UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE DIREITO
DEPARTAMENTO DE CIÊNCIAS PENAIS

MATHEUS SCHULTZ ZAMBONATO

AVANÇOS DA LEGISLAÇÃO BRASILEIRA NO COMBATE AOS CRIMES CIBERNÉTICOS

Porto Alegre
2022

Matheus Schultz Zambonato

AVANÇOS DA LEGISLAÇÃO BRASILEIRA NO COMBATE AOS CRIMES CIBERNÉTICOS

Trabalho de Conclusão de Curso apresentado ao Departamento de Ciências Penais da Faculdade de Direito da Universidade Federal do Rio Grande do Sul como requisito parcial para a obtenção do grau de Bacharel em Ciências Jurídicas e Sociais.

Orientador: Prof. Dr. Ângelo Roberto Ilha da Silva.

Aprovado em 10 de outubro de 2022.

BANCA EXAMINADORA:

_____
Prof. Dr. Ângelo Roberto Ilha da Silva - UFRGS
Orientador

_____
Prof. Dr. Marcus Vinícius Aguiar Macedo - UFRGS
Membro da banca

_____
Prof. Dr. Mauro Fonseca Andrade - UFRGS
Membro da banca

AGRADECIMENTOS

Agradeço aos meus pais, Jonas e Elaine, por todo apoio e incentivo dado, que vai muito além desta etapa acadêmica. Obrigado por mostrarem a importância do estudo e da educação, e por todo auxílio incondicional prestado durante minha trajetória do curso, seja na minha presença ou ausência.

Agradeço à minha irmã Mirela, já graduada nesta universidade pelo curso de Direito, pelos ensinamentos e dicas repassados durante este período, assim como pelo companheirismo no convívio longe de casa. Obrigado por servir de inspiração pessoal e profissional.

Agradeço aos amigos de Uruguaiana e de Porto Alegre, em especial aos colegas de aula, os quais ajudaram com o aprendizado e tornaram memorável este percurso.

Agradeço, por fim, a todos que contribuíram de alguma forma para minha formação acadêmica, deixando aqui registrado meu apreço pela Universidade Federal do Rio Grande do Sul.

RESUMO

O presente trabalho tem como objetivo examinar questões referentes ao crime cibernético e averiguar as mudanças realizadas na legislação brasileira para atuar no seu combate. Em um primeiro momento, a pesquisa busca compreender as origens da rede mundial de computadores, abordando o advento e evolução dessa ferramenta que serviu de meio para a prática de uma nova modalidade criminosa. Em seguida, é tratado do crime cibernético sob uma ótica geral, discutindo-se suas conceituações, classificações, sujeitos e demais características inerentes dessa prática delituosa. Ainda, são analisados os obstáculos enfrentados pelo Estado na persecução penal dos cibercrimes, os quais afetam diretamente o processo de investigação e repressão criminal. Por fim, é feito o exame das normas aplicáveis aos meios digitais, com enfoque nos avanços da legislação penal brasileira.

Palavras-chave: Direito digital. Crimes na internet. Avanços legislativos.

ABSTRACT

The present paper aims to examine issues related to cybercrime and investigate the changes made in Brazilian legislation to act in its fight. At first, the research seeks to understand the origins of the World Wide Web, addressing the advent and evolution of this tool that served as a means of a new criminal practice. Then, from a general pesperctive, cybercrime is evaluated through its concepts, classifications, subjects and other inherent characteristics. Also, the obstacles faced by the State in the criminal prosecution of cybercrimes are analyzed, those which directly affect the process of investigation and criminal prosecution. Finally, the rules applicable to digital media are viewed, with focus on the advances made in Brazilian criminal legislation.

Keywords: Digital law. Crimes on the Internet. Legislative accomplishments.

SUMÁRIO

1. INTRODUÇÃO

A internet surgiu, inicialmente, com o propósito de inovar a forma de comunicação dos militares dos Estados Unidos durante o período da guerra fria. Com o seu desenvolvimento e modernização no decorrer dos anos, essa ferramenta tecnológica transcendeu as suas pretensões originárias, transformando o cenário econômico, político e social, de modo que atualmente não é exagero argumentar que se tornou instrumento essencial da atividade humana.

É notório que o contínuo progresso da humanidade por meio da evolução tecnológica e científica provocam também mudanças expressivas na estrutura social. Nessa perspectiva, o advento da informática trouxe diversos benefícios à sociedade, mas também abriu caminho para a atuação de uma nova modalidade criminosa, até então desconhecida pelo Direito Penal.

Assim sendo, a presente monografia tem como objeto de estudo a criminalidade cibernética, espécie delituosa que possui como cerne o espaço virtual. Demonstra-se que esse ambiente interativo propiciou um novo local para a execução de crimes já existentes, bem como fez surgir novos ilícitos, praticados contra o sistema informatizado.

A pesquisa também trata da legislação brasileira e discute a respeito da sua transformação ao longo dos anos para combater as condutas criminosas praticadas pela internet. Verifica-se que a normatização do espaço cibernético é um dos maiores desafios que o Poder Público enfrenta, uma vez que seus usuários estão se adaptando constantemente, seja para o uso devido ou indevido das plataformas tecnológicas.

No capítulo inicial, são investigados a origem e o desenvolvimento da rede mundial de computadores, até o estágio de evolução atual. São apontados os impactos benéficos que essa tecnologia trouxe ao meio social, bem como seus aspectos negativos, no sentido de originar um ambiente sujeito a novas condutas criminosas.

Em um segundo momento, entra-se no tópico específico do crime cibernético, esclarecendo sua nomenclatura, conceito, classificações e sujeitos. Na sequência, são apresentadas as principais problemáticas enfrentadas pelos Estados no combate a essa nova natureza delitiva, como a questão do lugar do crime e a investigação e repressão criminal.

A parte final do trabalho se dedica à análise das normas aplicáveis aos meios digitais. Na esfera internacional, é abordada a Convenção de Budapeste, evento que resultou na celebração do primeiro instrumento internacional no combate à criminalidade cibernética.

Sob a ótica das normas nacionais, são investigadas as principais legislações que foram elaboraras com o intuito de enfrentar a criminalidade cibernética. Neste ponto, é constatado que a legislação brasileira, ainda que lentamente, vem se adequando no processo de investigação e punição dos transgressores virtuais.

A escolha da temática se justifica em razão da atualidade do assunto e de sua relevância jurídica, sobretudo quando se considera o papel de destaque que a internet assume em uma sociedade cada vez mais conectada e, por consequência, vulnerável a ataques criminosos.

Dessa forma, é de extrema importância que as modificações de hábitos da natureza humana sejam também acompanhadas por transformações na postura jurídica, para que assim o Direito possa atender aos interesses exigidos pela realidade moderna.

A metodologia adotada consiste na pesquisa bibliográfica, legislativa e jurisprudencial do tema, com a pretensão de expor os posicionamentos doutrinários no que tange às questões relacionadas aos crimes cibernéticos, assim como aos avanços das legislações pertinentes.

2. AVANÇOS TECNOLÓGICOS E IMPACTOS NO MUNDO JURÍDICO

Para compreender o fenômeno da criminalidade cibernética, mostra-se relevante primeiro abordar o contexto histórico da evolução tecnológica que culminou no surgimento da rede mundial de computadores, inovação que viabilizou um novo meio para a prática de atividades ilícitas, modificando substancialmente alguns conceitos tradicionais acerca da ideia de crime no âmbito do Direito Penal.

O alicerce do que hoje se concebe como internet deu-se no contexto da guerra fria, no auge da corrida espacial. Em 1957, a União Soviética fez o lançamento do primeiro satélite em órbita, o *Sputinik*, feito marcante que colocou o seu rival em xeque na disputa geopolítica. Em resposta, o Departamento de Defesa dos Estados Unidos criou a *Advanced Research Projects Agency* (ARPA), uma agência militar, com enfoque em desenvolver a ciência e tecnologia por meio de pesquisas, assim como prevenir ataques tecnológicos russos[1].

Entre os projetos que passaram a ser financiados estava a criação da computação interativa, com a implementação do uso de sistemas de tempo compartilhado, que buscava a interligação dos diferentes computadores do governo americano, idealizado como uma verdadeira simbiose entre o homem e a máquina[2].

Dessa forma, a pesquisa voltou-se ao aprimoramento das técnicas de comunicação de dados, acreditando-se na hipótese de que a integração computacional tornar-se-ia instrumento capaz de assegurar a integridade das informações militares sigilosas, até mesmo em eventuais ataques nucleares. Assim, foi criada a ARPANET, rede de computadores da ARPA, que propiciou, em 1969, o estabelecimento da primeira interconexão de computadores[3].

Na sequência, no início de 1972, foi arquitetado um programa para enviar e receber mensagens eletrônicas (e-mails) em razão da demanda que a ARPANET tinha de organizar os seus esforços internos entre os vários técnicos e cientistas. Diante disso, o fluxo de informações e o tráfego de dados foram crescendo gradualmente com a interconexão computacional[4].

---

[1] BRITO, Auriney. **Direito Penal Informático**. São Paulo: Saraiva, 2013, l. 325. E-book.

[2] VIEIRA, Eduardo. **Os bastidores da Internet no Brasil**. São Paulo: Manole, 2003. p. 5

[3] CASTELLS, Manuel. **A era da informação**: economia, sociedade e cultura. In: A Sociedade em rede. 5ª ed. São Paulo: Paz e Terra, 1999. v. 1, p. 61.

[4] CARVALHO, M. S. R. M. **A trajetória da Internet no Brasil**: do surgimento das redes de computadores à instituição dos mecanismos de governança. Tese (Mestrado) – Engenharia de Sistemas e Computação, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006. p. 40.

No entanto, a ARPANET ainda era uma rede muito restrita às universidades e entidades que possuíam ligação com os objetivos militares americanos, sem falar do dispendioso custo que era exigido para a manutenção dos equipamentos de comunicação. Foi somente com o desenvolvimento de outras redes de computadores que a internet começou a ganhar força e destaque universal.

Passou-se então à introdução de redes de domínio público, que acarretaram a desvinculação da internet aos laços estritamente militares, dando início ao processo de privatização. Neste compasso então que, em 1991, originou-se a World Wide Web (WWW), uma nova rede instituída inicialmente com enfoque acadêmico, que trilhou o seu percurso de desenvolvimento com seus recursos tecnológicos inovadores. Dentre eles, estava o sistema de hipertexto, recurso que propiciava a visualização de informações dispostas em documentos que integram referências internas para outros (hiperlinks), o que permitiu aos seus usuários realizarem, de maneira simples, a pesquisa de informações. Dentre esses e outros motivos, como o desenvolvimento de *softwares* práticos e baratos, a World Wide Web tornou-se a principal rede de acesso à internet, revolucionando a década de 1990 com sua expansão extraordinária[5].

À medida que a teia mundial se expandia, a comunidade em torno dela também crescia encontrando novos adeptos, de modo que se inaugurou uma verdadeira competição em busca do desenvolvimento de novas tecnologias, mediante a criação de servidores, browsers e demais programas que potencialmente agregavam valor ao uso da rede[6].

No Brasil, em 1995, a Internet teve grande impulso por meio da Empresa Brasileira de Telecomunicações (Embratel), que tentou ser o grande provedor da Internet comercial no Brasil. No entanto, a iniciativa não logrou êxito por conta da estratégia governamental da época, que tinha uma política de desestatização da economia, sobretudo no setor de telecomunicações. Com a saída da Embratel do meio, o Brasil viu-se com uma infraestrutura precária para atender às demandas dos usuários, impossibilitando muitos de acessar a rede. Dessa forma, coube às provedoras privadas de internet fornecer e desenvolver os serviços necessários para

[5] BRITO, Auriney. **Direito Penal Informático**. São Paulo: Saraiva, 2013. p. 24.

