit.

informáticos[410].

O Capítulo III, contempla normas que tratam da cooperação internacional referentes a extradição e auxílio mútuo em matéria penal e se divide em duas seções. A seção um sobre princípios gerais e na seção dois sobre disposições específicas e prevê as formas ou modalidades de auxílio mútuo, definindo normas específicas aplicáveis cada uma delas[411]. Por fim, o capítulo IV contém as denominadas disposições finais que compreendem as já tradicionais cláusulas constantes nas demais convenções adotadas pelo conselho da Europa[412].

Em suma, apesar do seu texto ser sucinto na regulamentação normativa, considera-se como principal aspecto, a política de incentivo à cooperação internacional entre os países signatários com compartilhamento de informações e tecnologias referentes ao combate a cibercriminalidade no cenário mundial.

Nesse sentido a relevância de uma cooperação coordenada no combate ao cibercrime é tão significativa que o Conselho da Europa, instituiu o comitê da convenção sobre crimes cibernéticos (T-CY), responsável por supervisionar a implementação da convenção pelos países que a assinaram. Além disso, foi criado o programa escritório para crimes cibernéticos (C-PROC) em Bucareste, Romênia, com o objetivo de promover o compartilhamento de experiências e o estabelecimento de parcerias entre os profissionais dos países signatários e convidados, facilitando assim a cooperação internacional. O C-PROC também se dedica ao desenvolvimento de programas de capacitação profissional, como o projeto GLACY (Ação Global contra Cibercrimes)[413].

4.1.2 Definições

Com o intuito de padronizar as múltiplas regulamentações em vigor nos diversos Estados envolvidos, a convenção em análise introduziu determinações que versam sobre infrações cometidas no âmbito do ciberespaço e associadas à informática[414]. O termo “sistema informático”, conforme definido pela convenção de Budapeste, refere-se a um conjunto de

[410] DELGADO. Op. Cit, pg154.

[411] *Ibidem.*

[412] *Ibidem*

[413] A Convenção de Budapeste sobre Cibercrime: benefícios e impacto na prática – Relatório do Conselho da Europa – disponível em < https://www.coe.int/en/web/cybercrime/the-budapest-convention > acesso em 10 de setembro de 2023.

[414]CONVENÇAÕ DE BUDAPESTE. Op. Cit.

dispositivos de hardware e software desenvolvidos para o processamento automático de dados. Esses sistemas podem incluir dispositivos de entrada, saída e armazenamento de dados e podem operar de forma independente ou em rede com outros dispositivos semelhantes[415].

Dados informáticos foi definido como qualquer representação de fatos, informações ou conceitos em uma forma adequada para processamento em um sistema informático, incluindo um programa apto a fazer um sistema informático executar uma função. São informações representadas de maneira adequada para serem armazenadas, processadas e transmitidas por sistemas informáticos. Além de armazenar os dados, os sistemas informáticos também são responsáveis por processá-los e transmiti-los para outros sistemas. O processamento de dados envolve um conjunto de procedimentos, instruções ou comandos a serem executados pelo sistema estabelecidos previamente por um programa de computador[416].

Dados de tráfego nos termos da convenção de Budapeste, são aqueles dados relacionados a uma determinada comunicação realizada por meio de um sistema informático, com exceção dos dados relativos ao próprio "conteúdo" da comunicação; isto é, são aqueles dados gerados pelos sistemas informáticos durante o processo de comunicação de outros dados, constituindo apenas elementos auxiliares da comunicação[417].

O termo "provedor de serviços" ou "prestador de serviços" abrange uma ampla categoria de pessoas jurídicas que desempenham um papel específico no que diz respeito à comunicação e ao tratamento de dados em sistemas informáticos e redes de computadores. De acordo com a alínea "c" do artigo 1º da convenção de Budapeste, esse termo inclui entidades, tanto públicas quanto privadas, que fornecem aos usuários a capacidade de se comunicarem entre si. Portanto, é irrelevante se o provedor oferece seus serviços gratuitamente ou mediante pagamento. O termo "provedor de serviços" também se aplica a entidades que armazenam ou tratam dados em função do serviço de comunicação oferecido ou em benefício dos usuários, como provedores de hospedagem ou provedores de conexão a uma rede de comunicação[418].

Em relação ao direito material, o tratado estabelece a tipificação de delitos relacionados aos sistemas e informações computacionais, abordando questões como crimes contra sistemas e dados informáticos, computadores, pornografia infantil e violações de direitos autorais. É

---

[415] *Ibidem.*

[416] DELGADO. Op. Cit.pg154.

[417] DELGADO. Op. Cit.pg154.

[418] *Ibidem.*

relevante ressaltar que a convenção restringe a noção de cibercrime a condutas dolosas, excluindo a consideração de situações culposas. Tal abordagem se justifica pela impraticabilidade de processar e condenar indivíduos que, sem intenção, disseminem malware, como, por exemplo, ao enviar um e-mail infectado, especialmente quando a maioria dos usuários da internet carece de conhecimento técnico para discernir a presença de ameaças virtuais. No âmbito do Direito Processual, a convenção também aborda questões cruciais, como as condições de preservação e conservação de dados, a busca e apreensão, o recolhimento em tempo real de informações computacionais e a interceptação, além de definir competências e estabelecer princípios de cooperação internacional[419].

No que se refere ao âmbito processual, a convenção demonstra a sua abordagem adaptativa às medidas tradicionais de procedimento, como, por exemplo, a busca e apreensão no ambiente eletrônico, e, adicionalmente, introduz um conjunto de novas medidas destinadas a apoiar as investigações, considerando o ambiente virtual dos dados eletrônicos. Nesse sentido, o título 2 do tratado oferece uma compilação de medidas legislativas e outras providências necessárias que os países signatários da convenção devem adotar com o propósito de viabilizar a persecução penal eficaz dos crimes cibernéticos em suas jurisdições[420].

4.2 Mecanismos de cooperação penal previstos na convenção de Budapeste

Com a facilitação do fluxo de informações e comunicações em nível global, as fronteiras físicas deixaram de ser um obstáculo significativo, consequentemente observou-se um crescente desafio no rastreamento e persecução de autores dos crimes cibernéticos, muitas vezes situados em localidades distintas daquelas onde seus atos produzem os efeitos.

No entanto, as legislações nacionais permanecem, em sua maioria, restritas a jurisdições territoriais específicas. Assim, a necessidade de abordar essas questões por meio de instrumentos legais de alcance internacional tornou-se imperativa. A convenção em análise surge como uma resposta a esse desafio, alinhando-se com a preocupação de preservar os direitos humanos em meio à emergente sociedade da informação.

Nesse sentido, os redatores da convenção incluíram um capítulo específico para tratar das questões relativas à cooperação internacional. Dessa forma o capítulo III estabelece três princípios gerais: primeiro no artigo 23º, princípios gerais relativos à cooperação internacional,

[419] DELGADO. Op. Cit.pg155.

[420] DELGADO. Op. Cit.pg154.

no artigo 24º princípios relativos à extradição e nos artigos 25º e 26º, princípios gerais relativos ao auxílio mútuo.

4.2.1 Princípios gerais relativos à cooperação internacional

A Convenção de Budapeste estabelece, em seu artigo 23º, três princípios fundamentais que orientam a cooperação internacional no combate ao cibercrime. O primeiro princípio destaca a ampla colaboração entre as partes signatárias do tratado, promovendo a utilização de instrumentos internacionais pertinentes sobre a cooperação internacional em matéria penal, acordos celebrados com base em legislações uniformes ou recíprocas e o direito nacional de cada Estado. Essa disposição visa agilizar a troca de informações, a coleta de evidências e outras medidas necessárias para enfrentar o cibercrime em uma abordagem global[421].

O segundo princípio concentra-se na cooperação para combater as infrações definidas na própria convenção como crimes informáticos, abrangendo, nesse contexto, a obtenção de provas relacionadas a essas práticas criminosas que afetam sistemas e dados, conforme estabelecido no artigo 14º, parágrafo 2, alíneas "a" e "b," que incluem as infrações delineadas nos artigos 2º a 11º da convenção[422].

Por fim, o terceiro princípio destaca que a aplicação dos instrumentos jurídicos internacionais de cooperação em matéria penal não exclui nem revoga disposições presentes em outros tratados e convenções dos quais o Estado signatário seja parte, notadamente aqueles relacionados à assistência jurídica mútua e extradição. Além disso, essa previsão ressalta a importância de respeitar as disposições do direito nacional que regulam aspectos específicos da cooperação internacional. Esses três princípios, portanto, estabelecem uma base sólida para uma cooperação internacional eficaz na luta contra o cibercrime, promovendo a harmonização das abordagens legais e garantindo o respeito aos direitos e tratados existentes[423].

4.2.2 Princípios relativos à extradição

Para o tratado, o tema da extradição é abordado detalhadamente no artigo 25º e seus subitens, do 1 ao 7. Para que a extradição seja aplicável entre as partes contratantes no contexto das infrações delineadas nos artigos 2º ao 11º, é requerido que a infração seja passível de

[421] CONVENÇAÕ DE BUDAPESTE. Op. Cit.

[422] CONVENÇAÕ DE BUDAPESTE. Op. Cit.

[423] DELGADO. Op. Cit.pg154

punição segundo a legislação de ambos os Estados envolvidos. Além disso, é essencial que a pena máxima prevista seja de privação de liberdade, com duração mínima de um ano. Caso haja discrepância nas penas entre os Estados, será aplicada a penalidade estipulada no tratado ou acordo pertinente, e não na convenção de Budapeste. Portanto, a decisão sobre a possibilidade de extradição dependerá diretamente do período máximo de privação de liberdade estabelecido para a infração em questão, sendo este o cerne do pedido de extradição[424].

É importante observar que a convenção dedica atenção especial à aplicação da extradição no contexto dos delitos elencados no item 1º do artigo 24º, estipulando que tais infrações devem ser passíveis de extradição nos termos de qualquer tratado de extradição existente entre as partes contratantes ou em acordos futuros que possam ser celebrados entre elas. Isso ressalta a relevância da cooperação internacional para a persecução dos crimes cibernéticos, garantindo que o processo de extradição seja eficaz e compatível com os instrumentos jurídicos já existentes ou a serem estabelecidos[425].

Ainda no contexto da extradição, a convenção no seu item 5, estabelece que a parte requerida não possui obrigação de efetuar a extradição caso avalie que os termos especificados em tratados ou legislação aplicável não tenham sido plenamente cumpridos. Isso ressalta a importância do princípio fundamental que rege a cooperação internacional, no sentido de que esta deve ocorrer de acordo com as disposições dos instrumentos internacionais em vigor entre as partes, acordos mútuos preexistentes ou as normativas nacionais vigentes[426].

Já o item sexto da convenção trata de a possibilidade de um Estado recusar a extradição de seus próprios nacionais. Consideremos, por exemplo, a situação em que dois Estados, "A" e "B", ambos signatários da Convenção, estão envolvidos, e um deles solicita a extradição de um nacional do outro estado. Se o Estado requerido recusar esse pedido, argumentando que não extradita seus nacionais ou que possui jurisdição sobre o caso, a convenção de Budapeste prevê uma solução específica. Nesse cenário, o Estado requerente tem a possibilidade de solicitar a abertura de um processo criminal no Estado requerido, a fim de investigar a infração alegada cometida pela pessoa que desejava ser extraditada. Essa disposição visa garantir que um indivíduo não escape da responsabilidade legal simplesmente por ser nacional do Estado

[424] *Ibidem.*

[425] DELGADO. Op. Cit.pg154

[426] CONVENÇAÕ DE BUDAPESTE. Op. Cit

requerido, assegurando que a justiça seja devidamente aplicada em casos de cibercrime, mesmo quando se envolvem nacionais de Estados signatários da convenção[427].

