FERNANDA LETÍCIA DE PAULA ABREU

CIBERCRIMINALIDADE NO BRASIL:

breve abordagem da legislação brasileira relacionada aos crimes cibernéticos

LAVRAS - MG
2023

FERNANDA LETÍCIA DE PAULA ABREU

CIBERCRIMINALIDADE NO BRASIL:

breve abordagem da legislação brasileira relacionada aos crimes cibernéticos

Monografia apresentada à Universidade Federal de Lavras, como parte das exigências do Curso de Direito, para a obtenção do título de Bacharela.

Prof. Dr. Ricardo Augusto de Araújo Teixeira

Orientador

LAVRAS - MG

2023

FERNANDA LETÍCIA DE PAULA ABREU

CIBERCRIMINALIDADE NO BRASIL:

breve abordagem da legislação brasileira relacionada aos crimes cibernéticos

CYBERCRIME IN BRAZIL:

a brief overview of Brazilian legislation related to cyber crimes

Monografia apresentada à Universidade Federal de Lavras, como parte das exigências do Curso de Direito, para a obtenção do título de Bacharela.

APROVADA em 27 de fevereiro de 2023

Dr. Ricardo Augusto de Araujo Teixeira UFLA

Dra. Ana Carolina Silva Severino PCMG

Prof. Dr. Ricardo Augusto de Araujo Teixeira

Orientador

LAVRAS - MG

2023

AGRADECIMENTOS

Aos meus pais, Maria e Luciano, e ao meu irmão Paulo por serem meus maiores exemplos e por sempre fazerem de tudo para que eu possa alcançar meus objetivos.

Aos meus familiares, principalmente minhas tias Maria da Glória e Maria José e meu padrinho José Félix por todo o suporte sem o qual eu não chegaria tão longe.

À minha dupla canina por serem fontes de amor incondicional e por deixarem minha vida mais leve.

Aos amigos de Lavras por terem se tornado a minha família no sul de Minas, por enfrentarem comigo os dias de luta e comemorarem ao meu lado os dias de glória.

Ao meu namorado por acreditar tanto em mim e por ser minha melhor companhia.

Aos meus professores por todos os conhecimentos transmitidos e os conselhos dados.

Aos grupos de estudos que participei, à Jurídica Júnior e aos locais onde tive o privilégio de estagiar, especialmente ao Juizado Especial da Comarca de Lavras, por serem peças fundamentais para o meu crescimento pessoal e profissional.

Ao professor e orientador Ricardo, por me fazer amar o Direito Penal e por ter me auxiliado no desenvolvimento deste trabalho.

RESUMO

A presente monografia tem como objetivo realizar uma abordagem da legislação brasileira relacionada aos crimes cibernéticos. Inicialmente, é apresentada a origem da internet e sua popularização no Brasil, seguida pela exploração da problemática dos crimes cibernéticos e seu crescimento durante a pandemia de COVID-19. Em seguida, são discutidos os conceitos de crime, bem como dos crimes cibernéticos e suas classificações. A legislação nacional é analisada em sequência. A pesquisa foi realizada pela vertente jurídico-social, por meio de um procedimento jurídico-interpretativo ou jurídico-compreensivo e do método de pesquisa dedutivo. Para embasamento deste trabalho, recorreu-se à revisão bibliográfica, análise de dados quantitativos e estudo das disposições das leis selecionadas. Concluiu-se que a legislação brasileira sobre crimes cibernéticos é incipiente e apresenta lacunas, e que a repressão efetiva à cibercriminalidade depende de medidas adicionais além da elaboração de leis.

Palavras-chave: Direito Penal. Crimes Cibernéticos. Legislação.

ABSTRACT

The present thesis aims to approach the Brazilian legislation related to cyber crimes. Initially, the origin of the internet and its popularization in Brazil is presented, followed by the exploration of the problem of cyber crimes and its growth during the COVID-19 pandemic. Then, the concepts of crime, as well as cyber crimes and their classifications, are discussed. National legislation is then analyzed. The research was carried out from the legal-social aspect, through a legal-interpretive or legal-comprehensive procedure and the deductive research method. To support this work, a literature review, quantitative data analysis and study of the provisions of selected laws were carried out. It was concluded that the Brazilian legislation on cyber crimes is incipient and presents gaps, and that effective repression of cybercrime depends on additional measures beyond the elaboration of laws.

Keywords: Criminal Law. Cybercrimes. Legislation.