[6] CARVALHO, M. S. R. M. **A trajetória da Internet no Brasil**: do surgimento das redes de computadores à instituição dos mecanismos de governança. Tese (Mestrado) – Engenharia de Sistemas e Computação, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006. p. 152.

a utilização da plataforma, caminho este imbuído de percalços e desafios que tiveram que ser vencidos ao longo dos anos[7].

Assim como sucedeu ao redor do globo, a internet comercial brasileira rapidamente cresceu com a popularização da World Wide Web, período em que houve o chamado “boom da internet”. Com a ampliação do acesso da tecnologia à população, surgiram diversas lojas virtuais, sistemas de busca, sites e blogs de conteúdos diversos, o que permitiu a desvinculação da rede do meio estritamente acadêmico. De certo modo, a internet foi responsável por acelerar a globalização, visto que os países encontraram uma ferramenta capaz de transcender as fronteiras físicas, permitindo a aproximação das relações econômicas, políticas e sociais[8].

Nos tempos atuais, a internet adquiriu papel essencial no funcionamento da sociedade em geral, modificando os mais diversos setores. A interconectividade proporcionou uma revolução dos meios de comunicação, das relações interpessoais e negociais, da política, da economia, entre outros incontáveis ramos sociais.

A maioria dos serviços prestados pelo Governo, tais como saúde, educação, segurança pública, de alguma maneira passam pela etapa de informatização, seja pelo acesso ao serviço seja pela obtenção de dados e informações. Alguns Estados, inclusive, reconheceram a importância da democratização tecnológica e implementaram políticas de inclusão digital visando a estimular o direito de acesso às ferramentas digitais[9].

A tecnologia também trouxe grandes avanços no sentido de facilitar as atividades cotidianas desempenhadas pelo ser humano, que encontrou um meio prático e acessível para executar suas tarefas, deixando de lado a necessidade de deslocamento físico. Enfim, são inegáveis os benefícios que o espaço cibernético trouxe na questão de conveniência.

Porém, em contrapartida, essa mudança paradigmática de reorganização social produziu um novo espaço para a atuação da criminalidade, que por sua vez também se adaptou à evolução tecnológica. Pode-se dizer que a sociedade cibernética trouxe uma nova concepção acerca da ideia de jurisdição, na medida em

---

[7] CARVALHO, M. S. R. M. **A trajetória da Internet no Brasil**: do surgimento das redes de computadores à instituição dos mecanismos de governança. Tese (Mestrado) – Engenharia de Sistemas e Computação, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006. p. 163/164.

[8] VIEIRA, Eduardo. **Os bastidores da Internet no Brasil**. São Paulo: Manole, 2003. p. 11/17.

[9] BRITO, Auriney. **Direito Penal Informático**. São Paulo: Saraiva, 2013, l. 272. E-book.

que a presença física e o espaço não são mais essenciais para a realização de atos ou fatos jurídicos[10].

Com efeito, esse novo ambiente social ficou sujeito à conduta de alguns indivíduos que se valeram da anonimidade e da falta de regulação da rede para praticar atividades lesivas a direitos, criando um local de instabilidade e insegurança para o usuário comum. Neste aspecto, observa-se que a tecnologia propiciou um novo meio para a prática de crimes já tipificados, que agora passaram a ser executados por meio da interatividade eletrônica.

Com o aumento do armazenamento de dados e informações online, criminosos passaram a atentar contra os sistemas informáticos, conduta que naturalmente ainda não tinha sido concebida pela ordem jurídica vigente. Dessa forma, emergiu a necessidade do Direito tutelar esse espaço por meio da tipificação de novos crimes e regularização do uso da plataforma.

Sendo assim, levando em consideração o contexto atual de extrema dependência das tecnologias de informação, faz-se necessário que o Direito acompanhe as mudanças da realidade moderna por meio da instituição de normas jurídicas suficientes que abordem as nuances dessa modalidade delituosa capaz de provocar danos imensuráveis à coletividade.

[10] MALAQUIAS, Roberto Antônio Darós. **Crime cibernético e prova:** a investigação criminal em busca da verdade. Curitiba: Juruá, 2012. p. 20.

3. CRIMES CIBERNÉTICOS

3.1 Quanto à denominação

Inicialmente, a título de esclarecimento, impende destacar as principais denominações utilizadas pela doutrina, pelo meio jurídico e até mesmo pela mídia no que tange à terminologia dos crimes cibernéticos, tendo em vista a ausência de um consenso acerca da definição da nomenclatura.

Assim, há quem opte pelas seguintes expressões: crimes de computador, *cybercrimes*, *computer crimes*, *computing crimes*, delitos informáticos, crimes virtuais, crimes eletrônicos, crimes digitais, *infocrimes*, crimes perpetrados pela Internet.

Depreende-se que, apesar de serem designações distintas, parece adequado adotar o entendimento genérico e usual de que pretendem se referir ao mesmo tópico, isto é, às infrações penais cometidas no espaço cibernético ou em razão de sua utilização[11].

Nessa perspectiva:

> [...]não há uma nomenclatura sedimentada pelos doutrinadores acerca do conceito de crime cibernético. De uma forma ou de outra o que muda é só o nome atribuído a esses crimes, posto que devem ser observados o uso de dispositivos informáticos, a rede de transmissão de dados para delinquir, o bem jurídico lesado, e ainda deve a conduta ser típica, antijurídica e culpável[12].

Desse modo, as terminologias supracitadas são usadas como sinônimos no presente trabalho, de modo a evitar a repetição de palavras. Não obstante, reconhece-se o ponto de vista dos demais autores que preferem fazer a distinção específica dos termos.

3.2 Conceituação

Diante da emergente realidade tecnológica em que novas ações lesivas surgem em um ritmo acelerado, há grande dificuldade na questão de elaborar um conceito

---

[11] JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016. p. 49. E-book.

[12] SILVA, Patrícia Santos da; SILVA, Matheus Passos. **Direito e crime cibernético**: análise da competência em razão do lugar no julgamento de ações penais. Brasília: Vestnik, 2015. p. 39.

definitivo sobre o que é de fato um crime cibernético. Levando em conta a ausência de definição legal, coube à doutrina tentar estruturar a conceituação e classificação dos referidos delitos:

> Os crimes virtuais são todas as condutas típicas, antijurídicas e culpáveis praticadas com a utilização de computadores ou qualquer outro sistema de informática, sendo estes diversos e tendo como classificação mais aceita a distinção entre crimes cibernéticos puros/próprios ou impuros/impróprios, tendo o autor do crime como o agente ativo, popularmente conhecido como hacker ou cracker, e qualquer pessoa física ou jurídica ou uma entidade titular, pública ou privada, que sofra a ação ou sobre quem recaiu tal ação é o agente passivo do crime[13].

Em visão semelhante lecionam Damásio de Jesus e Jose Antonio Milagre[14], aduzindo que o elemento central que caracteriza o crime informático é o uso da tecnologia da informação, na medida em que é o instrumento empregado para a prática da infração penal, ou então o próprio bem jurídico ofendido:

> Conceituamos crime informático como o fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação. Decorre, pois, do Direito Informático, que é o conjunto de princípios, normas e entendimentos jurídicos oriundos da atividade informática. Assim, é um ato típico e antijurídico, cometido através da informática em geral, ou contra um sistema, dispositivo informático ou rede de computadores. Em verdade, pode-se afirmar que, no crime informático, a informática ou é o bem ofendido ou o meio para a ofensa a bens já protegidos pelo Direito Penal.

De acordo com Cassanti[15], é toda atividade em que um computador ou uma rede de computadores é utilizada como uma ferramenta, base de ataque ou como meio do crime. Na visão de Castro[16], "crime de informática é aquele praticado contra o sistema de informática ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e os perpetrados através de computador."

Com base nessas definições, é possível concluir de maneira geral que o raciocínio dos autores em relação à conceituação do crime cibernético se aproxima,

---

[13] WENDT, Emerson. JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos**: ameaças e procedimentos de investigação. 2ª ed. Rio de Janeiro: Brasport, 2013. p. 18.

[14] JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016. p. 49. E-book.

[15] CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais**. Rio de Janeiro: Brasport, 2014, p.6.

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

porquanto o entendem como uma conduta típica, antijurídica e culpável, realizada com o auxílio dos sistemas informatizados, ou diretamente praticada contra ele.

Em síntese, depreende-se que qualquer ação ilegal que se utiliza de recursos tecnológicos como meio para a prática delituosa, seja ela contra seja por meio de computadores e seus sistemas, pode ser caracterizada como crime cibernético.

3.3 Classificações

Diante do surgimento dessa nova modalidade delituosa, houve também a necessidade de classificá-la para fins didáticos. Portanto, a seguir abordar-se-á a vertente doutrinária que divide os crimes cibernéticos em próprios e impróprios, por se tratar de sistematização simples, abrangente e de amplo uso acadêmico pelos estudiosos do tema.

3.3.1 Crime cibernético próprio

Os crimes cibernéticos próprios são aqueles que necessitam do espaço virtual para serem praticados e consumados, ou seja, estão necessariamente relacionados com a utilização do sistema de informática. Portanto, o agente criminoso visa a atingir com sua conduta delituosa primordialmente os sistemas informatizados ou de telecomunicações de dados, valendo-se destes para a execução do crime[17].

Nesse sentido, constata-se que a principal característica dessa classe delituosa é a exigência que o sujeito ativo utilize o sistema informático como objeto e meio de sua conduta. Por conta disso, o sujeito ativo geralmente é dotado de conhecimentos técnicos especiais e avançados na área da computação.

Para melhor compreensão, citam-se como exemplos os crimes de invasão de dispositivo informático, obtenção e transferência ilegal de dados, interceptação de sistema eletrônicos.

Como se vê, são condutas que surgiram em decorrência do desenvolvimento e aperfeiçoamento da internet e suas tecnologias, que diretamente proporcionaram o advento de ilícitos penais até então desconhecidos pela norma vigente. Na verdade,

[17] MALAQUIAS, Roberto Antônio Darós. **Crime cibernético e prova:** a investigação criminal em busca da verdade. Curitiba: Juruá, 2012. p. 60.

algumas ações ainda não foram tipificadas, dado o constante aprimoramento das técnicas ilegais utilizadas pelos usuários criminosos.

Analisando os crimes dessa natureza, vislumbra-se a possiblidade de lesão de novos bens jurídicos, tais como as informações armazenadas (dados), a segurança dos sistemas de redes informáticas ou de telecomunicações. Sob essa ótica, revela-se imprescindível que o Direito Penal de a devida tutela aos novos interesses derivados da sociedade de informação, protegendo do mesmo modo os bens jurídicos tradicionais[18].

3.3.2 Crime cibernético impróprio

Os crimes cibernéticos impróprios, por sua vez, são aqueles que já estavam previamente tipificados no ordenamento jurídico, mas que agora são praticados com o auxílio da tecnologia. Destarte, tal classificação diz respeito aos ilícitos penais tradicionais que encontraram no âmbito virtual novo *modus operandi*[19].

Nesse grupo estão inseridos, por exemplo, os crimes de calúnia, injúria, difamação, ameaça, falsidade ideológica, estelionato, pornografia infantil e todos os demais delitos passíveis de serem praticados com a utilização da tecnologia de informação.

Com efeito, o bem jurídico protegido não é essencialmente a integridade da rede internacional de computadores, de seus sistemas ou de equipamentos de informática, os quais são atingidos de modo secundário, mas sim qualquer outro bem jurídico como a honra, a vida, a integridade física[20].

Em que pese os bens jurídicos visados na execução dos crimes impróprios já estarem protegidos na legislação, nada impede que se atribua tipificação própria à conduta agora praticada no meio digital, visando a garantir a sua adequação ao sistema jurídico.

Portanto, conclui-se que a distinção de crimes impróprios e próprios se faz com base nos meios necessários para a realização do crime e na categoria do bem jurídico lesado ou posto em perigo.

---

[18] CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011, p. 55.
[19] CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011, p. 89.
[20] SILVA, Ângelo Roberto Ilha da, *et al*. **Crimes Cibernéticos**. 2ª ed. Porto Alegre: Livraria do Advogado, 2018. p.105.