4.2.3 Princípios Gerais relativos ao auxílio mútuo

O auxílio mútuo em matéria de Direito Internacional, conforme sua denominação sugere, desempenha um papel crucial na cooperação conjunta para o enfrentamento da cibercriminalidade. Essa colaboração se traduz, efetivamente, em assistência mútua, tal como evidenciado no artigo 25º da convenção de Budapeste. Neste dispositivo, a convenção estipula que os Estados partes, ou seja, aqueles que a ela aderiram, estão aptos a colaborar de forma ampla e abrangente, especialmente em investigações e procedimentos relacionados a crimes que afetam sistemas e dados informáticos. Além disso, destaca-se a relevância desse auxílio mútuo na fase de coleta de provas durante investigações criminais[428].

É digno de nota que, conforme delineado nos itens 1 e 2 do artigo 25º, a convenção permite a integração das disposições constantes nos artigos 27º a 35º de sua própria estrutura ao âmbito da legislação nacional dos Estados signatários. Esse mecanismo evidencia a flexibilidade da convenção de Budapeste ao reconhecer a necessidade de adaptação das normas internacionais às particularidades legais de cada país, viabilizando, assim, uma cooperação internacional mais efetiva no combate crimes cibernéticos. Portanto, o auxílio mútuo previsto na convenção de Budapeste desempenha um papel fundamental na promoção da colaboração internacional no enfrentamento da cibercriminalidade, assegurando a harmonização das medidas legais com as legislações nacionais dos Estados envolvidos[429].

Em seu artigo 26º, a convecção ainda estabelece medidas para agilizar o auxílio mútuo em casos de crimes cibernéticos. Em situações de urgência poderá ocorrer a troca de informações entre os Estados signatários por meio de fax ou e-mail, desde que haja segurança e autenticidade, sendo posteriormente confirmada oficialmente, se solicitado pelo Estado requerido. Isso se justifica pela volatilidade das evidências em sistemas informáticos, que podem ser comprometidas rapidamente, exigindo uma abordagem célere[430].

[427] DELGADO. Op. Cit.pg154

[428] CONVENÇAÕ DE BUDAPESTE. Op. Cit

[429] CONVENÇAÕ DE BUDAPESTE. Op. Cit.

[430] *Ibidem*.

No entanto, é importante ressaltar que a assistência mútua está sujeita às leis internas e acordos de assistência mútuas aplicáveis, garantindo salvaguardas para os direitos das pessoas no território do Estado requerido, conforme disposto no item 4º. Essas disposições não se aplicam se houver indicações claras na convenção que contradigam essas salvaguardas[431].

Além disso, o artigo 26º aborda a questão da dupla incriminação, permitindo a assistência mútua mesmo quando as terminologias legais diferem entre os Estados partes, desde que a conduta criminosa esteja prevista na convenção, será eliminado barreiras técnicas. A convenção também reconhece a possibilidade de informações relevantes surgirem durante investigações que levem a procedimentos adicionais, e permite que uma parte signatária informe a outra sobre essas informações, desde que não violem o direito interno e sejam mantidas em sigilo, conforme estipulado no item 2º do artigo 26º. Dessa forma a cooperação internacional se torna mais eficiente no combate aos crimes cibernéticos, sem ser obstaculizada por burocracia, desde que os direitos fundamentais sejam preservados[432].

4.2.4 O auxílio mútuo no âmbito da Rede 24/7

De acordo com a convenção de Budapeste, os estados membros devem ter estabelecimento de uma rede integrada de "pontos de contato" com o propósito de facilitar a cooperação mútua e compartilhamento de dados instantaneamente. Essa rede se configura como uma central de suporte e auxílio de grande porte, operando ininterruptamente, 24 horas por dia, durante todos os dias da semana. A disposição legal que fundamenta a criação dessa central 24/7 está no artigo 37º o qual estabelece:

> "O auxílio incluirá a facilitação, ou se o direito e práticas internas o permitirem, a aplicação direita das seguintes medidas: a) A prestação de aconselhamento técnico; b) A conservação de dados em conformidade com os artigos 29º e 30º; e c) A recolha de provas, informações de carácter jurídico e localização de suspeitos[433] .

Nota-se que a convenção enfatiza a necessidade de pessoal capacitado para atender às solicitações de auxílio e ressalta que essa abordagem complementa, mas não substitui, a cooperação internacional tradicional entre países[434].

---

[431] *Ibidem.*

[432] CONVENÇAÕ DE BUDAPESTE. Op. Cit.

[433] CONVENÇAÕ DE BUDAPESTE. Op. Cit.

[434] *Ibidem*

A ideia de um auxílio direto, preservação e compartilhamento de evidências sobre a temática dos crimes cibernéticos já havia sido discutida durante um encontro de países do G8[435] em 1997, resultando na criação do subgrupo *High-Tech Crime*, com o objetivo de permitir a persecução de criminosos cibernéticos. Isso levou à criação de uma rede de contato entre esses países devido à morosidade dos canais tradicionais de cooperação internacional. Essa rede opera 24/7 e envolve pontos de contato que se comunicam diretamente e rapidamente, formalizando a cooperação por meio de pedidos formais[436].

Esses pontos de contato têm a responsabilidade de fornecer assistência imediata, aconselhamento técnico, preservação e coleta de dados, além de informações essenciais para esclarecer os fatos e localizar suspeitos. A cooperação direta entre esses pontos de contato é fundamental para evitar limitações e obstáculos na investigação de crimes cibernéticos[437].

Entretanto, é relevante destacar que o Brasil já faz parte ativamente dessa rede de colaboração contínua, operante 24 horas por dia e durante todos os sete dias da semana, no âmbito do G-8. Este grupo reúne aproximadamente cinquenta nações, todas elas comprometidas com a cooperação mútua em situações de crimes cibernéticos que abrangem mais de uma jurisdição internacional[438].

A convenção reforça essa rede de apoio para agilizar a assistência mútua entre os Estados Partes. A rede de pontos de contato age como um canal suplementar de comunicação, facilitando a assistência mútua de acordo com as atribuições de cada ponto de contato. Essas atribuições incluem a prestação de aconselhamento técnico, preservação de dados, coleta de provas, fornecimento de informações sobre o direito e localização de suspeitos (artigo 35º, parágrafo 1º).O aconselhamento técnico envolve fornecer orientações técnicas essenciais, como ajudar o Estado requerente a prevenir invasões ou ataques aos seus sistemas informáticos e

---

[435] A sigla G-8 corresponde ao grupo dos oito países mais ricos e influentes do mundo, fazem parte os Estados Unidos, Japão, Alemanha, Canadá, França, Itália, Reino Unido e Rússia. Antes chamada de G-7, a sigla alterou-se com a inserção da Rússia, que ingressou no grupo em 1998. Explicitamente, a função do G-8 é a de decidir qual ou quais caminhos o mundo deve seguir, pois esses países possuem economias consolidadas e suas forças políticas de globalização, abertura de mercados, problemas ambientais, ajudas financeiras para economias em crise, entre outros. FREITAS, Eduardo de. "G-8"; *Brasil Escola*. Disponível em: https://brasilescola.uol.com.br/geografia/g8.htm. Acesso em 08 de setembro de 2023.

[436]BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silvera. Manual de Investigação Cibernética: à Luz do Marco Civil da Internet. Rio de Janeiro: Editora Brasport, 2016. Ebook kindle, pg103.

[437] BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silvera, Op. Cit.

[438] CONTE, Christiany Pegorari. Jurisdição e competência nos crimes informáticos. Revista Brasileira de Meio Ambiente Digital e Sociedade da Informação, v. 1, n. 1, p. 49-208, 2014.

proteger dados importantes[439].O fornecimento de informações sobre o direito refere-se a informar sobre a legislação em vigor no Estado requerido, explicando o funcionamento do sistema jurídico, suas instituições e as normas relevantes para a assistência mútua. Isso vai além de simplesmente enviar cópias de textos legais, incluindo informações gerais sobre como o sistema legal opera, suas instituições e as normas que afetam a execução da pena, como circunstâncias agravantes, atenuantes e as condições para a prestação de assistência mútua[440].

4.3 Processo de adesão do brasil à convenção Budapeste

4.3.1 Contexto e motivações para a adesão do Brasil

Nos últimos anos, o Brasil tem intensificado sua participação na comunidade internacional por meio de acordos e tratados em matéria penal, submetendo-se à jurisdição de Cortes estrangeiras e estabelecendo protocolos de assistência mútua. Essas relações internacionais estão respaldadas pela Constituição Federal, especificamente no artigo 4º e seus incisos.

A Emenda Constitucional 45/2004, representou um avanço significativo nas relações internacionais ao introduzir o §3º no artigo 5º da Constituição[441]. Esse parágrafo conferiu status de Emenda Constitucional aos tratados e convenções internacionais sobre direitos humanos, eliminando conflitos de hierarquia no ordenamento jurídico nacional. O §3º estabelece que tais tratados e convenções, aprovados pelo Congresso Nacional em dois turnos, por três quintos dos votos dos membros de cada Casa, têm o mesmo valor que emendas constitucionais.

Nesse contexto, a adesão do Brasil à convenção de Budapeste era amplamente percebida como um benefício significativo para o país. Como mencionado anteriormente, o Brasil enfrenta uma lacuna na legislação relativa à cibersegurança e crimes cibernéticos, agravada pela carência de recursos estruturais para enfrentar essa problemática Em 2020 O ministério público por meio do parecer n 736/2020, solicitou celeridade na adesão à convenção, alertando que os crimes cibernéticos não tem sido enfrentado de forma eficiente pela falta de capacitação e ausência de ferramentas jurídicas aptas a permitir a persecução penal, o que acarreta um

[439]CONVENÇAÕ DE BUDAPESTE. Op. Cit

[440]CONVENÇAÕ DE BUDAPESTE. Op. Cit

[441] CONSTITUIÇÃO FERDERAL, 1988. Op. Cit.

aumento de insegurança dos usuários brasileiros na internet e dificulta a prevenção dos ataques e ocorrências[442].

Além disso, o parecer enfatizava o crescimento da incidência de crimes cibernéticos, acompanhado pela migração de infrações comuns no ambiente digital. Vale ressaltar que a obtenção de provas digitais, fundamental para estabelecer a materialidade e autoria de diversos delitos, frequentemente requer o uso de interceptações telemáticas e acesso a arquivos armazenados em serviços de computação em nuvem o que demanda a necessidade de uma cooperação e auxílio mútuo entre os países envolvidos[443].

O Brasil foi convidado à convenção em dezembro de 2019. Esse compromisso foi posteriormente ratificado pelo congresso nacional, por meio do Decreto Legislativo n.º 37, formalizado em 16 de dezembro de 2021. Dando continuidade ao processo de adesão, o Governo brasileiro apresentou o instrumento de ratificação da convenção ao Secretário-Geral do Conselho da Europa em 30 de novembro de 2022. Como resultado, a convenção entrou em vigor no plano jurídico internacional para o Brasil em 1º de março de 2023 e foi devidamente incorporada ao sistema jurídico nacional por meio do Decreto 11.491, promulgado em 12 de abril de 2023[444].