LISTA DE ABREVIATURAS

art.	Artigo
arts.	Artigos
p.	Página
n.	Número
n.p	Não paginado

LISTA DE SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
ARPANET	*Advanced Research Projects Agency Network*
BITNET	*Because It's Time Network*
CERT.BR	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CNN	*Cable News Network*
CP	Código Penal
CPP	Código de Processo Penal
ECA	Estatuto da Criança e do Adolescente
EMBRAPA	Empresa Brasileira de Pesquisa Agropecuária
EMBRATEL	Empresa Brasileira de Telecomunicações
ENIAC	*Electronic Numerical Integrator And Computer*
FDR	Finanças, Direito e Renda
FGV	Fundação Getulio Vargas
GDPR	*General Data Protection Regulation*
IBGE	Instituto Brasileiro de Geografia e Estatística
IP	*Internet Protocol*
LGPD	Lei Geral de Proteção de Dados Pessoais
MCI	Marco Civil da Internet
MILNET	*Military Network*
NSA	*National Security Agency*
NSFNET	*National Science Foundation Network*
OMS	Organização Mundial da Saúde
PNAD	Pesquisa Nacional por Amostra de Domicílios
UNICAMP	Universidade Estadual de Campinas
WIFI	*Wireless Fidelity*
WWW	*World Wide Web*
5G	Quinta Geração

SUMÁRIO

1. INTRODUÇÃO

Émile Durkheim, psicólogo, filósofo e sociólogo francês do século XIX, em sua obra "As regras do método sociológico" contribuiu para a sociologia criminal ao estudar o que denominou "Fato Social" que diz respeito à forma de agir dos indivíduos em uma sociedade. Durkheim (2007) teceu a teoria de que o crime por si só é um fato social normal, tornando-se patológico somente quando atinge um grau de ocorrência extremamente elevado dentro da organização social.

O sociólogo afirma que o crime seria uma consequência da própria convivência humana, sendo possível observar sua ocorrência nas mais diversas sociedades. Durkheim (2007) entende o crime como algo útil por conta de sua função reguladora da evolução moral e que a pena não seria um "remédio" para uma patologia e sim um elemento de coesão social, responsável pela promoção de uma consciência coletiva.

Tomando por base a sociologia durkheimiana, Bittencourt (2021) entende que o crime exerce a função de "manter aberto o canal de transformações de que a sociedade precisa" (2021, p. 19) e que "as relações humanas são contaminadas pela violência, necessitando de normas que as regulem" (2021, p. 19), ressaltando a importância da legislação penal para a manutenção da ordem.

Destarte, partindo do pressuposto de que a criminalidade é um fenômeno comum às diversas organizações sociais, podemos afirmar que, na era pós-modernidade em que vivemos, este acontecimento tem ganhado novos delineamentos. A partir das transformações provenientes das revoluções tecnológicas e do surgimento e popularização da Internet, também tem se originado novos crimes e novas formas de cometê-los utilizando-se de dispositivos digitais. Perante isto, a cibercriminalidade é um tema que vale a pena ser sondado pelos estudiosos do Direito.

Assim, o propósito deste trabalho será o de elaborar uma breve análise do arcabouço legislativo brasileiro, de forma a verificar como tem sido tratada a questão dos crimes cibernéticos no país. Este estudo torna-se indispensável diante da atualidade e da relevância do assunto e das lacunas ainda existentes na produção acadêmica voltada à referida problemática.

Em primeiro lugar, a título de contextualização, iremos abordar a origem da Internet, em tempos de Guerra Fria até a sua chegada e popularização no Brasil, por volta dos anos 90. Será frisado como este artifício foi capaz de transformar a sociedade, salientando suas vantagens, sem perder de vista a problemática da cibercriminalidade. Neste ponto, será feito

um breve histórico do desenrolar das ocorrências dos crimes cibernéticos no país e, em seguida, serão apresentados dados atualizados acerca deste fenômeno, com enfoque na pandemia de COVID-19.

Logo após, para fins didáticos, serão apresentadas as principais teorias referentes ao conceito analítico de crime, além de conceitos e classificações específicas dos crimes cibernéticos difundidos pela doutrina.

Por último, finalmente iremos partir para a análise das principais legislações nacionais que versam e/ou impactam diretamente no campo dos delitos virtuais, quais sejam, o Marco Civil da Internet; a Lei Geral de Proteção de Dados; a Lei de Crimes Cibernéticos (Lei Carolina Dieckmann); a Lei Azeredo; a Lei n. 14.155/2021; a Lei n. 11.829/2008; além da Lei n. 13.718/2018 e da Lei n. 13.722/2018. Também será explorado sobre a Convenção de Budapeste, tratado internacional recentemente adotado pelo Brasil.