3.4 Sujeitos

Para que uma determinada ação seja considerada crime, necessário se faz a existência do sujeito ativo e do sujeito passivo. Nesse sentido, Nucci[21] pondera que o sujeito ativo "é a pessoa que pratica a conduta descrita pelo tipo penal", enquanto o sujeito passivo "é o titular do bem jurídico protegido pelo tipo penal incriminador, que foi violado".

Tratando-se de crime cometido por meio da informática, o sujeito ativo ganha algumas particularidades.

No que tange ao crime cibernético impróprio, não se nota grande diferença em comparação com o criminoso usual, na medida em que este apenas pratica sua conduta em outro meio, a exemplo dos crimes contra a honra. Aqui, basta que o transgressor tenha acesso à rede, sendo prescindível conhecimento profundo sobre o funcionamento dos sistemas informatizados.

De outra via, nos ilícitos classificados como próprios o responsável pela infração é normalmente amplo entendedor do mundo informático, tendo em vista a especialidade técnica exigida para a execução do crime, como nos casos de invasão de dispositivo eletrônico e obtenção ilegal de dados[22].

Na tentativa de enquadrar estes indivíduos em um grupo criminoso, há uma variedade de termos utilizados para se referir aos autores de condutas ilícitas no meio virtual. Dentre eles, os mais comuns são os *hackers* e *crackers*, os quais este trabalho irá se ater.

Os *hackers* e os *crackers* são muito semelhantes no quesito de possuir vasto conhecimento aprofundado em informática, sendo que a distinção principal se dá na finalidade de seus atos[23].

Desse modo, os *hackers* utilizam de seu domínio tecnológico para invadir sistemas privados, sem, entretanto, danificá-los. São usuários que identificam

---

[21] NUCCI, Guilherme de Souza. **Curso de direito penal**: parte geral: arts. 1º a 120 do Código Penal. Rio de Janeiro: Forense, 2017. p. 275/277.

[22] CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011, p. 97.

[23] ALMEIDA, Jessica de Jesus, *et al*. **Crimes cibernéticos.** Caderno de Graduação - Ciências Humanas e Sociais - UNIT - SERGIPE, *[S. l.]*, v. 2, n. 3, 2015. p. 226. Disponível em: https://periodicos.set.edu.br/cadernohumanas/article/view/2013. Acesso em: 1 set. 2022.

vulnerabilidades em softwares e tentam corrigir suas falhas, sendo que, por muitas vezes, trabalham em prol da segurança de dados em empresas.

Já a motivação dos *crackers* é primariamente criminosa, na medida em que buscam obter vantagem ilícita por intermédio de práticas que prejudicam empresas ou pessoas. Neste grupo estão inseridos os usuários que invadem sites e plataformas virtuais para auferir ganho monetário, normalmente também se apropriando de informações sigilosas.

No que diz respeito ao sujeito passivo, verifica-se que a vítima não ostenta denominação específica, tal qual ocorre no polo ativo. Apenas vale lembrar que o titular do bem jurídico lesado pode ser tanto pessoa física como também pessoa jurídica, exposto à interatividade dos meios eletrônicos.

4. DIFICULDADES NO COMBATE À CRIMINALIDADE VIRTUAL

4.1 Territorialidade e lugar do crime

A primeira questão essencial para punição de qualquer conduta criminosa é averiguar se ela é ou não alcançada pela lei penal brasileira. Neste ponto, importante ressaltar que o Código Penal consagrou o princípio da territorialidade em seu art. 5º, o qual prevê a aplicação da lei penal ao crime praticado dentro do território nacional.

No entanto, dada a conjuntura do ciberespaço, percebe-se que o poder-dever de punir do Estado teve que ser repensado para além dos parâmetros convencionais de território como espaço físico[24].

Na concepção de Miguel Reale Junior[25], território é definido como toda área pela qual o Estado exerce sua soberania, que compreende a área geográfica que assenta o país. Todavia, não se limita somente ao espaço terrestre, na medida em que também abrange a zona de fronteira, marcada por rios, lagos e mar, assim como o subsolo e o espaço aéreo.

Na mesma linha de raciocínio, Cláudio Brandão[26] assevera que a definição de território nacional já está exposta na norma legislativa. Portanto, o conceito de território não é geográfico, mas sim político-normativo: é o espaço no qual o Estado exerce a sua soberania.

Levando em consideração tais definições, e considerando que a sociedade digital rompe com as restrições territoriais presentes no mundo físico, constata-se que o ciberespaço constrói um novo ambiente, conhecido como rede, em que a localização da informação passa a ser o principal elemento identificador do território. Dessa forma, não sendo o ciberespaço de fato um território, caracteriza-se especificamente pelo fluxo de informações por intermédio de redes de comunicação[27].

Daí surge a dificuldade: como determinar o lugar da prática criminosa? A arquitetura aberta da internet propicia um ambiente transnacional que não se limita às

---

[24] CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011, p. 122.

[25] REALE JÚNIOR, Miguel. **Instituições de direito penal**. Rio de Janeiro: Forense, 2009. p. 105.

[26] BRANDÃO, Cláudio. **Curso de direito penal:** parte geral. Rio de Janeiro: Forense, 2010. p. 89/90.

[27] CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011, p. 122.

fronteiras estatais delimitadas geograficamente, o que resulta em obstáculos na verificação da jurisdição competente entre países.

Outrossim, a consumação de um crime praticado pela internet ocorre em todos os lugares do mundo em que essa conduta lesiva tenha se dado, o que geram diversos problemas de competência e de conflito de normas. Sobre esse tópico, assim reflete Patricia Peck Pinheiro[28]:

> Alguns outros princípios do Direito devem ser repensados dentro do escopo do Direito Digital, como o princípio da territorialidade. Onde fica a porta? Até onde um ordenamento jurídico tem alcance? O problema não está apenas no âmbito da Internet, mas em toda sociedade globalizada e convergente, na qual muitas vezes não é possível determinar qual o território em que aconteceram as relações jurídicas, os fatos e seus efeitos, sendo difícil determinar que norma aplicar utilizando os parâmetros tradicionais.

Portanto, os critérios usados para identificar a jurisdição competente de crimes tradicionais por muitas vezes não se adequam aos crimes informáticos, visto que estes têm como característica o fato de poderem ser cometidos à distância, produzindo efeitos em local distinto, em países diversos, gerando, assim, situações jurídicas plurilocalizadas e possivelmente conflitantes[29].

Assim sendo, a determinação do local do crime é assunto de diversos questionamentos dos operários do Direito. Acerca do tema, o Código Penal dispõe em seu art. 6º:

> Art. 6º - Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado.

Como se observa, o Brasil adotou a denominada teoria da ubiquidade, aplicada pela maioria dos países do mundo, que leva em consideração tanto o momento executivo quanto o consumativo do crime. Dessa forma, qualquer fragmento de conduta que tenha relação com o solo nacional faz incidir a aplicação da lei penal pátria.

Impende esclarecer, todavia, que o dispositivo não tem como objetivo o estabelecimento de competência de foro (reservado aos artigos 70 a 91 do Código de Processo Penal), na medida em que sua função é verdadeiramente a de abordar os

---

[28] PINHEIRO, Patricia Peck. **Direito digital**. 7ª ed. Saraiva, 2021. p. 54. E-book.
[29] KIST, Dario José. **Prova digital no processo penal.** Leme: JH Mizuno, 2019. p. 81.

denominados “crimes à distância”, ou seja, os delitos que atingem o território de dois ou mais países.

Em termos práticos, parece adequado inferir que a teoria da ubiquidade resolve todos os casos. Afinal, se o delito tiver sua conduta no Brasil ou o resultado real ou potencial projetado para dentro de nossas fronteiras, considera-se o delito praticado aqui.

No entanto, a solução é muito mais relativa do que se costuma pensar. À luz dessa problemática, leciona Spencer Toth Sydow[30]:

> A regra do Código Penal leva em consideração que delitos a distância são praticados por um sujeito, diretamente. Por impossibilidade histórica, não se levou em consideração que é possível programar e comandar para que um programa (Bot) fora de nossos domínios territoriais (e equivalentes) faça às vezes da conduta penalmente relevante, ficando a ação humana apenas mediatamente relacionada. Também, a regra parte do pressuposto que os efeitos jurídicos se dão no local em que o objeto material foi atingido, sem levar-se em conta que há transitoriedade de agente após o momento da conduta. Afora o fato de que na informática o local da conduta pode estar fora do país. Finalmente, não se levou em consideração que, na virtualidade, é possível obter resultados fora dos domínios territoriais com grande facilidade, mesmo que se busque ideologicamente ofender um bem jurídico brasileiro.

Não obstante, o Código Penal alcança a grande maioria das situações por meio da aplicação da teoria da ubiquidade. Porém, alguns doutrinadores ponderam que nosso diploma legal não seria suficiente para a solução do problema da aplicação da lei penal no espaço, tornando-a incerta e insegura no que tange aos crimes informáticos.

Dario José Kist[31] relata que não basta dizer que o local do crime é onde ocorreu o comportamento delitivo ou se observou o resultado, porque, no caso concreto, as peculiaridades inerentes a esse tipo de infração penal, em especial a sua plurilocalização, fazem com que em decorrência de um único fato sejam instaurados mais de um processo, ou até mesmo não seja instaurado nenhum, devido à dificuldade que se tem em definir qual das jurisdições pode ou deve atuar.

Celso Valin[32] aponta como melhor opção considerar-se como local do crime cibernético aquele em que está localizado o agente, porquanto compreende que o

---

[30] SYDOW, Spencer Toth. **Curso de direito penal informático**: partes geral e especial. 3ª ed. Salvador: Jvspodium, 2022. p. 321.

[31] KIST, Dario José. **Prova digital no processo penal**. Leme: JH Mizuno, 2019. p. 100/102.

[32] VALIN, Celso. **A questão da jurisdição e da territorialidade nos crimes praticados pela Internet.** Direito, sociedade e informática: limites e perspectivas da vida digital. Florianópolis: Fundação Boiteux, 2000. p. 116.

país do transgressor teria melhores condições de aplicar a sanção penal, evitando eventual discussão sobre extradição.

Por sua vez, Damásio de Jesus[33] entende que, para casos relacionados à internet, deveria ser adotado algo semelhante à teoria da atividade, a qual determina como sendo o local do crime aquele em que o agente praticou o delito.

Independentemente da postura adotada, a doutrina é uníssona ao tratar da necessidade de se firmar um documento internacional que aponte parâmetros globais a serem tomados, a fim de evitar que a criminalidade cibernética fique impune ou que venha a ser punida mais de uma vez, configurando *bis in idem*.

E para que haja essa cooperação entre os países, os tratados e as convenções internacionais possuem papel fundamental, tema este que será melhor analisado em capítulo posterior do trabalho.

Conclui-se, então, que o estudo da aplicação da lei penal no espaço não poderá mais ser realizado desconsiderando a existência do ciberespaço, meio em que a interatividade social ignora os contornos dos elementos físicos, no qual uma atividade criminosa pode se consumar em países diversos, a qualquer ou ao mesmo tempo, fragmentando-se o *iter criminis*[34].

4.2 Investigação e repressão criminal

As novas formas de se praticar crimes representam grande dificuldade para os órgãos de persecução penal, que devem ser instrumentalizados para o enfrentamento de todos os problemas penais relacionados com o tema, existentes e os que ainda surgirão. Nesse aspecto, relevante apontar os principais desafios para a investigação e repressão criminal dos crimes cibernéticos.

No direito digital, os *logs* e o endereço IP (internet protocol) são as principais evidências que devem ser coletadas para permitir efetiva investigação dos crimes virtuais. Uma vez que na rede impera a anonimidade, a obtenção destas informações servirá de norte para o processo de identificação da autoria.

Os *logs* consistem em arquivos de texto nos quais são registradas diversas informações relativas à utilização de internet pelo usuário (*log* de conexão) e à

[33] JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016. p. 62. E-book.