Dessa forma, a convenção de Budapeste foi incorporada ao ordenamento jurídico brasileiro em um contexto em que várias questões relacionadas à criminalidade virtual ganhavam destaque, como vazamento de dados, golpes informáticos e disseminação de fake news pela internet. Essa temática requer um amplo debate, visando ao desenvolvimento de políticas públicas abrangentes, incluindo políticas criminais adequadas para enfrentar o problema, que transcende a esfera estritamente criminal[445].

É essencial adaptar e atualizar as condutas criminalizadas pela convenção às demandas atuais, considerando a evolução da tecnologia e dos métodos utilizados pelos criminosos. Além

---

[442] BRASIL. Ministério Público Federal. Procuradoria-Geral da República. Ofício nº 736/2020, de 30 de julho de 2020. Convenção sobre o Crime Cibernético. Brasília, DF: Ministério Público Federal, 2020. Disponível em: http://www.mpf.mp.br/pgr/documentos/Oficio736DaviAlcolumbre.pdf. Acesso em: 01 mai. 2021.

[443] BRASIL. Ministério Público Federal. Procuradoria-Geral da República. Ofício nº 736/2020. Op. Cit.

[444] BRASIL. Decreto Legislativo nº Nº 11.491, de 12 de maio de 2023: Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Brasília, 12 maio 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-11.491-de-12-de-abril-de-2023-476680563. Acesso em: 28 ago. 2023.

[445] MURATA, Ana Maria Lumi Kamimura; TORRES, Me Paula Ritzmann. A convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora? Boletim IBCCRIM, v. 31, n. 368, 2023. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/575/108

disso, é crucial realizar uma análise abrangente do ordenamento jurídico nacional para evitar excesso de punições ou normas penais ineficazes, o que poderia resultar em insegurança jurídica e possíveis abusos por parte do Estado[446].

4.4.2 Impactos da adesão do Brasil e a necessidade de harmonização

Embora a convenção demande que seus membros se submetam aos princípios fundamentais e normas estabelecidas em convenções anteriores, sua aplicação é caracterizada por uma considerável flexibilidade, sendo adaptada às peculiaridades da legislação interna de cada país signatário. O enfoque principal consiste em oferecer diretrizes e não em propor soluções inflexíveis e uniformes para os desafios identificados. Teoricamente, essa abordagem poderia facilitar a harmonização do ordenamento jurídico brasileiro[447].

Vale ressaltar que mesmo antes da adesão do Brasil ao tratado o legislador nacional já havia percebido a necessidade de criminalizar certas condutas mencionadas no texto da convenção, como invasão de dispositivo informático, pornografia infantil e violação de direitos autorais. No entanto, para que essas medidas fossem de fato aplicadas efetivamente, é necessário complementar a legislação, definindo com clareza as condutas incriminadas e as penas correspondentes[448].

Desse modo, a adesão do Brasil à convenção representa uma significativa ampliação da proteção legal e do combate às condutas que, atualmente, apesar de tipificadas demandam interpretações e não são claras. Um exemplo é apresentado no artigo 6º, alínea "a", da convenção, que classifica como infração penal a criação de dispositivos ou programas informáticos com a finalidade de cometer delitos no ambiente virtual. Outra disposição relevante encontra-se no artigo 7º, que aborda a prática de falsidade informática. A inclusão de tais tipificações no ordenamento jurídico brasileiro seria altamente benéfica, visto que tais condutas já são recorrentes em território nacional, porém suas tipificações não são pacificadas[449].

Um exemplo dessa lacuna legislativa são as famosas condutas conhecidas como o "golpe de clonagem de WhatsApp". Nesse golpe, os cibercriminosos cadastram o número de

[446] MURATA, TORRES. Op. Cit.

[447] COLTRO, Rafael Khalil; WALDMAN, Ricardo Libel. Op. Cit. p. 104-123, 2021.

[448]MURATA, TORRES. Op. Cit.

[449] COLTRO, Rafael Khalil; WALDMAN, Ricardo Libel. Op. Cit. p. 104-123, 2021.

telefone do usuário em outro dispositivo, após o qual o usuário legítimo recebe um SMS contendo um código de acesso. A vítima, enganada, fornece esse código aos criminosos, resultando no bloqueio de sua conta do WhatsApp. Nesse momento, os criminosos assumem a identidade da vítima e frequentemente solicitam dinheiro aos contatos da pessoa cujo WhatsApp foi invadido. Em algumas situações, os criminosos podem até violar a privacidade da vítima, acessando suas conversas, fotos e outros documentos pessoais disponíveis no aplicativo de mensagens[450].

Contudo, a falta de tipificação específica representa um obstáculo para o efetivo combate a essas práticas. É frequente que as autoridades policiais apenas iniciem investigações nos casos em que seja evidente um prejuízo financeiro para alguma das vítimas, enquadrando a conduta como estelionato, porém predomina o entendimento de que se não houver prejuízo financeiro da vítima não ocorrerá crime, pois o delito de estelionato exige um efetivo prejuízo para ser configurado, deixando impune a conduta na maioria dos casos[451].

Nesse sentido, a tentativa de aplicar a conduta prevista no art. 171º do Código Penal à situação em questão, que envolve um golpe realizado através do *whatsApp*, revela-se consideravelmente ineficaz, uma vez que não abrange a criminalização da conduta anterior ao prejuízo financeiro, a qual, por si só, já constitui uma grave violação à privacidade da vítima. A impunidade nestes casos é resultado da ausência de uma tipificação específica para essa conduta. À luz desse contexto, a convenção de Budapeste pode também desempenhar um papel crucial no combate a essas práticas, uma vez que em seu art. 7º tipifica exatamente a conduta praticada pelos fraudadores, restando ao ordenamento jurídico brasileiro a tarefa de determinar a pena correspondente[452].

No que diz respeito à compatibilidade das normas brasileiras com as disposições do tratado, a tabela a seguir oferece uma síntese esclarecedora sobre o ordenamento jurídico atual. Nela, fica evidente que a legislação brasileira tipifica a maioria dos crimes cibernéticos exigidos pelo acordo:

RECOMENDAÇÃO DA CONVENÇÃO [453]	LEGISLAÇÃO BRASILEIRA

[450] COLTRO, Rafael Khalil; WALDMAN, Ricardo Libel. Op. Cit. p. 104-123, 2021.

[451] COLTRO, Rafael Khalil; WALDMAN, Ricardo Libel. Op. Cit. p. 104-123, 2021.

[452] COLTRO, .Rafael Khalil; WALDMAN, Ricardo Libel. Op. Cit. p. 104-123, 2021.

[453] CONVENÇÃO DE BUDAPESTE. Op. Cit.

Artigo 2º - Do acesso ilegal ou não autorizado a sistemas informatizados	Artigo 154-A e 154-B Código Penal[454] Invasão de dispositivo informático (público ou privado).
Artigo 3º- Da interceptação ou interrupção de comunicações	Artigo10 (Lei 9.296 de 1996/96) Interceptação sem autorização judicial
Artigo 4º - Da interferência não autorizada sobre os dados armazenados	Sem previsão
Artigo 5º - Interferência em dados informáticos	Artigo 313-B Código Penal Modificação ou alteração ilícita de sistemas de informação.
Artigo 6º Uso abusivo de dispositivo digital	Artigo 154-A e 154-B Código Penal Invasão de dispositivo informático (público ou privado).
Artigo 7º Falsidade informática	Artigo 297 Código Penal Falsificação documentos públicos
Artigo 8º Fraude Informática	Artigo 171 Código Penal – Estelionato Artigo 155 Código Penal – Furto por Fraude
Artigo 9º - Da pornografia infantil ou pedofilia	241 da Lei 8.069, de 1990, Estatuto da Criança e do Adolescente (ECA)[455]
Artigo 10º - Da quebra relacionadas com violação direito do autor dos direitos conexos.	Lei 9.609, de 1998, (a Lei do Software), da Lei 9.610 de 1998, (a Lei do Direito Autoral)[456] e da Lei 10.695 de 2003 lei da Pirataria)[457]
Artigo 11º - Das tentativas ou ajudas a condutas criminosa	285-A do Código Penal

Tabela 06

Possivelmente algumas previsões presentes na convenção demandarão de uma atualização da legislação penal em vigor no país, notadamente em relação a delitos como a violação de dados e interferências em sistemas, bem como as disposições contidas no artigo

[454] CÓDIGO PENAL, 1940. Op. Cit.

[455] Estatuto da Criança e do Adolescente: Lei federal nº 8069, de 13 de julho de 1990. Rio de Janeiro: Imprensa Oficial, 2002. BRASIL.

[456] 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

[457] 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

12º, que atribuem responsabilidade a pessoas jurídicas. Este último aspecto representa um dos desafios mais significativos em nosso ordenamento, uma vez que coloca dirigentes de pessoas jurídicas na posição de responsáveis por atos praticados por indivíduos sob sua autoridade ou benefício, ou quando a supervisão e o controle falham, resultando em um delito[458].

Para Patrícia Peck, a distinção entre uma organização criminosa agindo e uma empresa envolvida em infrações como violações de direitos autorais ou pornografia infantil, que poderiam também culpar o dirigente, é uma problemática que requer uma análise mais aprofundada. Outro ponto de relevância é o artigo 15º, que preconiza a necessidade de adotar medidas excepcionais, tais como ordens de autoridade para investigações, que não dependem de autorização judicial, em situações de flagrante delito. Essa disposição se estende a cenários como revistas em veículos, blitz de trânsito, inspeções em aeroportos, revistas em eventos públicos, entre outros. Ações relacionadas à autoridade, realizadas sem intervenção judicial, mas que têm o potencial de identificar ameaças substanciais, são essenciais no contexto do combate aos crimes cibernéticos [459].

Para Murata e torres há uma discrepância na redação deste artigo sobre a responsabilidade da pessoa jurídica. No texto em inglês, utiliza-se apenas a expressão "*corporate liability*", sem adjetivar a responsabilidade como civil, penal ou administrativa, e continua estipulando que os Estados-parte devem adotar medidas necessárias para garantir que as pessoas jurídicas possam ser responsabilizadas por crimes previstos na convenção. Por outro lado, no decreto brasileiro, utiliza-se o termo "responsabilidade penal da pessoa jurídica", assegurando que "pessoas jurídicas possam ser consideradas penalmente responsáveis". Essa diferença na redação, embora aparentemente sutil, esclarece a potencial incompatibilidade entre as partes 1 e 2 do artigo 12º do Decreto, que inicialmente preveem a responsabilidade de forma exclusivamente penal, e a parte 3, que sugere que a responsabilidade da pessoa jurídica pode ser civil, criminal ou administrativa[460].

No entanto, o texto da convenção permite que cada Estado membro decida, de acordo com as peculiaridades de seu ordenamento jurídico, a forma mais adequada e eficaz de responsabilização das pessoas jurídicas, adaptando-se aos princípios orientadores da

---

[458] 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/#:~:text=**Por%20Patr%C3%ADcia%20Peck%20%E2%80%93%20Sobre,trazemos%20por%20decreto%20para%20c%C3%A1. Acesso:10. mai. 2023

[459] PINHEIRO, Patrícia Peck, Sobre a adesão do Brasil à Convenção de Budapeste. Op. Cit.