[34] BRITO, Auriney. **Direito Penal Informático**. São Paulo: Saraiva, 2013, l. 1583. E-book.

utilização de determinado serviço na internet (*log* de acesso). Dessa forma, apontam a data, horário, fuso horário, duração da conexão e o número do protocolo de internet (IP). Este último é uma representação numérica de onde um dispositivo está conectado à internet, sendo, portanto, instrumento essencial para a identificação da localização geográfica do usuário[35].

Em posse destas informações, os órgãos investigativos vão utilizá-las para identificar o criminoso. Então, será solicitado que o provedor de acesso à internet, o provedor de conteúdo, a *lan house* ou o administrador de rede privada informe os dados identificativos do computador e do indivíduo a quem foi atribuído o IP, consoante consta nas informações apresentadas pelo *log*[36].

Ocorre que a preservação da evidência em crimes praticados na internet é uma das grandes barreiras com que a investigação criminal se depara. O caminho é bem longo desde a procura da vítima na delegacia de polícia até a expedição da ordem judicial determinando ao provedor a disponibilização dos registros de conexão e acesso a aplicações de internet[37].

Desse modo, sem a cooperação dos provedores de Internet ou de serviços, é praticamente impossível apurar a autoria de delitos cibernéticos quando praticados de forma anônima. Até recentemente, antes da promulgação do Marco Civil da Internet, não havia previsão legal acerca da obrigação dos provedores a disponibilizar os registros e informações que permitam a identificação de algum usuário, o que dificultava imensamente o procedimento investigativo.

Além disso, devido à volatilidade dos dados da internet, estes podem ser facilmente manipulados, alterados ou deletados, dificultando a individualização da autoria e materialidade delitiva[38].

Aliás, a obtenção do IP permite a identificação de um computador e de seu usuário, o que não implica necessariamente a determinação do autor do delito. Assim, necessário se faz comprovar ainda que aquele usuário foi o responsável por perpetrar a conduta ilícita investigada, levando em conta que o dispositivo informático pode ser

---

[35] JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016. p. 184. E-book.

[36] WENDT, Emerson. JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos**: ameaças e procedimentos de investigação. 2ª ed. Rio de Janeiro: Brasport, 2013. p. 243.

[37] BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de investigação cibernética à luz do Marco Civil da Internet**. Rio de Janeiro: Brasport, 2016. p. 51.

[38] BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de investigação cibernética à luz do Marco Civil da Internet**. Rio de Janeiro: Brasport, 2016. p. 52.

utilizado por diversas pessoas bem como o endereço IP pode ser manipulado por criminosos experientes.[39]

Outrossim o criminoso cibernético possui inúmeras facilidades decorrentes da falta de estrutura estatal para coibir a delinquência virtual. A ausência de capacitação dos policiais e de outros atores da persecução penal, como o Ministério Público e o Judiciário, resulta em processos carentes de provas materiais, colaborando com a impunidade dos infratores[40].

A atividade estatal deve planejar e buscar treinamento constante para aperfeiçoar os seus agentes com técnicas e equipamentos modernos a fim de fazer frente aos cibercriminosos, de modo a reprimir e acompanhar a evolução desses crimes. De tal sorte, políticas internas e políticas públicas nacionais voltadas aos órgãos de segurança pública são bem-vindas e motivarão os estados a investirem na qualificação de seus quadros[41].

No mais, os meios de prova do crime cibernético se submetem às mesmas disposições dos processos tradicionais, de modo que o exame pericial, as inspeções judiciais e a busca e a apreensão são métodos eficientes na produção de prova, pincipalmente quando realizados por profissionais capacitados e familiarizados com o meio eletrônico[42].

---

[39] PINHEIRO, Patricia Peck. **Direito digital**. 7ª ed. Saraiva, 2021. p. 69. E-book.

[40] MALAQUIAS, Roberto Antônio Darós. **Crime cibernético e prova:** a investigação criminal em busca da verdade. Curitiba: Juruá, 2012. p. 63.

[41] WENDT, Emerson. JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos**: ameaças e procedimentos de investigação. 2ª ed. Rio de Janeiro: Brasport, 2013. p. 248.

[42] MALAQUIAS, Roberto Antônio Darós. **Crime cibernético e prova:** a investigação criminal em busca da verdade. Curitiba: Juruá, 2012. p. 83/84.

5. PRINCIPAIS NORMAS APLICÁVEIS AOS MEIOS DIGITAIS

5.1 Convenção de Budapeste

O Conselho da Europa é o pioneiro na elaboração da primeira convenção internacional a tratar especificamente do crime cibernético. Atualmente integrado por 46 (quarenta e seis) Estados Membros e 6 (seis) países observadores, consiste em organização internacional regional criada em 5 de maio de 1949, que atua na defesa da democracia e na proteção dos direitos humanos, sendo reconhecida tradicionalmente pela celebração de instrumentos multilaterais sobre cooperação internacional em matéria penal.

Realizada sob a chancela do Conselho da Europa, em 2001, na cidade de Budapeste, a Convenção sobre o Cibercrime, ou simplesmente Convenção de Budapeste, teve como objetivo principal a estruturação de uma política criminal internacional, protegendo a sociedade contra a criminalidade no espaço virtual por intermédio da adoção de normas e diretrizes que visaram a melhoria da cooperação entre os Estados signatários[43].

O evento aconteceu no dia 23 de novembro de 2001, dias após os atentados terroristas de 11 de setembro contra os Estados Unidos, o que fez crescer ainda mais a imensa preocupação internacional sobre o tema, tendo em vista que o serviço de inteligência do Pentágono não conseguiu interceptar as mensagens enviadas entre os terroristas via correio eletrônico[44].

Nessa perspectiva, a convenção foi profícua no sentido de delimitar competências e poderes suficientes para combater de modo eficaz tais crimes, tanto em nível nacional como internacional, facilitando a detecção, investigação e o procedimento criminal. Sobre o tópico, pondera Damásio de Jesus[45]:

> De forma a conjugar esforços no combate aos crimes eletrônicos, foi realizada a chamada Convenção de Budapeste, acerca de cibercrimes, no âmbito do concelho da Europa. Trata-se, pois, de documentação de Direito Internacional Público, elaborada por comitê de especialistas, no escopo de que os países signatários implementem normas de direito material que façam frente ao crime cibernético. Assim, tem-se como um acordo internacional (...)

[43] MALAQUIAS, Roberto Antônio Darós. **Crime cibernético e prova:** a investigação criminal em busca da verdade. Curitiba: Juruá, 2012. p. 212.

[44] BRITO, Auriney. **Direito Penal Informático**. São Paulo: Saraiva, 2013. l. 763. E-book.

[45] JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016. p. 55. E-book.

> que fixa diretrizes às políticas nacionais e propõe a harmonização das legislações para que se possa combater o cibercrime de maneira eficiente.

Sua idealização veio da necessidade global de frear a constante e crescente onda de ataques virtuais aos internautas e pessoas jurídicas utilizadoras da rede mundial de computadores, os quais se tornaram reféns dessa nova modalidade criminosa.

No que se refere a sua forma, o tratado se divide em quatro capítulos, assim elencados: 1) Utilização de terminologias; 2) Medidas a serem tomadas em nível nacional; 3) Cooperação internacional; e 4) Disposições finais. O documento contém 48 artigos redigidos em texto didático e objetivo[46].

No primeiro capítulo, a convenção trata da nomenclatura e significado dos termos concebidos em decorrência da evolução tecnológica. Dessa forma, define os conceitos de sistema informático, dados informáticos, dados de tráfego, fornecedor de serviço.

No segundo capítulo, em um primeiro momento, o instrumento legal aborda questões de direito material, recomendando às partes adotarem medidas legislativas destinadas a tipificar determinadas condutas que violam ou ameaçam a segurança informática, tais como interceptação ilegal, interferência de dados e sistema, acesso ilegal, falsidade informática, entre outras.

Aqui é importante frisar que o tratado não estabelece disposições de natureza penal, visto que somente propõe a promulgação de leis penais relacionadas a certas condutas realizadas pelo meio digital, resguardando a cada Estado subscritor a definição dos tipos penais e dosimetria das sanções aplicáveis, em respeito à autonomia e soberania de cada país.

Ademais, em análise dos dispositivos, denota-se que não há a previsão da hipótese culposa, ou seja, somente estão presentes condutas dolosas. A justificativa razoável para tanto seria o fato de que, muitas vezes, o usuário comum da internet não tem o conhecimento técnico para perceber que está contribuindo com uma fraude eletrônica, como nos casos de repasse de links e e-mails maliciosos[47].

---

[46] CONSELHO DA EUROPA. **Convenção sobre o Cibercrime**. Budapeste, 23.XI.2001. Disponível em: https://rm.coe.int/16802fa428. Acesso em: 16 set. 2022.

[47] 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.

Na sequência, a Convenção de Budapeste trata das normas procedimentais, pelas quais busca adaptar as medidas processuais clássicas, como a busca e apreensão, no ambiente eletrônico, além de apresentar novas medidas que auxiliam nas investigações, com enfoque na cooperação jurídica internacional e auxílio mútuo entre os países.

Passo seguinte, estabelece princípios norteadores para definição do local da prática dos crimes, propondo solução para o problema de aplicação da legislação no ciberespaço, inclusive aspectos para solucionar problemas de *bis in idem*, quando dois ou mais países estão envolvidos nos crimes, assim como a resolução de conflitos positivos e prevenção de conflitos negativos de jurisdição.

Em especial, o art. 22 propõe determinações legais a serem observadas a fim da correta aplicação da competência dos julgadores. O item 5 do referido dispositivo traz a possibilidade de diálogo entre as partes para averiguar a jurisdição competente. Assim, quando mais de um Estado signatário reivindicar competência sobre a conduta cibernética criminosa, estes irão se consultar a fim de determinar a jurisdição mais apropriada para o procedimento penal.

Percebe-se a importância desse instrumento internacional para dirimir questões voltadas à jurisdição criminal bem como viabilizar trâmites legais investigativos e processuais referentes aos delitos praticados na internet, cuja ação criminosa alcança diferentes territórios.

No terceiro capítulo, com o propósito de combater a criminalidade informática conjuntamente entre os Estados, a Convenção trata dos aspectos da cooperação internacional, elencando os princípios gerais e provisões especificas. Por derradeiro, em seu capítulo final, o tratado dispõe sobre os atos associados à execução do documento internacional, como assinaturas e entrada em vigor.

Em suma, vislumbra-se que o Conselho Europeu se debruçou sobre a temática buscando equacionar a tutela jurídica em consonância com a soberania dos países signatários. Nessa convenção, o espaço cibernético foi definido como um tipo de espaço comum que é usufruído por todos aqueles que trafegam na internet ao se conectarem aos serviços de comunicação e informação. Diante disso, tal convenção foi elaborada não somente para criar tipos penais, mas também para estipular normas

de processo penal, conciliar procedimentos de direito penal internacional e estabelecer acordos referentes à tecnologia da informação[48].

Deve ser ressaltado que a Convenção de Budapeste atualmente é o único instrumento jurídico de caráter global para combate suficientemente satisfatório e hábil da criminalidade cibernética. Embora seja alvo de algumas críticas, como não considerar as diferenças tecnológicas, políticas, sociais e econômicas de cada país, ainda assim é o documento mais coerente e célere sobre delitos informáticos atualmente. Nesse sentido, quanto mais Estados o ratificarem, melhor será o alcance e capacidade para o combate a essa nova modalidade delituosa[49].

O respectivo tratado entrou em vigor em 01 de julho de 2004 e atualmente conta com mais de 65 países signatários[50]. Todavia, o Brasil foi convidado para adesão à convenção somente em dezembro de 2019. Assim, em 2020 o Poder Executivo encaminhou ao Congresso Nacional o processo de ratificação legislativa do acordo (Mensagem nº 412/2020). O texto foi aprovado pela Câmara dos Deputados em 06 de outubro de 2021, mediante o Projeto de Decreto Legislativo nº 255[51].

Em seguida, o referido Projeto foi encaminhado ao Senado Federal, que aprovou a adesão do Brasil à Convenção de Budapeste. A matéria foi promulgada em 17 de dezembro de 2021, por meio do Decreto Legislativo nº 37/2021[52]. A matéria ainda depende de depósito, junto ao Conselho da Europa, do instrumento de ratificação e da posterior promulgação pela Presidência da República, por meio de Decreto, na forma do art. 84, *caput*, inciso IV, da Constituição da República.

---

[48] 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.

[49] CIDRÃO, Tais Vasconcelos*, et al*. **A Oportunidade e Necessária Aplicação do Direito Internacional nos Ciberespaços**: Da Convenção de Budapeste à Legislação brasileira. Brazilian Journal of International Relations, Marília, v. 7, ed. 1, p. 66-82, jan./abr. 2018, p. 78.

[50] COUNCIL OF EUROPE. **Convention on Cybercrime**, Chart of signatures and ratifications of Treaty 185. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185. Acesso em: 15 set. 2022.

[51] BRASIL. **Projeto de Decreto Legislativo nº 255, de 2021.** Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Brasília: Congresso Nacional, 2021. Disponível em: https://www.camara.leg.br/propostas-legislativas/2287513. Acesso em: 15 set. 2022.

[52] BRASIL. **Decreto Legislativo nº 37, de 2021**. Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Brasília: Diário Oficial da União, 17/12/2021. p. 7, col. 2. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/150258. Acesso em: 15 set. 2022.

Como se vê, a adesão do Brasil ao documento internacional foi extremamente tardia e grande parte de seu êxito se deu por conta de pressões feitas pelos órgãos do sistema judiciário, que há muito tempo solicitavam a adesão ao documento.

Nesse sentido, é o ofício do MPF[53] emitido pela Procuradoria-Geral da República, que com base nas notas técnicas produzidas pelo GACC - Grupo de Apoio sobre Criminalidade Cibernética sobre a Convenção de Budapeste ressalta a importância da adesão do Brasil à Convenção para moldar a forma da investigação e cooperação internacional nessa área e solicita mais celeridade no âmbito da tramitação legislativa.

A nota técnica mencionada alerta que os delitos cibernéticos não têm sido combatidos de forma eficiente pela falta de capacitação e ausência de ferramentas jurídicas aptas a permitir a persecução penal, o que acarreta o aumento da insegurança dos usuários brasileiros na internet e dificulta a prevenção de ataques e ocorrências.

Além disso, foi apontado no documento o aumento exponencial do número de crimes cibernéticos, com migração de delitos comuns para o meio digital. Ressaltou-se que a obtenção de provas digitais para comprovação da materialidade e autoria delitiva de diversos crimes, inclusive homicídios e corrupção, depende, muitas vezes, de interceptações telemáticas e arquivos hospedados em “nuvem”, o que se tornou rotina dentre os operadores do direito, os quais se deparam com diversos obstáculos.

Dessa forma, a conclusão da ratificação do acordo se mostra de extrema relevância, pois tal instrumento internacional poderá ser utilizado para suplementar a legislação nacional que ainda é deficiente na matéria, estabelecendo na seara criminal parâmetros mais concretos para a persecução penal dos crimes virtuais.

Para cumprir com o desiderato, deve-se fomentar a capacitação e aprimoramento dos agentes públicos que atuam na persecução de tais delitos, interligando os órgãos judiciários e investigativos em um regime internacional de combate ao cibercrime.

Em que pese o movimento para integrar a Convenção de Budapeste ser extremamente recente, o Brasil vem, ao longo dos anos, muito lentamente, adotando

---

[53] BRASIL. Ministério Público Federal. Procuradoria-Geral da República. **Ofício nº 736/2020**, **de 30 de julho de 2020**. Convenção sobre o Crime Cibernético. Brasília: Ministério Público Federal, 2020. Disponível em: http://www.mpf.mp.br/pgr/documentos/Oficio736DaviAlcolumbre.pdf. Acesso em: 15 set. 2022.

medidas legislativas em consonância com o respectivo tratado internacional, conforme se depreende da análise das legislações internas a seguir.

5.2 Lei nº 12.737/2012 - Lei Carolina Dieckman

A Lei nº 12.737, promulgada na data de 30 de novembro de 2012, é responsável por acrescentar na legislação penal os artigos 154-A e 154-B, que tipificam o crime de invasão de dispositivo informático e sua devida ação penal, respectivamente. A norma também criminaliza os hackers e aqueles que falsificam documentos particulares e cartões de créditos pela internet, por meio da alteração dos arts. 266 e 298 do Código Penal.

A Lei nº 12.737 ficou popularmente conhecida como Lei Carolina Dieckmann, em referência à atriz brasileira foi vítima da divulgação indevida de suas imagens íntimas, após hackers terem invadido os seus arquivos e acessado os seus dados. O ocorrido instigou grande debate popular sobre a criminalização desse tipo de prática, sendo amplamente repercutido pela mídia nacional, fator que contribuiu para a edição da norma referida.

Na mesma data foi também sancionada a Lei nº 12.375/2012, conhecida como Lei Azeredo. Contudo, não foi tão abrangente quanto pretendia em seu projeto inicial, dado que dois dos quatro artigos da Lei foram vetados. Assim, limitou-se a estabelecer regras de estruturação da polícia judiciária para o enfrentamento da criminalidade cibernética e incluir um novo dispositivo na Lei de Combate ao Racismo.

Como se percebe, a lacuna legislativa sobre a ausência de tipificação de crimes cibernéticos perdurou por mais de décadas, somente acontecendo em 2012, o que gerou impacto negativo na sociedade brasileira e na comunidade internacional, as quais há muito tempo urgiam pela regulação do tema.

Nesse sentido, há o princípio da legalidade, desmembrado em dois: o princípio da anterioridade da lei penal e o da reserva legal, os quais preceituam que não se pode imputar pena ao indivíduo por crime inexistente, tendo em vista a imprevisibilidade anteriormente definida em lei. Somado ao fato de o Direito brasileiro vedar analogia em prejuízo do acusado (*in malam parte*), pode-se verificar que a

ausência de tipificação legal contribuiu para reforçar ainda mais a prática dessas atividades delitivas, favorecendo a impunidade dos transgressores virtuais[54].

Portanto, a função punitiva estatal ficou limitada, fazendo com que condutas que tinham como alvo o sistema informatizado fossem consideradas atípicas. Como exemplo concreto, cita-se a decisão do STF[55] na qual a carência de norma penal sobre crime cibernético (invasão de dispositivo cibernético) serviu como fundamento para o indeferimento de ordem cautelar de prisão e extradição:

> EXTRADIÇÃO – PRISÃO CAUTELAR – PLEITO FORMULADO PELA INTERPOL – POSSIBILIDADE – INOVAÇÃO INTRODUZIDA PELA LEI Nº 12.878/2013 – DELITO INFORMÁTICO (CRIME DIGITAL): "INVASÃO DE DISPOSITIVO INFORMÁTICO" (CP, ART. 154-A, ACRESCIDO PELA LEI Nº 12.737/2012) – **FATO DELITUOSO ALEGADAMENTE COMETIDO, EM TERRITÓRIO AMERICANO (ESTADO DO TEXAS), EM 2011 – CONDUTA QUE, NO MOMENTO EM QUE PRATICADA (2011), AINDA NÃO SE REVESTIA DE TIPICIDADE PENAL NO ORDENAMENTO POSITIVO BRASILEIRO – O SIGNIFICADO JURÍDICO DO PRINCÍPIO CONSTITUCIONAL DA RESERVA DE LEI EM MATÉRIA DE TIPIFICAÇÃO E DE COMINAÇÃO PENAIS (CF, ART. 5º, INCISO XXXIX) – "NULLUM CRIMEN, NULLA POENA SINE PRAEVIA LEGE" – DUPLA TIPICIDADE (OU DUPLA INCRIMINAÇÃO): CRITÉRIO QUE REGE O SISTEMA EXTRADICIONAL – NECESSIDADE DE QUE O FATO SUBJACENTE AO PEDIDO DE EXTRADIÇÃO (OU AO PLEITO DE PRISÃO CAUTELAR PARA EFEITOS EXTRADICIONAIS) ESTEJA SIMULTANEAMENTE TIPIFICADO , NO MOMENTO DE SUA PRÁTICA, TANTO NA LEGISLAÇÃO PENAL DO BRASIL QUANTO NA DO ESTADO ESTRANGEIRO – PRECEDENTES – SITUAÇÃO INOCORRENTE NO CASO, POIS A CONDUTA PUNÍVEL IMPUTADA AO SÚDITO ESTRANGEIRO RECLAMADO SOMENTE PASSOU A SER CONSIDERADA CRIMINOSA, NO BRASIL, EM ABRIL DE 2013** (QUANDO SE ESGOTOU O PERÍODO DE "VACATIO LEGIS" DA LEI Nº 12.737/2012, ART. 4º), POSTERIORMENTE, PORTANTO, À DATA EM QUE FOI ELA ALEGADAMENTE PRATICADA NOS ESTADOS UNIDOS DA AMÉRICA – EVOLUÇÃO DO TRATAMENTO LEGISLATIVO, NO BRASIL, PARA FINS PENAIS, DOS CRIMES INFORMÁTICOS – OCORRÊNCIA, AINDA, NA ESPÉCIE, DE OUTRO OBSTÁCULO JURÍDICO: DELITO INFORMÁTICO (OU CRIME DIGITAL, OU INFRAÇÃO PENAL CIBERNÉTICA) SEQUER PREVISTO NO ARTIGO II DO TRATADO DE EXTRADIÇÃO BRASIL/EUA – ROL EXAUSTIVO, FUNDADO EM "NUMERUS CLAUSUS", QUE DEFINE, NO CONTEXTO BILATERAL DAS RELAÇÕES EXTRADICIONAIS ENTRE BRASIL E EUA, OS CRIMES QUALIFICADOS PELA NOTA DE "EXTRADITABILIDADE" – PRECEDENTES, A ESSE RESPEITO, DO SUPREMO TRIBUNAL FEDERAL – CONSEQUENTE IMPOSSIBILIDADE DE PROCESSAR-SE DEMANDA EXTRADICIONAL FUNDADA EM DELITO ESTRANHO AO ROL TAXATIVO INSCRITO NO ARTIGO II DESSE

[54] MALAQUIAS, Roberto Antônio Darós. **Crime cibernético e prova:** a investigação criminal em busca da verdade. Curitiba: Juruá, 2012. p. 61.

[55] BRASIL. Supremo Tribunal Federal (2. Turma). **Questão de Ordem na Prisão Preventiva para Extradição 732**. Extradição. Prisão Cautelar. Pleito formulado pela Interpol. Possibilidade. Inovação introduzida pela lei nº 12.878/2013. Delito Informático (crime digital): "Invasão de dispositivo informático". Relator: Min. Celso de Mello, 11 de novembro de 2014. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=7645112. Acesso em: 19 set. 2021.

> TRATADO DE EXTRADIÇÃO – NATUREZA JURÍDICA DO TRATADO DE EXTRADIÇÃO (“LEX SPECIALIS”) – PRECEDÊNCIA JURÍDICA , QUANTO À SUA APLICABILIDADE, SOBRE O ORDENAMENTO POSITIVO INTERNO DO BRASIL – “PACTA SUNT SERVANDA ” – PRECEDENTES – A INADMISSIBILIDADE DA EXTRADIÇÃO (CAUSA PRINCIPAL) TORNA INVIÁVEL O ATENDIMENTO DO PEDIDO DE PRISÃO PREVENTIVA (MEDIDA REVESTIDA DE CAUTELARIDADE E IMPREGNADA DE CARÁTER ANCILAR E MERAMENTE ACESSÓRIO) – QUESTÃO DE ORDEM QUE SE RESOLVE NO SENTIDO DO INDEFERIMENTO DO PEDIDO DE PRISÃO CAUTELAR. (Grifou-se)

Assim sendo, a Lei nº 12.737/2012 veio para atender à demanda urgente que se tinha no ordenamento jurídico brasileiro em relação à edição de legislação voltada especificamente aos crimes ligados à internet.