[460] PINHEIRO, Patrícia Peck, Sobre a adesão do Brasil à Convenção de Budapeste. Op. Cit.

convenção. O modelo de responsabilidade proposto para as pessoas jurídicas está intrinsecamente vinculado aos crimes cometidos por pessoas físicas. Quando se trata de responsabilidade penal, conforme estabelecido no Decreto, é necessário realizar algumas considerações a fim de avaliar sua compatibilidade com o ordenamento jurídico nacional[461].

Cabe ressaltar que a Constituição de 1988 prevê a responsabilidade penal das pessoas jurídicas. O artigo 173º, parágrafo 5º, da Constituição, estipula a responsabilidade da pessoa jurídica, submetendo-a a punições compatíveis com sua natureza nos casos de atos praticados contra a ordem econômica e financeira, bem como contra a economia popular. Adicionalmente, o artigo 225º, parágrafo 3º, estabelece que condutas e atividades prejudiciais ao meio ambiente sujeitam os infratores, sejam pessoas físicas ou jurídicas, a sanções penais e administrativas, independentemente da obrigação de reparar os danos causados. O texto constitucional explicita os bens jurídicos que podem ensejar a responsabilidade penal da pessoa jurídica, e uma vez que a natureza do cibercrime não está atrelada ao bem jurídico, é plausível identificar condutas que se enquadram nas situações previstas, a fim de justificar essa forma de responsabilidade conforme o decreto em questão[462].

Outro ponto importante é que o tema da responsabilidade penal das pessoas jurídicas é altamente controverso, pelas complexidades dogmáticas que permeiam o Direito Penal brasileiro ao tentar conceber um modelo de responsabilidade compatível com os princípios orientadores deste sistema legal, pontos extremamente relevantes e podem gerar uma vasta discussão sobre a teoria da responsabilidade penal da pessoa jurídica[463].

O artigo 15º da referida legislação ressalta a necessidade de implementar medidas extraordinárias para a eficácia da investigação de crimes cibernéticos. Neste contexto, situa-se a prerrogativa de autoridades competentes para executar ações investigativas sem a necessidade imediata de uma ordem judicial. Para Peck esta disposição se torna particularmente pertinente em situações emergenciais ou de flagrante delito, onde a rapidez e a eficácia na resposta são essenciais para a identificação e contenção de ameaças no ambiente virtual[464].

No contexto dos prazos processuais, o artigo 16º estabelece um período de 90 dias para a preservação de evidências. Importante destacar que o Brasil já possui prazos mais extensos,

---

[461] MURATA, TORRES. Op. Cit.

[462] MURATA, TORRES. Op. Cit.

[463] MURATA, TORRES. Op. Cit..

[464] PINHEIRO, Patrícia Peck, Sobre a adesão do Brasil à Convenção de Budapeste. Op. Cit.

conforme estipulado no arco Civil da Internet. Além disso, o artigo 18º define de forma precisa o conceito de informação cadastral, uma definição de extrema importância no contexto da lei. Por fim, o artigo 20º regula a obtenção de dados em tempo real, um aspecto fundamental para a eficácia do combate aos crimes cibernéticos [465].

Nas palavras de Carolina Yumi, diretora do departamento de recuperação de ativos e Cooperação Jurídica Internacional (DRCI) do Ministério da Justiça e Segurança Pública (MJSP), enfatiza que a plena implementação da convenção de Budapeste no Brasil concretizará benefícios substanciais para o país. Esses benefícios englobam avanços nas normativas e políticas relacionadas ao combate aos crimes cibernéticos, bem como na coleta e preservação de evidências digitais. Adicionalmente, a convenção contribuirá para o aprimoramento da cooperação internacional nas investigações e esclarecimento de delitos cometidos no ciberespaço, ao mesmo tempo em que estimulará o Brasil a continuar desenvolvendo seu sistema jurídico e suas políticas frente ao avanço da cibercriminalidade. Portanto, esse processo requer uma abordagem equilibrada, que promova a intensificação da persecução penal ao mesmo tempo em que assegura a proteção dos dados pessoais[466].

Desse modo, o legislador deve ter cautela ao tipificar novas condutas trazidas pela convenção, para evitar sobreposições com tipos penais já existentes na legislação brasileira e o estabelecimento de penas desproporcionais. A análise cuidadosa do bem jurídico, a definição clara das condutas a serem incriminadas e a previsão de penas proporcionais são etapas cruciais que requerem um debate maduro para evitar que a legislação se torne ineficaz, gerando insegurança jurídica e possíveis abusos no exercício do poder estatal[467].

Em suma, embora a adesão do Brasil à convenção tenha sido tardia, observa-se um que o legislador brasileiro tem se esforçado na modernização da legislação penal nacional dos crimes cibernéticos. Destacam-se, nesse contexto, avanços significativos, como da lei 12.737/2012 e a recente promulgação da Lei n.º 14.155/2021, com o intuito de agravar as penalidades nos casos de delitos envolvendo a violação de dispositivos informáticos, furto e estelionato cometidos eletronicamente ou através da internet e principalmente o Marco civil da

[465] PINHEIRO, Patrícia Peck, Sobre a adesão do Brasil à Convenção de Budapeste. Op. Cit.

[466] 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. ago. 2023

[467] MURATA, TORRES. Op. Cit.

Internet. Essas iniciativas representam passos concretos em direção a uma legislação mais alinhada com os artigos tratados na convenção de Budapeste

4.4.3 Fortalecimento da cooperação internacional do Brasil no cenário mundial

Conforme abordado anteriormente, a cooperação internacional em assuntos penais se apresenta como uma solução indispensável para lidar com o cibercrime, dada a sua intrínseca natureza transnacional. A convenção de Budapeste, estabelecida em 2001, assume atualmente um papel de destaque como marco jurídico essencial para a promoção da coordenação e harmonização legislativa entre os Estados, com o objetivo de fortalecer a eficácia das políticas de combate aos crimes cibernéticos.

O relatório explicativo da convenção de Budapeste reconhece a volatilidade dos dados armazenados em dispositivos informáticos. Informações cruciais podem ser prontamente eliminadas por meio de processos automatizados, comprometendo assim a coleta de provas e, por conseguinte, os procedimentos de investigação criminal. Nesse contexto, considerando que autoridades encarregadas da persecução penal podem necessitar de dados armazenados em servidores localizados em jurisdições distintas da sua, a convenção destaca a importância de se estabelecer mecanismos que garantam a conservação e o compartilhamento desses dados, respeitando, é claro, os limites jurídicos impostos por cada Estado[468].

É dentro desse contexto que se inserem os mecanismos de cooperação internacional em matéria penal, essenciais para viabilizar a investigação e o combate efetivo aos crimes cibernéticos em uma era cada vez mais interconectada. A relevância da convenção no fomento de medidas de cooperação internacional está estreitamente ligada ao esforço de harmonização legislativa. Clough ressalta enfaticamente a necessidade de alcançar um certo grau de harmonização entre os Estados como um componente crucial na construção de um modelo eficaz para conter o avanço da cibercriminalidade. Para ilustrar essa necessidade, o autor apresenta um cenário exemplificativo em que, mesmo quando tanto a vítima quanto o autor do delito estão sujeitos à mesma jurisdição, as evidências do crime podem ter, em algum momento, transitado por outras jurisdições ou mesmo estar armazenadas em territórios jurídicos distintos[469].

Essa interconexão de jurisdições e a possibilidade de que as evidências cruciais para a investigação estejam dispersas geograficamente destacam a complexidade inerente ao

[468] CLOUGH, Jonathan. Op. Cit.

[469] CONVENÇÃO DE BUDAPESTE. Op. Cit.

enfrentamento da cibercriminalidade. Nesse contexto, a harmonização das leis e a promoção de medidas de cooperação internacional, como as delineadas na convenção, surgem como meios essenciais para lidar eficazmente com esses desafios, assegurando que a persecução penal seja eficiente e que os criminosos cibernéticos não encontrem refúgio em territórios onde as lacunas legais ou a falta de colaboração internacional possam permitir a impunidade[470].

Embora a convenção de Budapeste estimule amplamente a cooperação entre as partes e preconize agilidade nesse processo, é importante destacar que não existe uma obrigação expressa que imponha a uma das partes o fornecimento de informações de forma espontânea à outra. Em linhas gerais, a convenção não estabelece vínculos que obriguem os Estados a promoverem medidas de auxílio mútuo, permitindo, assim, que qualquer uma das partes possa recusar um pedido de cooperação, desde que tal recusa esteja em conformidade com as disposições da própria convenção[471].

Essa ausência de uma obrigação direta é justificada pelo fato de a convenção reconhecer a dependência do auxílio mútuo em cooperação internacional com a legislação doméstica de cada Estado e com os tratados internacionais aos quais eles estejam vinculados. Dessa forma, à medida que as medidas de auxílio mútuo se tornam mais intrusivas na jurisdição dos Estados signatários, a convenção condiciona a execução dessas medidas à celebração de acordos entre as partes envolvidas e à observância da legislação interna de cada Estado[472]

Nesse sentido, apesar de o Brasil manter extensos laços diplomáticos com a maioria das nações, o número de tratados e acordos internacionais em matéria penal é relativamente reduzido. Conforme informações do Ministério da Justiça e Segurança Pública, o país é signatário de 15 convenções internacionais de natureza multilateral, ou seja, aquelas envolvendo diversos países, incluído a recente adesão da convenção de Budapeste e detém apenas 21 acordos bilaterais, restritos a relações entre o Brasil e outro Estado[473].

ACORDOS MULTILATERAIS	DECRETOS	ACORDOS BILATERAIS	DECRETOS

[470] CONVENÇÃO DE BUDAPESTE. Op. Cit.

[471] CONVENÇÃO DE BUDAPESTE. Op. Cit.

[472] CLOUGH, Jonathan. Op. Cit. p. 714-716.

473 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. ago. 2023

		DECRETOS	
Convenção Contra o Tráfico Ilícito de Entorpecentes e Substâncias Psicotrópicas (Convenção de Viena)	Decreto nº 154, de 26 de junho de 1991	CANADÁ: Acordo de Assistência Mútua em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo do Canadá	Decreto nº 6.747, de 22 de janeiro de 2009
Convenção Interamericana para o Cumprimento de Sentenças Penais no Exterior	Decreto nº 5.919, de 10 de junho de 1996	CHINA: Acordo entre a República Federativa do Brasil e a República Popular da China sobre Assistência Jurídica Mútua em Matéria Penal	Decreto nº 6.282, de 03 de dezembro de 2007
Convenção Interamericana sobre Tráfico Internacional de Menores	Decreto nº 2.740, de 20 de agosto de 1998	BÉLGICA: Tratado entre a República Federativa do Brasil e o Reino da Bélgica sobre Auxílio Jurídico Mútuo em Matéria Penal	Decreto nº 9.130, de 17 de agosto de 2017

Convenção Interamericana contra a Fabricação e o Tráfico Ilícitos de Armas de Fogo, Munições, Explosivos e Outros Materiais Correlatos	Decreto nº 3.229, de 29 de outubro 1999	COLÔMBIA: Acordo de Cooperação Judiciária e Assistência Mútua em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo da República da Colômbia em Matéria Penal	Decreto nº 3.895, de 23 de agosto de 2001
Protocolo de Assistência Jurídica Mútua em Assuntos Penais-MERCOSUL	Decreto nº 3.468, de 17 de maio de 2000	COREIA DO SUL: Acordo entre a República Federativa do Brasil e a República da Coréia sobre Assistência Judiciária Mútua em Matéria Penal	Decreto nº 5.721, de 13 de março de 2006
Convenção Sobre o Combate da Corrupção de Funcionários Públicos Estrangeiros em Transações Comerciais Internacionais	Decreto nº 3.678, de 30 de novembro de 2000	CUBA: Acordo de Cooperação Judicial em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo da República de Cuba	Decreto nº 6.462, de 21 de maio de 2008
Convenção Interamericana contra a Corrupção	Decreto nº 4.410, de 7 de outubro de 2002	ESPANHA: Acordo de Cooperação e Auxílio Jurídico Mútuo em Matéria Penal entre a República Federativa do Brasil e o Reino da	Decreto nº 6.681, de 08 de dezembro de 2008

		Espanha	
Convenção das Nações Unidas contra o Crime Organizado Transnacional (Convenção de Palermo)	Decreto nº 5.015, de 12 de março de 2004	EUA: Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América	Decreto nº 3.810, de 02 de maio de 2001
Convenção Interamericana contra o Terrorismo	Decreto nº 5.639, de 26 de dezembro de 2005	FRANÇA: Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo da República Francesa	Decreto nº 3.324, de 30 de maio de 1999
Convenção das Nações Unidas Contra a Corrupção (Convenção de Mérida)	Decreto nº 5.687, de 31 de janeiro de 2006	HONDURAS: Tratado entre o Governo da República Federativa do Brasil e o Governo da República de Honduras sobre Auxílio Jurídico Mútuo em Matéria Penal	Decreto nº 8.046, de 11 de julho de 2013
Convenção Interamericana sobre Assistência Mútua em Matéria Penal	Decreto nº 6.340, de 03 de janeiro de 2008	ITÁLIA: Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo da República Italiana	Decreto nº 862, de 09 de julho de 1993
Acordo Complementar ao Acordo de Assistência Jurídica Mútua em Assuntos Penais entre os Estados Partes do Mercosul, Bolívia e Chile	Decreto nº 8.331, de 12 de novembro de 2014	JORDÂNIA: Acordo sobre Auxílio Jurídico Mútuo em Matéria Penal entre a República Federativa do Brasil e o Reino Hachemita da Jordânia	Decreto n° 9.729, de 15 de março de 2019
Convenção de Auxílio Judiciário em Matéria Penal entre os Estados Membros da CPLP	Decreto nº 8.833, de 4 de agosto de 2016	MÉXICO: Acordo de Assistência Jurídica Internacional em Matéria Penal entre a República Federativa do Brasil e os Estados Unidos Mexicanos	Decreto n° 7.595, de 1° de novembro de 2011

Protocolo para eliminar o Comércio Ilícito de Produtos de Tabaco	Decreto nº 9.516, de 1 de outubro de 2018	NIGÉRIA: Acordo de Assistência Jurídica Mútua em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo da República Federal da Nigéria	Decreto n° 7.582, de 13 de outubro de 2011
Convenção sobre o Crime Cibernético (Convenção de Budapeste)	Decreto nº 11.491, de 12 de abril de 2023	PANAMÁ: Acordo de Assistência Jurídica Mútua em Matéria Penal entre a República Federativa do Brasil e a República do Panamá sobre Auxílio Jurídico Mútuo em Matéria Penal	Decreto n° 7.596, de 1° de novembro de 2011
		REINO UNIDO DA GRÃ-BRETANHA E IRLANDA DO NORTE: Tratado de Assistência Jurídica Mútua em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo do Reino Unido da Grã-Bretanha e Irlanda do Norte	Decreto nº 8.047, de 11 de julho de 2013

		SUÍÇA: Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo da Confederação Suíça	Decreto nº 6.974, de 07 de outubro de 2009
		SURINAME: Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo da República do Suriname	Decreto nº 6.832, de 29 de abril de 2009
		TURQUIA: Acordo sobre Auxílio Jurídico Mútuo em Matéria Penal entre a República Federativa do Brasil e a República da Turquia	Decreto nº 9.065, de 31 de maio de 2017
		PERU: Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo da República do Peru	Decreto nº 3.988, de 29 de outubro de 2001

		UCRÂNIA: Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo da Ucrânia	Decreto nº 5.984, de 12 de dezembro de 2006

Tabela 07 Fonte: Site Ministério da Justiça e Segurança Pública.

A Convenção, nesse contexto, assume um papel complementar, destinado a suplementar outros acordos multilaterais ou bilaterais já celebrados pelo Brasil. Contudo, é importante ressaltar que, quando a Convenção é aplicada de forma subsidiária a outros instrumentos jurídicos internacionais, deve haver consonância entre ambos, de modo a evitar conflitos com os princípios estabelecidos na própria Convenção[474].

Nesse sentido, com o desenvolvimento tecnológico e a emergência de uma sociedade hiperconectada os crimes cibernéticos se tornam o epicentro das preocupações globais em matéria de segurança. A Convenção de Budapeste, nesse cenário, estabelece um marco normativo internacional fundamental, desempenhando papel significativo na articulação e fortalecimento da cooperação penal internacional. É importante enfatizar, entretanto, que a efetividade deste instrumento depende de sua integração e harmonização com os ordenamentos jurídicos domésticos e outros instrumentos jurídicos internacionais

Desse modo, a adesão a um tratado internacional, como a convenção de Budapeste, representa um passo significativo no sentido de promover a cooperação internacional no combate aos crimes cibernéticos. No entanto, é importante ressaltar que a mera adesão a esse tratado não significa que o país tenha atingido seu objetivo final nessa empreitada. Pelo contrário, a cooperação internacional deve ser uma busca constante, uma vez que quanto mais conexões de auxílio entre Estados forem estabelecidas, mais eficiente será à resposta a criminalidade cibernética. A adesão na convenção de Budapeste representa apenas o primeiro passo na construção de uma extensa rede de colaboração entre nações.

Neste contexto, a ênfase deve ser dada à flexibilidade, adaptabilidade e robustez das estruturas jurídicas e operacionais, tanto a nível nacional quanto internacional. A multiplicidade de tratados bilaterais, embora valiosa, pode ser otimizada por instrumentos multilaterais como

[474] CLOUGH, Jonathan. Op. Cit. p. 714-716

a convenção de Budapeste, que proporciona uma plataforma unificada e coesa, promovendo eficácia, consistência e harmonização nas iniciativas de combate ao crime cibernético[475].

Portanto, a adesão à convenção de Budapeste não exaure e nem resolve todos os problemas da criminalidade cibernética no contexto penal, mas se apresenta como um ponto de partida; uma iniciativa que catalisa esforços contínuos e colaborativos para enfrentar os desafios emergentes e evolutivos dos crimes cibernéticos. Reitera-se a necessidade de um contínuo compromisso com a inovação, a colaboração e a harmonização legislativa e operacional, elementos chave para navegar com eficácia na complexidade multifacetada do ciberespaço e garantir a integridade e segurança digital.

CONCLUSÃO

A presente pesquisa se propôs-se a responder, fundamentalmente, às seguintes indagações: quais são os desafios político-criminais enfrentados pelo ordenamento jurídico brasileiro diante dos crimes cibernéticos? Além disso, procurou-se avaliar a relevância da cooperação internacional em matéria penal, considerando a recente adesão do Brasil à convenção de Budapeste, bem como os possíveis desafios na harmonização legislativa.

Para tanto, a dissertação foi estruturada em quatro capítulos. O primeiro capítulo examinou os eventos históricos que levaram ao surgimento da sociedade da informação, do ciberespaço e os desafios oriundos de uma sociedade em rede hiperconectada. Analisou-se a evolução tecnológica e a origem da internet, em especial sua concepção durante a Guerra Fria como um meio de comunicação para salvaguardar as discussões sobre estratégias de guerra dos Estados Unidos. Foi apresentada para uma melhor compreensão do tema o surgimento dos primeiros crimes cibernéticos no contexto histórico mundial e no cenário brasileiro, bem como as diversas discussões acerca das definições e características desses crimes no ordenamento

[475] VERONESE, Alexandre. CALABRICH, Bruno. Cybercrime in Brazil After the COVID-19 Global Crisis: An Assessment of the Policies Concerning Internacional Cooperation for Investigations and Prosecutions. 2022

jurídico brasileiro.

O segundo capítulo trouxe uma análise aprofundada acerca do conceito de cooperação internacional em matéria penal e sua importância no cenário global de enfrentamento do crime cibernético. Ao examinar as respostas a este instituto, tornou-se evidente que questões relacionadas à sociedade da informação e a criminalidade digital, num contexto onde o sistema jurídico e o papel do Estado estão em constante evolução, precisam estar sempre alinhadas com a comunidade internacional. Observou-se que, para uma resposta mais eficiente à persecução penal, conceitos como soberania, tempo e local do crime precisam ser recontextualizados à luz da integração e da necessidade de um sistema de cooperação penal integrado, uma vez que esses conceitos sofreram alterações significativas no com o surgimento do ciberespaço e os crimes cibernéticos.

No terceiro capítulo, explorou-se a evolução do ordenamento jurídico brasileiro frente aos crimes cibernéticos, desde suas primeiras discussões e propostas legislativas as últimas atualizações penais. Constatou-se que diversas condutas relacionada aos crimes cibernéticos existentes no texto da convenção de Budapeste já encontram tipificação na legislação penal nacional, conforme à análise da Lei 12.737, o Marco Civil da Internet, a LGPD, a nova lei 141.32/2021 que criminaliza o *stalking* e principalmente a mais recente Lei 14.155/2021, que tornou mais severa as penalidades para a invasão de dispositivos informáticos em consonância com a recomendação disposto no artigo 2º da convenção que trata do acesso ilegal ou não autorizado a sistemas informatizados.

Entretanto, determinados aspectos processuais ainda enfrentam obstáculos legais, especialmente quando transcendem fronteiras nacionais, demandando uma abordagem de cooperação internacional integrada constante. Nesse quesito apesar dos avanços normativos, persiste um descompasso entre o arcabouço jurídico e os crimes cibernéticos, isso se deve a rapidez com que as informações são disseminadas no ambiente virtual, a volatividade das provas e principalmente o anonimato que as redes proporcionam para o criminoso.

Nota-se que a criminalização de algumas condutas dos crimes cibernéticos não é suficiente diante dos entraves que é a realidade na persecução penal, como a adoção de paradigmas territoriais incompatíveis com a natureza dos crimes cibernéticos e normas com interpretações ambíguas. Ressalta-se que a proposta deste estudo não visa uma perspectiva punitivista, mas sim evidenciar as lacunas existentes que ainda resultam em impunidade para diversos atos delitivos virtuais.

No último capítulo foram abordados os questionamentos acerca da recente adesão do Brasil a convenção de Budapeste sobre os crimes cibernéticos e sua importância no cenário

internacional por se tratar de um documento que trata especificamente da criminalidade virtual e possui como principal característica a harmonização das legislações penais, definições das terminologias e outras disposições importantes para o Direito Penal e seus desafios frente a persecução penal.

Nesse ponto, a incorporação da convenção de Budapeste pelo Brasil no ordenamento jurídico merece atenção quanto os possíveis desafios na harmonização da convenção com o ordenamento jurídico interno, trata-se da interpretação de alguns dispositivos do Decreto 11.491/2023, que introduziu o texto da convenção no ordenamento jurídico brasileiro, em relação à responsabilidade penal da pessoa jurídica, e estabelece a responsabilidade do grupo como penal, devendo ser considerada uma sugestão, e não uma ordem.