A tipificação do delito de invasão de dispositivo cibernético é mais uma forma de garantir 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.

A lei, porém, recebeu diversas críticas de especialistas em crimes de internet, peritos, juristas e profissionais de segurança da informação, que a julgaram insuficiente e sujeita a interpretações divergentes, dada a sua redação confusa, com penas excessivamente brandas.

Diante disso, recentemente o dispositivo foi modificado, como se abordará posteriormente ao se tratar da Lei nº 14.155/21. Não obstante, a inovação jurídica trazida pelo art. 154-A do Código Penal se coadunou com as necessidades da época, que exigia a criminalização de conduta tida como injusta, como pôde ser observada na grande repercussão do episódio da atriz brasileira.

Apesar de longe resolver o problema da carência de normas cibernéticas, mesmo com suas falhas e limitações, a Lei nº 12.737 foi um grande marco para o início da proteção de vítimas de crimes virtuais.

5.3 Lei nº 12.965/2014 - Marco Civil da Internet

Com o objetivo de estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil, foi aprovada a Lei nº 12.965, de 23 de abril de 2014,

conhecida como Marco Civil da Internet, que trouxe conceitos e procedimentos, propondo-se a acabar com a ausência de disciplina legal no ciberespaço[56].

O texto da Lei nº 12.965 conta com 32 artigos, elencados em cinco capítulos, quais sejam: 1) disposições preliminares; 2) dos direitos e garantias dos usuários; 3) da provisão de conexão e aplicações da Internet; 4) da atuação do poder público; e 5) disposições finais.

O Marco Civil da Internet não traz sanções de cunho criminal, mas sim apresenta como propósito minimizar as práticas criminosas mediante a regulação da internet com base em três princípios essenciais: a liberdade de expressão, a privacidade e a neutralidade da rede, os quais servem como parâmetros na atribuição da responsabilização civil aos usuários e aos provedores de acesso.

A legislação se mostrou de extrema importância ao reconhecer as relações jurídico-virtuais que, até aquele momento, não dispunham de regulamentação civil, o que produzia demasiada insegurança jurídica, gerando decisões judiciais contraditórias[57].

Com efeito, impende frisar que o Marco Civil, a despeito de visar primordialmente à tutela dos direitos civis na internet, tem também aplicação no Direito Penal e Processual Penal, tendo em vista que disciplina as formas de apuração da materialidade e autoria dos delitos cibernéticos[58].

A Lei nº 12.965 traz, portanto, disposições que interessam à investigação criminal, procedimento que encontra diversas dificuldades no âmbito dos crimes virtuais, já que a determinação da localização do infrator depende de uma série de complexidades técnicas que exigem cooperação e compartilhamento de informações dos provedores de serviços da internet.

Até então, inexistia norma que obrigasse os provedores de Internet ou de serviços a registrarem os registros das atividades de seus usuários. Na maioria das vezes, para que se apure a autoria do delito, faz-se indispensável a cooperação de

---

[56] BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de investigação cibernética à luz do Marco Civil da Internet**. Rio de Janeiro: Brasport, 2016. p. 25.

[57] LEMOS, Ronaldo. O Marco Civil Como Símbolo do Desejo por Inovação no Brasil. In: LEITE, George Salomão; LEMOS, Ronaldo. **Marco Civil da Internet.** Parte 1. São Paulo: Atlas, 2014, p. 3-11.

[58] BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de investigação cibernética à luz do Marco Civil da Internet**. Rio de Janeiro: Brasport, 2016. p. 26.

terceiros, que geralmente administram e oferecem os serviços, aplicações ou hosts utilizados para a prática dos delitos ou que serviram de ambiente para o crime digital[59].

A título exemplificativo, no Brasil, os episódios de suspensão judicial do aplicativo de mensagens “WhatsApp”, provocados pela falta da observância legal da empresa em fornecer os dados das conversas de criminosos, poderiam ter sido evitados com a devida cooperação internacional, evitando assim os transtornos decorrentes do impedimento do uso do aplicativo em todo território nacional.

Em breve síntese, pode-se afirmar que o Marco Civil da Internet é uma espécie de Constituição da internet, que procurou estabelecer, de diversas formas, os direitos e deveres dos usuários das redes informáticas, dos provedores de acesso e de conteúdo, bem como do próprio Estado, garantindo a capacidade de guarda de prova da materialidade e autoria para a penalização do infrator.

Por fim, vale fazer menção à Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18 - LGPD), que, em complemento ao Marco Civil da internet, criou diretrizes mais específicas sobre o tratamento de dados e privacidade dos cidadãos, inclusive aqueles provenientes do mundo digital.

5.4 Lei nº 13.964/2019 - Pacote Anticrime

A Lei 13.964/19, conhecida como Pacote Anticrime, trouxe importantes alterações no Código Penal, no Código de Processo Penal e em legislações esparsas, com o objetivo de elevar a eficácia no combate ao crime. Publicada no dia 24 de dezembro de 2019, a Lei 13.964/19 entrou em vigor no dia 23/01/2020.

À época da promulgação da Lei, 24 dispositivos foram vetados pela Presidência da República. No entanto, mais de um ano depois, em sessão realizada em 19/04/2021, o Congresso Nacional derrubou 16 dos 24 vetos presidenciais, sendo a norma republicada no Diário Oficial da União em 30/04/2021.

No que se refere aos crimes praticados pela internet, a Lei 13.964/2019, após a derrubada do veto, introduziu novo parágrafo ao art. 141 do Código Penal, que prevê disposições aplicáveis aos crimes contra a honra, nos seguintes termos:

---

[59] JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016. p. 184. E-book.

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

Considerando o cenário do meio cibernético, o legislador preocupou-se em agravar a pena daquele que comete crime contra a honra por intermédio das redes sociais e da rede mundial de computadores.

O parágrafo havia sido vetado pela Presidência da República sob a justificativa de violar o princípio da proporcionalidade entre o tipo penal descrito e a pena cominada, uma vez que o artigo 141, inciso III, já tutelava o agravamento da pena na hipótese de qualquer dos crimes contra a honra ser cometido por meio que facilite a sua divulgação ou na presença de várias pessoas. Além disso, foi alegado que o aumento da sanção provocaria superlotação das delegacias e, por consequência, redução do tempo e da força de trabalho para se dedicar ao combate de crimes graves, tais como homicídio e latrocínio[60].

Todavia, o veto acabou sendo derrubado pelo Congresso Nacional. Na concepção de Guilherme de Souza Nucci[61], a decisão foi correta, tendo em vista que o artigo 141, inciso III, à época de sua previsão, não contabilizou a rede mundial de computadores como um meio de divulgação; levava em conta situações menos gravosas na presença de várias pessoas, a exemplo de reunião de condomínio. Nesse sentido, aponta que a previsão de aplicação do triplo da pena é proporcional à potencialidade lesiva do crime cometido pelas redes sociais, dada a disseminação extremamente ampla e rápida da ofensa na internet. No mais, relata que nenhuma estatística criminal conhecida faz um paralelo entre crimes contra a honra e delitos graves, como homicídio ou latrocínio, de forma que a investigação de uns não interfere em nada na apuração de outros.

Com o acréscimo dessa causa de aumento de pena, a inferência lógica que se pode fazer é que o legislador visou a combater as *fake news*, ou notícias falsas, as quais consistem na distribuição deliberada de desinformação ou boatos, com o intuito

---

[60] BRASIL. **Mensagem nº 726, de 24 de dezembro de 2019.** Mensagem de veto. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/Msg/VEP/VEP-726.htm. Acesso em: 23 set. 2022.

[61] NUCCI, Guilherme de Souza. **Desembargador Nucci avalia pontos da lei anticrime que voltam a valer.** Disponível em: https://www.migalhas.com.br/quentes/344322/desembargador-nucci-avalia-pontos-da-lei-anticrime-que-voltam-a-valer. Acesso em: 23 set. 2022.

de prejudicar outrem ou obter vantagem, prática muito presente nos meios eletrônicos, sobretudo no jogo político.

Nessa perspectiva, a alteração legislativa busca promover reprimenda maior aos crimes de calúnia, difamação e injuria quando praticados pela internet, que, considerando o atual contexto, podem tomar proporções desmedidas, acarretando consequências para além da reputação do ofendido.

5.5 Lei nº 14.155/2021

No dia 27 de maio de 2021, após um intervalo de nove anos, a Lei nº 14.155/2021 foi sancionada para realizar alterações na Lei nº 12.737/12 (Lei Carolina Dieckman), que disciplina o crime de invasão de dispositivo informático, previsto no art. 154-A do CP, de modo a modificar a sua redação e tornar mais severa a sua pena.

Da mesma forma, a legislação em comento trouxe ao ordenamento jurídico modalidades específicas do crime de furto e estelionato quando praticados por meio eletrônico, além de definir regras de competência para este último.

5.5.1 Da invasão de dispositivo informático

A redação antiga do delito de invasão de dispositivo informático previa o seguinte:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

Com a alteração promovida pela nova Lei nº 14.155/2021, a norma legal passou a vigorar conforme o exposto:

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

Assim, uma das fragilidades observadas no dispositivo antigo é que ele restringiu a tipicidade da conduta aos casos em que há a violação indevida de mecanismos de segurança. Isto é, se o dispositivo informático não possui mecanismo de proteção, não há o preenchimento da elementar do tipo incriminador[62].

Em sentido semelhante, é a crítica tecida por Luiz Regis Prado[63]:

> Essa menção – mecanismo de segurança – é, em princípio, desnecessária. Senão, veja-se. Nem todos os dispositivos informáticos têm mecanismo de segurança. A invasão pode ocorrer com ou sem mecanismo de segurança, visto que este último também tem vulnerabilidades. Assim, conforme o texto legal, pode ocorrer que se invada um dispositivo e se alegue que não dispunha ele de mecanismo de segurança. Haveria lacuna de punibilidade.

Portanto, a previsão "mediante violação indevida de mecanismo de segurança" consistia em grave imprecisão legislativa, por não amparar os usuários cujos sistemas estivessem desprovidos desses mecanismos. Tratava-se de equívoco do legislador insanável pela interpretação, pois não é possível a analogia *in malam partem*. A lógica é a mesma para a hipótese de não ser punível o furto em residência sem alarme ou de um veículo destrancado[64].

Dessa forma, o trecho "mediante violação indevida de mecanismo de segurança" foi retirado e, assim, bens sem proteção de senha agora também encontram respaldo na normal legal.

Além disso, o fragmento "titular do dispositivo" foi alterado para "usuário do dispositivo". Tal mudança teve por objetivo deixar claro que o sujeito passivo do delito não precisa ser necessariamente o proprietário do dispositivo, podendo a invasão ocorrer em dispositivo que esteja sendo utilizado por alguém que não é seu dono, mas que teve a sua privacidade violada[65].

No entanto, as variadas interpretações doutrinárias quanto ao texto legal continuam existindo, de forma que alguns doutrinadores entendem que a norma apresenta duas condutas, quais sejam a de "invadir" e a de "instalar", como refere

---

[62] NUCCI, Guilherme de Souza. **Manual de direito penal**. 16ª ed. Rio de Janeiro: Forense, 2020. p. 983.

[63] PRADO, Luiz Regis. **Tratado de Direito Penal**: parte especial – arts. 121 a 249 do CP. v. 2. 3ª ed. Rio de Janeiro: Forense, 2019. p. 451.

[64] VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos**. Belo Horizonte: Fórum, 2013. p. 95.

[65] CAVALCANTE, Márcio André Lopes. **Lei 14.155/2021**: promove alterações nos crimes de violação de dispositivo informático, furto e estelionato. Disponível em: https://www.dizerodireito.com.br/2021/05/lei-141552021-promove-alteracoes-nos.html. Acesso em: 21 set. 2022.