Isso ocorre porque o debate sobre a criação de um modelo de imputação de responsabilidade penal para entidades jurídicas ainda parece estar em estágios iniciais no âmbito legislativo, exigindo uma análise mais aprofundada de sua viabilidade, tanto em termos de hipóteses de responsabilização quanto em relação à adequação dos modelos de responsabilidade aos princípios orientadores do Direito Penal.

Outro ponto importante que merece atenção são as disposições do artigo 15º, que autoriza a implementação de medidas excepcionais como ordens de autoridade para investigações. Estas não requerem, necessariamente, uma ordem judicial e podem ser mobilizadas em circunstâncias de ameaças elevadas, como em situações de flagrante, revistas em locais públicos e abordagens veiculares, entre outros, como forma de assegurar que as condutas tipificadas no capítulo 2 recebam sanções adequadas.

Assim, necessário considerar que, apesar da convenção prescrever que as condutas em questão sejam submetidas a sanções efetivas, proporcionais e dissuasivas, englobando penas privativas de liberdade, o contexto brasileiro exige uma abordagem diferenciada. A aplicação de penas privativas de liberdade é uma estratégia controversa no cenário nacional, marcado por um sistema carcerário sobrecarregado e índices alarmantes de reincidência criminal.

Ao ponderar a adesão ao tratado, é indispensável priorizar o princípio do Direito Penal como *ultima ratio*. Onde a aplicação do Direito Penal se fizer necessária, é essencial que se atribua especial consideração às alternativas penais que não envolvam o encarceramento. A promoção de medidas alternativas se faz necessária para aliar eficácia e humanidade na resposta às infrações, garantindo uma abordagem que seja não apenas punitiva, mas também reformativa e socialmente responsável.

A incorporação da convenção de Budapeste como decreto promove não apenas a progressão legislativa pelo congresso nacional, visando ajustes na legislação interna, mas

também capacita a intervenção ágil de entidades administrativas e executivas, como o Ministério da Segurança Pública. Isso é sustentado pelos princípios de colaboração e assistência recíproca delineados nos artigos 23º e 25º, e pela facilitação da troca de informações, conforme prescrito no artigo 26º.

A relevância dessas disposições é amplificada ao considerar a frequência de crimes cibernéticos originados fora das fronteiras nacionais. A implementação efetiva dos mecanismos de cooperação internacional propostos pela convenção poderia, indubitavelmente, influenciar positivamente a resolução desses crimes, proporcionando um ambiente cibernético mais seguro e regulado.

Embora se observe um avanço incremental na capacidade do sistema jurídico brasileiro de regulamentar atividades conduzidas no âmbito digital, a profundidade e amplitude desses progressos permanecem ainda ilimitados. Nesse contexto, a convenção de Budapeste se destaca, não apenas por proporcionar a classificação de uma gama diversificada de atividades maliciosas realizadas digitalmente, mas também por estabelecer uma abordagem mais eficiente na persecução penal e no compartilhamento de informações. Dado que muitas atividades no ciberespaço transcenderem as fronteiras geográficas, demandando a necessidade de uma resposta jurídica unificada e com maior celeridade.

Nesse sentido, a incorporação do Brasil à convenção de Budapeste emerge como um remédio pertinente para as deficiências legislativas existentes no cenário digital do país. Embora a construção de um sistema jurídico independente seja uma alternativa, a complexidade e os desafios associados, exacerbados pela polarização política e ideológica prevalente no Brasil, tornam essa opção menos atraente para o momento.

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 ao crime cibernético. Sendo signatários da convenção, o Brasil não apenas fornece um quadro jurídico reconhecido internacionalmente, mas também promove a cooperação internacional em matéria penal, oferecendo diretrizes valiosas para a criação e adaptação de futuras leis nacionais.

Contudo, é importante deixar claro que a adesão à convenção é apenas parte da solução. É essencial que o Brasil continue desenvolvendo uma legislação nacional robusta e apropriada que complemente as disposições do tratado e seja capaz de responder efetivamente às mudanças dinâmicas da criminalidade virtual no contexto internacional.

Ao projetar futuros cenários sobre o tema, torna-se necessário propor uma reflexão acerca da viabilidade de o Brasil ratificar o 2º protocolo adicional à convenção de Budapeste

que foi aberto para adesão em 2022. Este protocolo já foi atualizado e estipula mecanismos específicos para a colaboração direta entre as autoridades do Estado solicitante e o provedor de conteúdo no Estado acionado. Estão inclusos, dentre outras provisões, a emissão de determinações para a revelação de nomes de domínio e dados cadastrais de assinantes, bem como regulamentações para videoconferências e comitês conjuntos de inquérito. Tal estrutura revela uma constante e criteriosa atenção às evoluções internacionais, sempre almejando aprimoramentos na eficácia da persecução penal dos crimes cibernéticos[476].

REFERÊNCIAS

ABADE, DENISE NEVES. Direitos fundamentais na cooperação jurídica internacional: Extradição, assistência jurídica, execução de sentença estrangeira e transferência de presos. E-book [kindle]. São Paulo: Saraiva, 2013.

ALBUQUERQUE, Roberto Chacon de. A Criminalidade Informática. Sao Paulo: Juarez de Oliveira, 2006. Disponível em: https://core.ac.uk/download/pdf/185253434.pdf. Acesso em: 14 ago. 2023.
ALLE, SAULO STEFANONE. Cooperação jurídica internacional e auxílio direto ativo em matéria penal. Belo Horizonte: Arraes Editores, 2017.

ANANIAS, Ricardo A. R. e WANDERLEY, Lucas F. Delito Informático e a Lei 12.737/12(Lei Carolina dieckamnn). In: (Vários) Anais do IV Congresso De Ciências Jurídicas:Jurisdição, Estado e Cidadania e VII Encontro Científico do Curso de Direito. 2014
APPADURAI, A. (1996). Modernidade em Dispersão: Ensaios sobre as Artes e a Identidade Global. Editora UFMG.

ARAÚJO, A. L., & SILVA, M. R. (2021). Cibercrime no Brasil: Uma análise das práticas ilegais e suas complexidades no ambiente digital. Revista Brasileira de Segurança Cibernética, 8(2), 45-62.
ARAUJO, Nádia de. Cooperação jurídica internacional no Superior Tribunal de Justiça: Comentários à Resolução n. 9/2005. Rio de Janeiro: Renovar, 2010, p. 94.

[476] COUNCIL OF EUROPE. Second additional protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Estrasburgo: Council of Europe, 2021b. Disponível em: https://rm.coe.int/special-edition-second-protocol-en--2021/1680a69930. Acesso em: 14 set 2023

ARAUJO, Nádia. A importância da cooperação jurídica internacional para a atuação do estado brasileiro no plano interno e internacional. In: MANUAL DE COOPERAÇÃO JURÍDICA INTERNACIONAL E RECUPERAÇÃO DE ATIVOS. Cooperação em matéria penal. Brasília. Secretária Nacional de Justiça, 2008.

ARAS, Vladimir. Blog do Vlad. O crime de stalking do art. 147-A do Código Penal. [2021]. Disponível em: https://vladimiraras.blog/2021/04/01/o-crime-de-stalking-doart- 147-a-do-codigo-penal.

BARBAGALO, Fernando Brandini. Cibercriminalidade e crimes informáticos: uma aproximação entre a legislação italiana e brasileira. Pg05.

BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. Investigação Cibernética á Luz do Marco Civil da Internet. Sao Paulo: Brasport, 2016. 240 p. Disponível em: https://pt.scribd.com/read/405795372/Manual-de-Investigacao-Cibernetica-A-luz-do-Marco-Civil-da-Internet#. Acesso em: 14 ago. 2023.

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silvera. Manual de Investigação Cibernética: à Luz do Marco Civil da Internet. Rio de Janeiro: Editora Brasport, 2016. Ebook kindle, pg103.
BASTOS, Celso Ribeiro. Curso de Teoria do Estado e Ciência Política. São Paulo: Saraiva: 1999.

BECHARA, Fábio Ramazzini; FLORES, Dímitri Molina. Crimes cibernéticos: qual é o lugar do crime para fins de aplicação da pena e determinação da competência jurisdicional?.Revista Direito Mackenzie, v. 13, n. 2, p. 1-21, 2019.

BEDNAR, P.M.; KATOS, V.; HENNEL, C. Cyber-Crime Investigations: Complex Collaborative Decision Making. In: Third International Annual Workshop on Digital Forensics and Incident Analysis. WDFIA 2008. Malaga, Spain. 9 p. Disponível em: https://lucris.lub.lu.se/ws/files/5676843/5045156.pdf.

BOITEUX, Luciana. Crimes informáticos: Reflexões sobre a política criminal inseridas no contexto internacional atual. Revista Brasileira de Ciências Criminais. São Paulo: Revista dos Tribunais, 2004. p. 170.
BORTOT, Jessica Fagundes. Crimes cibernéticos: aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional. Virtuajus, v. 2, n. 2, p. 338-362, 2017.

BRANT, Cássio Augusto Barros. O microssistema do direito tecnodigital. Belo Horizonte, 2016.

BRASIL, Lei n. 14.132, de 31 de março de 2021. Disponível em: http://planalto.gov.br/ccivel_03/_Ato2019-20233/2021/Lei/L14132.htm.Acesso em ago. 2023.

BRASIL, Ministério da Economia. Organização para a Cooperação e Desenvolvimento Econômico – OCDE. Disponível em: http://www.fazenda.gov.br/assuntos/atuacao-internacional/cooperacao-internacional/ocde.

BRASIL. Código Eleitoral. Lei nº 4.737, de 15 de julho de 1965. Disponível em: https://www.tse.jus.br/legislacao/codigo-eleitoral/codigo-eleitoral-1/codigo-eleitoral-leinb0-4.737-de-15-de-julho-de-1965.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidente da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 14 ago. 2023.

BRASIL. Decreto Legislativo nº Nº 11.491, de 12 de maio de 2023: Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro

de 2001. Brasília, 12 maio 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-11.491-de-12-de-abril-de-2023-476680563. Acesso em: 28 ago. 2023.

BRASIL. Decreto-Lei 2.848 de 7 de dezembro de 1940. Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 25 jul. 2023.

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 12.737 de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 20 jul. 2023.

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.

BRASIL. Lei 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 jul. 2023.

BRASIL. Lei 13.105 de 16 de março de 2015. Código de Processo Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 17 jul. 2023.

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: 20 jul. 2023.

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.

BRASIL. Lei 13.964 de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/201/lei/l13964.htm. Acesso em: 21 jul. 2023.

BRASIL. Lei 14.132 de 31 de março de 2021. Acrescenta o art. 147-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de perseguição; e revoga o art. 65 do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14132.htm. Acesso em: 20 jul. 2023.

BRASIL. Lei 14.155 de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponívelem:https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 20 jul. 2023.

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 n. 12.965, de 23 de abril de 2014. Brasília, 2014. Disponível em: <http://www.planalto.gov.br/ccivel_03/_ato2011-2014/2014/Lei/L12965.htm. Acesso em 23ago.2023.
BRASIL. Ministério da Justiça. Cartilha de Cooperação Jurídica Internacional em Matéria Penal. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-protecao/lavagem-de-dinheiro/drci/publicacoes/manuais/cooperacao-juridica-internacional-em-materia-penal/cartilha-penal-09-10-14-1.pdf.