Guilherme de Souza Nucci[66]. Já para Rogério Greco[67] e Cezar Roberto Bitencourt[68] , o núcleo seria apenas o ato de “invadir”, sendo o “instalar” um ato secundário, originária da conduta de invadir.

Outra modificação substancial se refere ao *quantum* das sanções. A Lei mais recente majorou a pena do crime invasão de dispositivo informático para a reclusão de 1 (um) a 4 (quatro) anos, e multa, substituindo a previsão antiga de detenção, de 3 (três) meses a 1 (um) ano, e multa.

Da mesma forma, para o crime em questão também foi atualizada a majorante prevista no § 2º, que agora prevê o aumento de pena de 1/3 a 2/3, bem como a qualificadora do § 3º, a qual estabelece reclusão, de 2 a 5 anos, e multa, em substituição das redações antigas, que previam, respectivamente, o aumento de pena de 1/6 a 1/3, e reclusão de 6 meses a 2 anos, e multa.

Desse modo, infere-se que o art. 154-A do CP deixou de ser crime de menor potencial ofensivo, não estando mais sujeito à competência do Juizado Especial Criminal (art. 61 da Lei nº 9.099/95).

Como se percebe, o legislador previu maior sancionamento para a prática delitiva, atendendo à crítica majoritária, a qual dizia que o dispositivo cominava penas muito brandas, não estando apto a tutelar à altura da gravidade do delito, sobretudo considerando o incremento recente das técnicas de engenharia social.

5.5.2 Do furto mediante fraude eletrônica

No ano de 2020, em razão da pandemia do coronavírus e do distanciamento social, a internet tornou-se uma ferramenta fundamental para a realização de atividades pessoais e profissionais. Por conta do aumento do número de usuários conectados à rede, os golpes eletrônicos, por consequência, também cresceram expressivamente, o que ensejou uma resposta do Poder Público.

Dessa forma, a Lei nº 14.155/2021 promoveu duas alterações no art. 155, que trata sobre furto: 1) inseriu o § 4º-B, prevendo a qualificadora de furto mediante fraude

---

[66] NUCCI, Guilherme de Souza. **Manual de direito penal**. 16ª ed. Rio de Janeiro: Forense, 2020. p. 983.

[67] GRECO, Rogério. **Código Penal comentado**. 11ª ed. Niterói: Impetus. 2017. p. 384.

[68] BITENCOURT, Cezar Roberto. **Código Penal Comentado**. 8ª ed. São Paulo: Saraiva, 2014. p. 680.

cometido por meio de dispositivo eletrônico ou informático; e 2) acrescentou o § 4º-C, com duas causas de aumento de pena relacionadas com o § 4º-B.

Vale lembrar que até a promulgação da Lei nº 14.155/2021, as subtrações fraudulentas cometidas pela rede mundial de computadores se enquadravam na qualificadora do art. 155, § 4º, inciso II, com pena de dois a oito anos. Todavia, em razão dos prejuízos provocados e da maior dificuldade de apuração revelada nesses casos, o legislador decidiu inserir no art. 155 qualificadora específica para as situações em que o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático[69].

Para melhor visualização, colaciona-se o excerto legal do furto mediante fraude cometido por meio de dispositivo eletrônico ou informático:

> Art. 155. (...)
> § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.

Assim, pode-se dizer que a norma em análise é uma hipótese de qualificadora da qualificadora, na medida em que o art. 155, § 4º, inciso II do Código Penal qualifica o furto com emprego de fraude, prevendo uma pena de 02 (dois) a 08 (oito) anos de reclusão, ao passo que o art. 155, § 4º-B prevê uma pena de 04 (quatro) a 08 (oito) anos de reclusão para os furtos realizados mediante fraude, por meio de dispositivo eletrônico. Aqui, portanto, além do meio, o instrumento empregado ganha relevância para qualificar a conduta[70].

É possível perceber também que, ao final do texto, o legislador buscou se antecipar às mudanças tecnológicas, ao estipular preceito que atrai interpretação analógica do meio fraudulento. Do mesmo modo, denota-se que o dispositivo vem alinhado à nova redação do crime de invasão de dispositivo informático,

---

[69] 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 em: 21 set. 2022.

[70] FIGUEIREDO, Rudá. **Crimes eletrônicos e Lei 14.155/2021**. Disponível em: https://www.direitoempalavrassimples.com.br/crimes-eletronicos-e-lei-14-155-2021. Acesso em: 21 set. 2022.

consubstanciado no art. 154-A do Código Penal, que, de forma mais técnica, eliminou a exigência da "violação indevida de mecanismo de segurança".

A respeito dos casos de aumento de pena do furto mediante fraude cometido por meio de dispositivo eletrônico, a inovação legislativa traz duas hipóteses:

> Art. 155 (...)
> § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
> I – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional;
> II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável.

No primeiro inciso, a pena é aumentada em razão do fato representar, de algum modo, ameaça à soberania nacional. Além disso, essa circunstância acarreta maior dificuldade na identificação e eventual responsabilização penal dos envolvidos, justificando maior reprimenda.

Já no segundo inciso, o incremento da sanção se dá por conta das características das vítimas, idosa ou vulnerável, que demandam maior proteção estatal.

Ponto controverso da norma diz respeito ao trecho que considera a relevância do resultado gravoso como parâmetro para a aplicação da dosimetria da pena. Trata-se de fórmula inédita no Código Penal, a qual, todavia, não foi bem recebida pela doutrina majoritária. Sobre o tópico, leciona Rogério Sanches Cunha[71]:

> Essa não nos parece a melhor forma de aplicar a causa de aumento de pena. Ora, se a majorante se refere ao crime cometido fora do território nacional e ao crime cometido contra idoso ou vulnerável, são as características intrínsecas do idoso, do vulnerável e da transnacionalidade do meio de execução que justificam primariamente o aumento. Se essas são as circunstâncias do crime, impõe-se o aumento, cuja variação, sim, deve se basear na maior gravidade do caso concreto. Utilizar a gravidade como fundamento da majorante, e não como algo derivado das circunstâncias mencionadas nos incisos I e II, subverte a lógica da aplicação da pena. Se o fundamento para a majoração fosse a extensão do prejuízo, o texto legal deveria consistir em algo como "Aumenta-se a pena de 1/3 a 2/3 conforme a relevância do resultado".

[71] 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 em: 21 set. 2022.

Ademais, para que o autor responda pelas causas de aumento de pena, é indispensável que exista dolo, ou seja, é necessário que o agente saiba que, no caso concreto, está sendo utilizado um servidor mantido no exterior ou que a vítima seja idosa ou vulnerável – o que, dada a natureza do crime cibernético, muitas vezes não acontece.

5.5.3 Do estelionato mediante fraude eletrônica

A Lei nº 14.155/2021 também realizou três alterações no art. 171, que trata sobre estelionato: 1) inseriu o § 2º-A, prevendo a qualificadora do estelionato mediante fraude eletrônica; 2) acrescentou o § 2º-B, com uma causa de aumento de pena relacionada com o § 2º-A; e 3) modificou a redação da causa de aumento de pena do § 4º.

Nesse sentido, foi introduzido no crime de estelionato uma qualificadora semelhante à inserida no furto:

> Art. 171 (...)
> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.

Como se vê, a lei não faz referência expressa a dispositivo eletrônico ou informático. Contudo, não é difícil perceber que a fraude praticada por meio de redes sociais, telefone, e-mail ou outro meio análogo exige justamente o manuseio de tais dispositivos.

Nesses casos, ao contrário do que acontece no furto, a vítima, ao fornecer informações que possibilitam a prática do crime, integra diretamente o ardil preparado pelo estelionatário para obter a vantagem indevida. Assim, a principal distinção é que no estelionato virtual ocorre a entrega voluntária da coisa pela vítima, em decorrência da fraude empregada pelo agente, ao passo que no furto mediante fraude eletrônica ocorre a subtração da coisa, servindo a fraude como meio de iludir a vigilância ou a atenção da vítima[72].

---

[72] ANDREUCCI, Ricardo Antonio**. Furto mediante fraude por meio de dispositivo eletrônico ou informático.** Disponível em: https://emporiododireito.com.br/leitura/furto-mediante-fraude-por-meio-de-dispositivo-eletronico-ou-informatico. Acesso em: 21 set. 2022.

Houve ainda duas alterações relativas às causas de aumento de pena para o estelionato:

> Art. 171 (...)
> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.
> § 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso.

Ambas as majorantes em questão seguem o mesmo caminho da majorante prevista no furto mediante fraude eletrônica, no sentido de preceituar pena mais gravosa ao crime praticado mediante servidor mantido fora do território nacional bem como praticado contra idoso e vulnerável. Também está presente a "relevância do resultado gravoso" como elemento normativo do tipo, o qual terá seu conteúdo definido por via de interpretação judicial e que, como já citado, não agradou os operadores do direito.

Impende salientar que houve inovação legislativa em benefício do réu na qualificadora do estelionato praticado contra idoso ou vulnerável, na medida em que antes o patamar de aumento da pena deveria ser necessariamente dobrado, enquanto agora ele pode ser aumentado de 1/3 até o dobro.

Por derradeiro, a Lei nº 14.155/2021 tratou da competência do crime de estelionato, acrescentando o § 4º no art. 70 do CP:

> Art. 70. (...)
> § 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção.

Com esta norma, o legislador visa a robustecer a tutela das vítimas dos estelionatos plurilocais, estabelecendo o foro do domicílio da vítima para o exercício da ação penal, independentemente do local da consumação do delito ou, em caso de tentativa, do lugar onde foi praticado o último ato de execução.

Dessa forma, a mudança legislativa tem o condão de aproximar a vítima da autoridade policial responsável pela investigação, favorecendo a obtenção de provas

do delito e garantindo, em última análise, o acesso do jurisdicionado à justiça. Do mesmo modo, resolve a insegurança jurídica do tema que possuía intensa oscilação jurisprudencial[73].

Apesar de não ser ideal, a Lei nº 12.737/2012 representa um avanço no combate às fraudes virtuais, por meio da implementação de penas mais rigorosas e descrição típica própria das condutas, o que possibilita certa melhora na persecução penal desses delitos que, diante do cenário atual da tecnologia, são cada vez mais presentes na sociedade.

5.6 Demais condutas praticadas por meio da internet

Gradativamente, foram introduzidos no Código Penal Brasileiro e em leis esparsas dispositivos que incriminam outras condutas praticadas por meio da internet. Alguns delitos merecem destaque especial, dado o seu grande número de incidência ou relevância jurídica.

O Estatuto da Criança e do Adolescente (ECA) tipifica a partir de seu art. 240 os delitos relacionados à pornografia infantojuvenil, sejam eles cometidos pela internet ou não. Com efeito, no ano de 2008, a Lei nº 11.829/2008 foi sancionada com o intuito de "aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet[74].

O legislador teve cuidado especial na redação dos tipos penais, acrescentando e alterando dispositivos para aumentar a abrangência da legislação, como pode ser observado na previsão das condutas consideradas criminosas, as quais podem ser realizadas em qualquer meio para incidência da norma. Logicamente, então, abarcou-se o meio de sistema de informática ou telemático.

Com efeito, a maioria das condutas criminosas que envolvem pornografia infantojuvenil, passíveis de serem realizadas pela internet, estão devidamente tipificadas no ECA nos seus respectivos artigos, quais sejam: produção (art. 240),

---

[73] CAVALCANTE, Márcio André Lopes. **Lei 14.155/2021**: promove alterações nos crimes de violação de dispositivo informático, furto e estelionato. Disponível em: https://www.dizerodireito.com.br/2021/05/lei-141552021-promove-alteracoes-nos.html. Acesso em: 21 set. 2022.

[74] SILVA, Ângelo Roberto Ilha da, *et al*. **Crimes Cibernéticos**. 2ª ed. Porto Alegre: Livraria do Advogado, 2018. p. 92.

comercialização (art. 241), compartilhamento (art. 241-A), armazenamento (art. 241-B), simulação de participação (art. 241-C) e aliciamento ou constrangimento (art. 241-D)[75].

Ainda sobre os crimes contra a dignidade sexual, importante fazer menção à Lei nº 13.718/2018, a qual, por intermédio do art. 218-C do Código Penal, tipificou a divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia - prática comumente realizada pelo meio informático. Assim, dentre as suas disposições, a norma visou ao combate da chamada pornografia de vingança (*revenge porn*), que são as situações em que uma das partes de uma relação afetiva, após o fim do relacionamento, decide expor a intimidade do casal ou da outra parte por meio da publicação do material obtido em confiança[76].

Acerca do ato de *bullying*, a Lei nº 13.185/2015 institui o Programa de Combate à Intimidação Sistemática. Assim, quando houver a intimidação sistemática por intermédio da rede mundial de computadores, a prática será caracterizada como *cyberbullying*, nos termos do art. 2º, parágrafo único, da legislação em comento. Contudo, embora seja repreendida, a conduta não é considerada crime, inexistindo assim qualquer previsão de figura criminosa.

A conduta de perseguição (*stalking*), de outra via, tem previsão legal no art. 147-A do Código Penal. Nesse aspecto, a Lei nº 14.132, de 31 de março de 2021, com sua redação abrangente, tipificou também a modalidade de perseguição pelos meios cibernéticos (*cyberstalking*), consistente na utilização de redes sociais, mensagens de texto e e-mails para importunar a vítima.

No mais, cumpre lembrar que a informática trouxe em seu bojo novas formas de realizar velhos crimes. Grande parte dos delitos tradicionais, como a exemplo do crime de ameaça e delitos resultantes de preconceito de raça ou cor, já são protegidos pelo Direito Penal, ainda que estes encontrem novo *modus operandi* em decorrência da evolução tecnológica.

---

[75] BRITO, Auriney. **Direito Penal Informático**. São Paulo: Saraiva, 2013. l. 2351. E-book.

[76] SYDOW, Spencer Toth; DE CASTRO, Ana Lara Camargo. **Exposição pornográfica não consentida na internet**: da pornografia de vingança ao lucro. Belo Horizonte: D'Plácido, 2017. p. 9.

6. CONSIDERAÇÕES FINAIS

Como observado, é evidente que o progresso da humanidade por meio da evolução tecnológica e científica ocasiona mudanças significativas na estrutura social. Em especial, o advento da internet revolucionou os meios de comunicação, das relações interpessoais e negociais, da política, da economia e de outros incontáveis setores.

Contudo, as facilidades e conveniências proporcionadas pelo desenvolvimento da informática vieram acompanhadas do surgimento de um novo gênero de criminalidade, que encontrou no espaço cibernético novo local para a execução de crimes já existentes, assim como um ambiente capaz de originar condutas ilícitas ainda não concebidas pelo Direito.

Nesse sentido, o ordenamento jurídico brasileiro teve que se adaptar à nova realidade moderna para combater efetivamente a criminalidade cibernética, por meio da tipificação específica de condutas praticadas contra o sistema informatizado, assim como pela adequação legal dos crimes tradicionais quando realizados no ambiente virtual.

Ocorre que o Brasil demorou demasiadamente para iniciar as mudanças legislativas para o enfrentamento do tema. A lacuna legislativa perdurou por mais de décadas, resultando em insegurança jurídica e na impossibilidade de punição de certas condutas.

Felizmente, o cenário vem se modificando, como pode se perceber na recente movimentação do Brasil para adesão à Convenção de Budapeste, principal documento jurídico internacional no combate aos crimes virtuais. A efetiva comunicação judicial e policial em caráter global, aliado à uniformização mínima das leis, facilitam o processo de persecução penal desses delitos.

Do mesmo modo, a edição e adaptação das legislações nacionais para abordar a criminalidade cibernética ganhou força nos últimos anos, de modo que condutas realizadas no espaço virtual passaram a receber tipificação própria, com reprimendas mais rigorosas.

Para o combate eficaz da criminalidade cibernética, o Direito precisa se adaptar juntamente com as mudanças provocadas pela internet. Legislações atualizadas com demandas pertinentes ao ciberespaço, capacitação de agentes públicos, cooperação

internacional e processos céleres que se amoldem à dinâmica dos cibercrimes são fatores imprescindíveis para a tutela eficaz.

A concretização desses elementos está sendo observada pelo ordenamento jurídico pátrio, ainda que de forma incipiente. Todavia, a velocidade com a qual a internet se desenvolve é inúmeras vezes superior às retificações legislativas. Assim, há muito a ser regulado e alterado para proporcionar uma melhora na aplicação e eficácia da lei penal, em consonância com os interesses da sociedade digital.

REFERÊNCIAS

ALMEIDA, Jessica de Jesus, *et al*. **Crimes cibernéticos.** Caderno de Graduação - Ciências Humanas e Sociais - UNIT - SERGIPE, *[S. l.]*, v. 2, n. 3, 2015. Disponível em: https://periodicos.set.edu.br/cadernohumanas/article/view/2013. Acesso em: 1 set. 2022.

ANDREUCCI, Ricardo Antonio**. Furto mediante fraude por meio de dispositivo eletrônico ou informático.** Disponível em: https://emporiododireito.com.br/leitura/furto-mediante-fraude-por-meio-de-dispositivo-eletronico-ou-informatico. Acesso em: 21 set. 2022.

BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de investigação cibernética à luz do Marco Civil da Internet**. Rio de Janeiro: Brasport, 2016.

BITENCOURT, Cezar Roberto. **Código Penal Comentado**. 8ª ed. São Paulo: Saraiva, 2014.

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.

BRANDÃO, Cláudio. **Curso de direito penal:** parte geral. Rio de Janeiro: Forense, 2010.

BRASIL. **Decreto Legislativo nº 37, de 2021**. Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Brasília: Diário Oficial da União, 17/12/2021. p. 7, col. 2. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/150258. Acesso em: 15 set. 2022.

BRASIL. **Mensagem nº 726, de 24 de dezembro de 2019.** Mensagem de veto. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/Msg/VEP/VEP-726.htm. Acesso em: 23 set. 2022.

BRASIL. Ministério Público Federal. **Crimes cibernéticos**: roteiro de atuação. 2ª. ed. rev. Brasília: MPF/2ª CCR, 2013.

BRASIL. Ministério Público Federal. Procuradoria-Geral da República. **Ofício nº 736/2020**, **de 30 de julho de 2020**. Convenção sobre o Crime Cibernético. Brasília: Ministério Público Federal, 2020. Disponível em: http://www.mpf.mp.br/pgr/documentos/Oficio736DaviAlcolumbre.pdf. Acesso em: 15 set. 2022.

BRASIL. **Projeto de Decreto Legislativo nº 255, de 2021.** Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Brasília: Congresso Nacional, 2021. Disponível em: https://www.camara.leg.br/propostas-legislativas/2287513. Acesso em: 15 set. 2022.

BRASIL. Supremo Tribunal Federal (2. Turma). **Questão de Ordem na Prisão Preventiva para Extradição 732**. Extradição. Prisão Cautelar. Pleito formulado pela Interpol. Possibilidade. Inovação introduzida pela lei nº 12.878/2013. Delito Informático (crime digital): "Invasão de dispositivo informático". Relator: Min. Celso de Mello, 11 de novembro de 2014. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=7645112. Acesso em: 19 set. 2021.

BRITO, Auriney. **Direito Penal Informático**. São Paulo: Saraiva, 2013.

CARVALHO, M. S. R. M. **A trajetória da Internet no Brasil**: do surgimento das redes de computadores à instituição dos mecanismos de governança. Tese (Mestrado) – Engenharia de Sistemas e Computação, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais**. Rio de Janeiro: Brasport, 2014.

CASTELLS, Manuel. **A era da informação**: economia, sociedade e cultura. In: A Sociedade em rede. 5 ed. São Paulo: Paz e Terra, 1999. v. 1.

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

CAVALCANTE, Márcio André Lopes. **Lei 14.155/2021**: promove alterações nos crimes de violação de dispositivo informático, furto e estelionato. Disponível em: https://www.dizerodireito.com.br/2021/05/lei-141552021-promove-alteracoes-nos.html. Acesso em: 21 set. 2022.

CIDRÃO, Tais Vasconcelos*, et al*. **A Oportunidade e Necessária Aplicação do Direito Internacional nos Ciberespaços**: Da Convenção de Budapeste à Legislação brasileira. Brazilian Journal of International Relations, Marília, v. 7, ed. 1, p. 66-82, jan./abr. 2018.

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 em: 21 set. 2022.

CONSELHO DA EUROPA. **Convenção sobre o Cibercrime**. Budapeste, 23.XI.2001. Disponível em: https://rm.coe.int/16802fa428. Acesso em: 16 set. 2022.

COUNCIL OF EUROPE. **Convention on Cybercrime**, Chart of signatures and ratifications of Treaty 185. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185. Acesso em: 15 set. 2022.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.

FIGUEIREDO, Rudá. **Crimes eletrônicos e Lei 14.155/2021**. Disponível em: https://www.direitoempalavrassimples.com.br/crimes-eletronicos-e-lei-14-155-2021. Acesso em: 21 set. 2022.

GRECO, Rogério. **Código Penal comentado**. 11ª ed. Niterói: Impetus. 2017.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016. E-book.

KIST, Dario José. **Prova digital no processo penal**. Leme: JH Mizuno, 2019.

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

MARRA, Fabiane Barbosa. **Desafios do direito na era da internet**: uma breve análise sobre os crimes cibernéticos. São Paulo: Journal of Law and Sustainable Development: v. 7, n. 2, 2019.

NUCCI, Guilherme de Souza. **Curso de direito penal**: parte geral: arts. 1º a 120 do Código Penal. Rio de Janeiro: Forense, 2017.

NUCCI, Guilherme de Souza. **Desembargador Nucci avalia pontos da lei anticrime que voltam a valer.** Disponível em: https://www.migalhas.com.br/quentes/344322/desembargador-nucci-avalia-pontos-da-lei-anticrime-que-voltam-a-valer. Acesso em: 23 set. 2022.

NUCCI, Guilherme de Souza. **Manual de direito penal**. 16ª ed. Rio de Janeiro: Forense, 2020. p. 983.

PINHEIRO, Patricia Peck. **Direito digital**. 7ª ed. Saraiva, 2021.

PRADO, Luiz Regis. **Tratado de Direito Penal**: parte especial – arts. 121 a 249 do CP. v. 2. 3ª ed. Rio de Janeiro: Forense, 2019.

REALE JÚNIOR, Miguel. **Instituições de direito penal.** Rio de Janeiro: Forense, 2009.

SILVA, Ângelo Roberto Ilha da, *et al*. **Crimes Cibernéticos**. 2ª ed. Porto Alegre: Livraria do Advogado, 2018.

SILVA, Patrícia Santos da; SILVA, Matheus Passos. **Direito e crime cibernético**: análise da competência em razão do lugar no julgamento de ações penais. Brasília: Vestnik, 2015.

SYDOW, Spencer Toth. **Curso de direito penal informático**: partes geral e especial. 3ª ed. Salvador: Jvspodium, 2022.

SYDOW, Spencer Toth; DE CASTRO, Ana Lara Camargo. **Exposição pornográfica não consentida na internet**: da pornografia de vingança ao lucro. Belo Horizonte: D'Plácido, 2017.

VALIN, Celso. **A questão da jurisdição e da territorialidade nos crimes praticados pela Internet.** Direito, sociedade e informática: limites e perspectivas da vida digital. Florianópolis: Fundação Boiteux, 2000.

VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos**. Belo Horizonte: Fórum, 2013. p. 95.

VIEIRA, Eduardo. **Os bastidores da Internet no Brasil**. São Paulo: Manole, 2003.

WENDT, Emerson. JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos**: ameaças e procedimentos de investigação. 2ª ed. Rio de Janeiro: Brasport, 2013.