BRASIL. Ministério Público Federal. Procuradoria-Geral da República. Ofício nº 736/2020, de 30 de julho de 2020. Convenção sobre o Crime Cibernético. Brasília, DF: Ministério Público Federal, 2020. Disponível em: http://www.mpf.mp.br/pgr/documentos/Oficio736DaviAlcolumbre.pdf. Acesso em: 01 mai. 2021.

BRASIL. Superior Tribunal de Justiça. Habeas-corpus nº 76689/PB, da 1ª Turma, Brasília, DF, 22 de setembro de 1998. Disponível em: ttps://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=76856.

BRASILEIRO, Anaís Eulálio. A cooperação jurídica internacional no terrorismo. 2018. Dissertação de Mestrado. Brasil.

CABETTE, Eduardo Luiz Santos. Jogo da Baleia Azul: Tipificação penal e competência para processo e julgamento. 2017. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2017/04/24/jogo-da-baleia-azul-tipificacao-penal-e-competencia-para-processo-e-julgamento/. Acesso em: 14 ago. 2023.

CAPEZ, Fernando; PRADO, Stela. Código Penal Comentado. 5. ed. São Paulo: Saraiva, 2014.

CAIADO, F.; CAIADO, M. Combate à pornografia infantojuvenil com aperfeiçoamentos na identificação de suspeitos e na detecção de arquivos de interesse. In: ministério público federal. Crimes cibernéticos. Brasília: MPF, 2018. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos.
Câmara dos Deputados da República Federativa do Brasil (1999), "Projeto de Lei nº 84/1999", http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028, acesso em set, 2023.

COIADO, Renata; SANI, Ana Isabel. Criminalização do stalking no Brasil. Revista LEX de Criminologia & Vitimologia, v. 3, n. 1, p. 73-102, 2021

CARNEIRO, Lucas Vitor Vitório; SANTOS, Jackson Novaes; EDLER, Gabriel Octacilio Bohn. direito cibernético: o impacto gerado pela lei carolina dieckmann no combate aos crimes virtuais realizados contra as crianças e adolescentes. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 8, n. 11, p. 2061-2080, 2022.

Carolina Dieckmann fala pela 1ª vez sobre fotos e diz que espera "justiça". G1, São Paulo. 14 maio 2012. Disponível em: . Acesso em: 30 jul. 2017.

Cartilha de segurança para internet: Ransomware. Disponível em: https://www.cert.br/

CASTELLS, M. A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar, 2003

CASTELLS, Manuel. A era da informação: economia, sociedade e cultura. Paz e Terra, 23ª edição, Rio de Janeiro, 2021.

CASTELLS, Manuel. A era da informação: economia, sociedade e cultura. Vol. 2 – A sociedade em Rede. Paz e Terra. 1999.

CASTRO, José Roberto Wanderley. a tipicidade dos crimes cibernéticos no direito penal brasileiro: um estudo sobre o impacto da lei 12.737/2012 e a (des)construção de uma dogmática penal dos crimes cibernéticos. Tese. Programa de Pós-Graduação em Direito do Centro de Ciências Jurídicas/Faculdade de Direito do Recife da Universidade Federal de Pernambuco. Recife. 2018.

CASTRO, Luís Fernando Martins. Direito da informática e do ciberespaço. Revista de Derecho. Informático. n. 064, novembro 2003. Disponível em: <http://www.alfa-redi.org/rdi-articulo.shtml?x=1270>.Acesso em: 3 abr.2009.

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.

CERQUEIRA, Tarcisio Queiroz. O Direito do ciberespaço. Jus Navigandi, Teresina, 1 nov. 1999. Disponível em: https://edisciplinas.usp.br/pluginfile.php/114200/mod_resource/content/1/O%20Direito%20do%20ciberespa%C3%A7o%20-%20Revista%20Jus%20Navigandi%20-%20Doutrina%20e%20Pe%C3%A7as_Tarciso%20Cerqueira.pdf. Acesso em: 16 maio 2023.

CERT.BR, Centro de estudos, resposta e tratamentos de incidentes de segurança no brasil.

CERVINI, Raul; TAVARES, Juarez. Princípios da cooperação judicial penal internacional no protocolo Mercosul. São Paulo: RT, 2000.

CIBERCRIME, NA CONVENÇÃO SOBRE O. VLADIMIR CHAVES DELGADO. 2007. Tese de Doutorado. Centro Universitário de Brasília.pg154.

CLOUGH, Jonathan. A world of difference: the Budapest Convention on cybercrime and the challenges of harmonisation. 2014. Monash University Law Review, vol. 40, nº.3, p. 698-736.

COLLI, Maciel. Cibercrimes. Limites e perspectivas à investigação policial de crimes cibernéticos. Curitiba: Juruá Editora, 2010. P. 160.

COLTRO, Rafael Khalil; WALDMAN, Ricardo Libel. CRIMINALIDADE DIGITAL NO BRASIL: A PROBLEMÁTICA E A APLICABILIDADE DA CONVENÇÃO DE BUDAPESTE. Revista Em Tempo, v. 21, n. 1, p. 104-123, 2021.

CONCI, Luiz Guilherme Arcaro. O controle de convencionalidade como parte de um constitucionalismo transnacional fundado na pessoa humana. Revista de Processo. Vol. 232/2014, Jun/2014, p. 363.

CONSELHO DA EUROPA. Convenção Europeia, de 04 de novembro de 1950. Convenção Para A Proteção dos Direitos do Homem e das Liberdades Fundamentais. Disponível em:https://rm.coe.int/16802fa428. Acesso em 14 ago.2023.

COUNCIL OF EUROPE. Second additional protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Estrasburgo: Council of Europe, 2021b. Disponível em: https://rm.coe.int/special-edition-second-protocol-en--2021/1680a69930.

Acesso em: 14 set 2023

COUNCIL OF EUROPE. Convention on cybercrime: Special edition dedicated to the draft-ers of the Convention (1997-2001). Estrasburgo: Council of Europe, 2021a. Disponível em: https://rm.coe.int/special-edition-budapest-convention-en-2022/1680a6992e. Acesso em: 14 set 2023.

CONTE, Christiany Pegorari. Jurisdição e competência nos crimes informáticos. Revista Brasileira de Meio Ambiente Digital e Sociedade da Informação, v. 1, n. 1, p. 49-208, 2014.

CONTE, Christiany Pegorari; FIORILLO, Celso ANTONIO Pacheco. CRIMES NO MEIO AMBIENTE DIGITAL. 2. ed. Sao Paulo: Saraiva, 2016.

COUNCIL OF EUROPE. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows.

CRESPO, Marcelo Xavier de Freitas. Crimes Digitais. São Paulo: Saraiva, 2017.

CUNHA, Rogério Sanches, Manual de Direito Penal: Parte Especial (arts. 121 ao 361). 11. ed. Salvador: JusPODIVM, 2019.

CUNHA, Rogério Sanches, Manual de Direito Penal: Parte Especial (arts. 121 ao 361). 11. ed. Salvador: JusPODIVM, 2019. Pg. 136

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

DAOUN, Alexandre Jean. Crimes informáticos. In: Blum, Renato M. S. Opice (coord). Direito Eletrônico: a internet e os tribunais. Baruru: Edirpo, 2001.

DE ARAÚJO ALVES, Matheus. Crimes Digitais: análise da criminalidade digital sob a perspectiva do Direito Processual Penal e do Instituto da Prova. Editora Dialética, 2020,pg 23, Ebook kindle

DIAS, Vera Elisa M. A Problemática da Investigação do Cibercrime. 2010. Disponível em www.verbojuridico.net/doutrina/2011/veradias_investigacaocibercrime.pdf>. Acesso em 20 de maio de 2018.Disponível em: <http://www.infobrasil.inf.br/userfiles/26-05-S5-2-68766-Investigacao Digital.pdf>.

DOMINGOS, Fernanda Teixeira Souza; RODER, Priscila Costa Shreiner. Obtenção de provas digitais e jurisdição na internet. São Paulo: EMAG, 2017.
Estatuto da Criança e do Adolescente: Lei federal nº 8069, de 13 de julho de 1990. Rio de Janeiro: Imprensa Oficial, 2002. BRASIL.

EUROPE, Council Of. CONSELHO DA EUROPA: quem somos. QUEM SOMOS. 2023. Disponível em: https://www.coe.int/pt/web/about-us/who-we-are. Acesso em: 28 ago. 2023.

FERREIRA, Ivette Senise. A Criminalidade Informática. In: LUCCA, Newtow de; SIMÃO FILHO, Adalberto (Coord.). Dirieto & Internet – Aspectos Jurídicos Relevantes. São Paulo: Edipro, 2001FILHO, Adalberto (Coord.). Dirieto & Internet – Aspectos Jurídicos Relevantes. São Paulo: Edipro, 2001. p 207-237.

FIGUEIREDO, Alani Caroline Osowski; RIOS, Rodrigo Sánchez. Proteção de dados pessoais e direitos fundamentais: desafios frente à cooperação jurídica internacional em matéria penal. Revista Científica do CPJM, v. 2, n. 07, p. 114-129, 2023.

FIORILLO, Celso Antônio Pacheco. Princípios constitucionais do direito da sociedade da informação: a tutela jurídica do meio ambiente digital. Saraiva Educação SA, 2017. Ebook Kindle
FRAGOSO, Suely. Realidade Virtual e Hipermídia - somar ou subtrair? São Leopoldo: Cyberlegenda nº 9, 2002. Disponível em:<http://www.uff.br/mestcii/sueli1.htm>. Acesso em: 1 set.2023.

FREITAS, Eduardo de. "G-8"; Brasil Escola. Disponível em: https://brasilescola.uol.com.br/geografia/g8.htm. Acesso em 08 de setembro de 2023.

FREITAS, Sérgio Henrique; Reis, Cristianne, et.al. A INTERPOL E O COMBATE AOS CRIMES TRANSNACIONAIS. Disponível em: https://www.defesa.gov.br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/XV_cadn/a_interpol_e_o_combate_aos_crimes_transnacionais.pdf.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. Anuário Brasileiro de Segurança Pública. Dados estatísticos. Atualizado em: 22/08/2022. Disponível em: https://forumseguranca.org.br/anuario-brasileiro-seguranca-publica/ Acesso em 22 set 2023.

GAVISON, R., & MINTCHEV, V. (2022). Transnational Cybercrime: Rethinking Global Cooperation. Boston University International Law Journal, 40(1), 1-32.
GENNARINI, Juliana Caramigo. A criminalização do Stalking. Direito Penal e Processo Penal, v. 3, n. 1, p. 67-79, 2021.

GIBSON, Willian. Neuromancer. São Paulo: Aleph, 2003, pg 381. Ebook Kindle

GLENNY, Misha. McMáfia: o crime organizado sem fronteiras. Porto: Civilização Editora, 2008.

GOUVÊA, Sandra. O direito na era digital: crimes praticados por meio da informática. Maual Editora Ltda, 1997.

GRECO, R. Curso de direito penal: parte especial. 13. ed. Niterói: Impetus, 2016. v. 2.

GRINOVER, Ada Pellegrini. As garantias processuais na cooperação internacional em matéria penal. In: Revista Forense, vol. 373, ano 100, Rio de Janeiro: Forense, maio/jun. 2004. p. 4-5.

GUEIROS, Artur; JAPIASSÚ, Carlos Eduardo. Direito penal: volume único. São Paulo: Atlas, 2018.

GUIDI, GUILHERME BERTI DE CAMPOS. provas no estrangeiro Cloud Act and the reflections on the systematics of evidence collection abroad. Revista de Direito, v. 2019, p. 07-08.

GUIDI, Guilherme Berti de Campos; REZEK, Francisco. Crimes na internet e cooperação internacional em matéria penal entre Brasil e Estados Unidos. Rev. Bras. Polít. Públicas, Brasília, v. 8, nº 1, 2018. p.276-288. https://doi.org/10.5102/rbpp.v8i1.5130. Disponível em: https://www.publicacoesacademicas.uniceub.br/RBPP/article/viewFile/5130/3713. Acesso em: 20 jul. 2023.

HAN, B.-C. Sociedade do cansaço. 2. ed. Petrópolis: Vozes, 2017. Disponível em: https://edisciplinas.usp.br/pluginfile.php/5000148/mod_resource/content/1/Sociedade%20do%20cansa%C3%A7o.pdf. Acesso em: 14 ago. 2023.

HUNGRIA, Nelson . Comentários ao Código Penal. 4º ed. Rio de Janeiro: Forense, 1958, Vol. 1.

JAPIASSÚ, Carlos Eduardo Adriano. O Direito Penal Internacional. São Paulo. Tirant lo Blach, 2020.

JAPIASSÚ, Carlos Eduardo A. O direito penal internacional e os crimes internacionais. Revista Interdisciplinar do Direito-Faculdade de Direito de Valença, v. 9, n. 1, p. 69-90, 2012.

JESUS, Damásio Evangelista de; MILAGRE, José Antônio. Manual de Crimes Informáticos. 1ª ed. São Paulo: Saraiva, 2016. *E-book Kindle.*

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: 03 set.2023.

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.
KUMMER, Fabiano R.DIREITO PENAL NA SOCIEDADE DA INFORMAÇÃO. Paraná: E-book Kindle, 2017.

LA CHAPELLE, Bertrand; FEHLINGER, Paul. Jurisdiction on the internet: from legal Arms race to to transnational cooperation. Internet & jurisdiction. Paper series, n 28, April 2016. Disponível em: www.internetjurisdiction.net. Acesso em 14 ago 2023.

LEONARDI, Marcel. Fundamentos de Direito Digital. Revista dos Tribunais. São Paulo. 2019. *Ebook Kindle.*

LÉVY, Pierre. Cibercultura. São Paulo: Editora 34, 2010. Pg15.

LIMA, Luciano Flores de (Org.). Cooperação Jurídica Internacional em matéria penal. Porto Alegre: Verbo Jurídico, 2010.

LIMA, Paulo Marco Ferreira. Crimes de Computador e Segurança Computacional. São Paulo: Editora Atlas.

MALAQUIAS, Roberto Antônio Darós. Crime Cibernético e Prova – A investigação criminal em busca da verdade. Curitiba: Juruá Editora, 2012.

MALDONADO, Laura Braga; SOTERO, Andrea Luiza Escarabelo. Aplicabilidade da Lei Geral de Proteção de Dados Pessoais Lei 13.709/18—sanções administrativas e criminais. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, v. 7, n. 3, p. 221-229, 2021

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-específica-2. Acesso em 14 de abr. 2023.

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. ago. 2023.

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.

MINISTÉRIO DA JUSTIÇA. Manual de Cooperação Jurídica Internacional. Matéria Penal e

Recuperação de Ativos, 4. ed. Brasília, 2019. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-protecao/lavagem-dedinheiro/institucional-2/publicacoes/manuais/cooperacao-juridica-internacional-em-materia-penal/manual-penalonline-final-2.pdf. Acesso em: 27 abr. 2023, p. 10.

MIRABETE, Julio Fabbrini. Manual de direito penal: parte geral. 23. ed. São Paulo: Atlas, 2006. Vol. 1. Revista e atualizada por Renato N. Fabbrini.

MURATA, Ana Maria Lumi Kamimura; TORRES, Me Paula Ritzmann. A convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora? Boletim IBCCRIM, v. 31, n. 368, 2023. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/575/108.

NASCIMENTO, Samir de Paula. Cibercrime: Conceitos, modalidades e aspectos jurídico-penais. Revista Âmbito Jurídico, 3 set. 2019. Internet e Informática. Disponível em: https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime.

NETO, Arnaldo. Cibercrime e Cooperação Penal Internacional: Um Enfoque à Luz da Convenção de Budapeste,p. 121. Disponível em: < http://www.egov.ufsc.br/portal/sites/default/files/arnaldo-sobrinho-cibercrime-e-cooperacaopenal-internacional.pdf >. Acesso em 30 abr. 2023.

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-cre sceram-94.

PEREIRA, Evandro della Vecchia. Investigação Digital: conceitos, ferramentas e estudos de caso. 2010.

PIMENTEL, Alexandre Freire. Direito cibernético: um enfoque teórico e lógico-aplicativo. Rio de Janeiro: Renovar, 2000.

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

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/#:~:text=**Por%20Patr%C3%ADcia%20Peck%20%E2%80%93%20Sobre,trazemos%20por%20decreto%20para%20c%C3%A1. Acesso:10. mai. 2023.

PINHEIRO, Patrícia Peck. Proteção de dados pessoais: Comentários à lei n. 13.709/2018-lgpd. Saraiva Educação SA, 2020. pg 1488.

PINHEIRO, Patrícia Peck; HAIKAL, Victor Auilo. A nova lei de crimes digitais. 2013. Disponível em: <www.pppadvogados.com.br/Publicacoes.aspx?v=1&nid=1432>. Acessado em:14/05/2023.

PORTUGAL. Lei de Cooperação Judiciária Internacional em Matéria Penal (lei n. 144/99, de 31 de agosto). Disponível em: http://www.gddc.pt/legislacao-linguaportuguesa/portugues/Lei144-99rev.html. Acesso em: 22/03/2007.

QUEIROZ, Claudemir; VARGAS, Raffael. Investigação e perícia forense computacional. Certificações, Leis processuais e estudos de caso. São Paulo: Brasfort, 2010.

ROCHA, Carolina Borges. A evolução criminológica do Direito Penal: Aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012. Jus Navigandi, Teresina, ano, v. 18, 2013.

ROHRMANN, Carlos Alberto. Curso de direito virtual. Belo Horizonte: Del Rey, 2005.
SANCHES, A. G.; ANGELO, A. E. 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/1> Acesso em: 03 jan. 2021.

SIEBER, Ulrich. Legal aspects of computer-related crime in theinformation society – Comcrime-Study. União Europeia,Universidade de Wüerzburg. Versão 1.0, jan. 98. Archivi Del Novento . Disponível em: http://www.archividelnovecento.it/archivinovecento/cappato/C12Dirittiumanipaesiextracom/DonneAfghanistan/Desktop/sieberem: 3 ago 2023.

SILVA, Marco Antonio Marques da; FREITAS, Jayme Walmer de. Código de Processo Penal comentado. São Paulo: Saraiva, 2012.

SILVA, Nathália Sueli Meneguetti; FLORINDO, Susam Carla Oliveira Dionizio; SACRAMENTO, Karina Adriana. Da (in) efetividade da aplicação da lei n° 14.132/2021 no brasil. Facit Business and Technology Journal, v. 2, n. 42, 2023

SOUZA, Solange Mendes de. Cooperação jurídica penal no Mercosul: novas possibilidades. Rio de Janeiro: Renovar, 2001.

SOUZA, Thiago. História da internet. Disponível em ttps://www.todamateria.com.br/historia-dainternet/. https://www.todamateria.com.br/historia-da-internet. Acesso em 14 abr. 2023.

SPINIELI, Andre Luiz Pereira. Crimes Informáticos: Comentários ao projeto de lei nº 5.555/2013. 3. ed. Brasilia: Ministério Público Federal, 2018. (Crimes Cibernéticos - Coletãnea de artigos). Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos.
Strasbourg, 8.XI.2001. Disponível em: http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm. Acesso em: 03/09/2023.

TAVORA, Nestor; ALENCAR, Rosmar Rodrigues. Curso de Direito Processual Penal. Salvador: Jus Podivm, 2012. p. 383.

THEOPHILO JÚNIOR, Roque. Cibernética Tecnologia e Psicologia. São Paulo, Academia Brasileira de Psicologia, 2000. Disponível em: <http://www.psicologia.org.br/internacional/ap11.htm>.
TIEDEMANN, Klaus. Lecciones de derecho penal económico. Barcelona: PPU, 1993.

TROTTA, Sandro Brescovit; FERREIRA, Luciano Vaz. Cooperação jurídica internacional em matéria penal: contornos históricos. Sistema Penal & Violência, v. 5, n. 1, 2013.

TRUMAN, Jennifer L.; MORGAN, Rachel E. Stalking Victimization, 2016. U.S. Departmentof Justice, 2021. Disponível em: [https://www.bjs.gov/content/pub/pdf/sv16.pdf].stalking e cyberstalking: considerações críticas sobre o delito tipificado no art. 147-a do código penal brasileirO. Pg. 14 Acesso em: 21.09.23.

VERONESE, Alexandre. CALABRICH, Bruno. Cybercrime in Brazil After the COVID-19 Global Crisis: An Assessment of the Policies Concerning Internacional Cooperation for Investigations and Prosecutions. 2022.

VERONESE, Alexandre. Cooperação jurídica e proteção de dados pessoais – A necessidade de inserção do Brasil nos tratados do Conselho da Europa. Disponível em: < https://www.jota.info/opiniao-eanalise/colunas/judiciario-e-sociedade/cooperacao-juridica-e-protecao-de-dados-pessoais-12042019>. Acesso em 08 maio 2023.

VERVIEW, Global. Essential Digital Headlines: overview of the adoption and use of connected devices and services. Overview Of The Adoption And Use Of Connected Devices And Services. 2023. Disponível em: https://www.amper.ag/post/we-are-social-e-hootsuite-digital-2023-visao-geral-global-resumo-e-relatorio-completo. Acesso em: 15 ago. 2023.

VIANA, Tulio; MACHADO, Felipe. Crimes informáticos. Belo Horizonte: Fórum, 2013.

VIANNA, Túlio Lima. Fundamentos de direito penal informático: do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense.

WANG, Qianyun. A Comparative Study of Cybercrime in Criminal Law: China, US,England, Singapore and the Council of Europe. Tese (doutorado) – Erasmus University.Rotterdam. Rotterdam, 2016, pg 15.

WEBER, Patrícia Maria Núñez. Cooperação internacional penal: conceitos básicos. Temas de Cooperação Internacional: Coleção MPF Internacional, Brasília, v. 2, n. 2, p. 1-248, 2015. Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/temas-de-cooperacao-internacional-1a-edicao. Acesso em: 14 ago. 2023.

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

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=10aa7f8b3c7 c. Acesso em: 15 mai. 2023.

WERMUTH, Maiquel Ângelo Dezordi. STALKING E CYBERSTALKING: CONSIDERAÇÕES CRÍTICAS SOBRE O DELITO TIPIFICADO NO ART. 147-A DO CÓDIGO PENAL BRASILEIRO. Revista Brasileira de Ciências Criminais, v. 186, n. 2021, p. 105-126, 2021.,