2. BREVE HISTÓRIA DA INTERNET

2.1 Origem e popularização

Conforme lições de Castells (2003), os primórdios da Internet datam de meados do século XX durante o conflito travado entre Estados Unidos e União Soviética conhecido como Guerra Fria. Em face da iminência de ataques, tornou-se primordial que os países formulassem aparatos tecnológicos capazes de reforçar suas defesas, configurando a chamada corrida armamentista.

Nesse contexto, os Estados Unidos desenvolveram a ARPAnet, utilizada inicialmente para o compartilhamento de informações entre laboratórios de pesquisa. Sobre a ARPAnet, Lins (2013, p. 15) leciona: “Em lugar de um sistema de controle centralizado, a rede operaria como um conjunto de computadores autônomos que se comunicariam entre si”.

Segundo Castells (2003), a ARPAnet foi se expandindo até que, na década de 80, alterou o seu nome para ARPA-Internet, sendo destinada a pesquisas, enquanto que a MILnet, criada pelo Departamento de Defesa dos Estados Unidos, era utilizada para fins militares. O autor menciona que, na década seguinte, a ARPA-Internet e a NSFnet foram descontinuadas, possibilitando o surgimento de operações privadas de Internet.

Como bem pontua Lins (2013), até esse momento, o uso da rede de computadores era restrito, sendo uma ferramenta empregada exclusivamente por organizações do governo e pela

comunidade acadêmica. Mas, o autor ressalta que essa realidade é alterada com o surgimento da *World Wide Web (WWW)* ou *Web*, e do *browser* ou navegador (LINS, 2013, p. 24).

Assim sendo, conclui Lins (2013) que essas tecnologias foram responsáveis por tornar público o acesso à Internet e pelo início de seu uso comercial, favorecendo a popularização destes artifícios na sociedade. Segundo o estudo Digital 2022: *Global Overview Report*, publicado pelo site Datareportal, tem-se hoje cerca de 5 (cinco) bilhões de usuários ativos na Internet no mundo, o que traduz mais de 60% da população mundial[1].

Especialistas em tecnologia enumeraram as 25 (vinte e cinco) maiores e mais revolucionárias invenções humanas dos últimos 25 (vinte e cinco) anos, tendo a Internet liderado a lista. Em segundo lugar aparece o celular, seguido pelo computador, pela fibra óptica e pelo *e-mail*, respectivamente[2]. Na época atual, é um desafio imaginar a sociedade sem essas inovações, considerando todos os benefícios que estas nos proporcionam.

No subtópico a seguir veremos, sucintamente, como a Internet foi implementada no Brasil, além de analisarmos dados que retratam a abundante presença da rede mundial de computadores na vida dos brasileiros.

2.2 Da BITNET ao 5G: breve histórico da Internet no Brasil

Em solos nacionais, Carvalho (2006) discorre que, as primeiras conexões só foram acontecer após membros da comunidade científica reconhecerem o crescimento do uso da Internet no âmbito internacional e demandarem pela importação dessa tecnologia para o país, tratando-se de uma facilitadora de troca de informações entre os pesquisadores. Assim, no final da década de 80, foi implementada a BITNET, uma rede de computadores que interligava diversas universidades e centros de pesquisas de várias partes do globo e que possibilitava essa comunicação rápida e barata dentro do meio acadêmico. A BITNET foi uma rede cooperativa em que era possível o correio eletrônico e o transporte de arquivos entre computadores.

---

[1] ALMENARA, Igor. Mais de 5 bilhões de pessoas tem acesso à internet, aponta pesquisa. **Canal Tech**. 16 abr. 2022, Internet. Disponível em: <https://canaltech.com.br/internet/mais-de-5-bilhoes-de-pessoas-tem-acesso-a-internet-214836/> Acesso em: 02 nov. 2022

[2] BENATTI, Luciana. Internet: a grande invenção dos últimos 25 anos. **Exame**. 9 out. 2008, Tecnologia. Disponível em: <https://exame.com/tecnologia/internet-a-grande-invencao-dos-ultimos-25-anos-m0075764/>. Acesso em: 02 nov. 2022

Ainda segundo Carvalho (2006), o pontapé inicial do uso comercial da Internet no Brasil desenrola-se na década de 90, quando a Embratel instaurou a prestação de serviços por via discada que aproveitava-se de linhas telefônicas para propiciar a conexão com um provedor de serviços de Internet. Esta via logo tornou-se obsoleta, visto que apresentava desvantagens como a instabilidade e a lentidão, além de um alto custo. Na segunda metade da década de 2000, a internet discada foi substituída pela banda larga.

A contar deste momento, o ramo de tecnologia tem se dedicado a criar mecanismos capazes de proporcionar melhor navegabilidade, oferecendo maior rapidez e estabilidade. Exemplo disso é a fibra óptica que pode atingir até 20 (vinte) vezes mais velocidade de conexão do que a via cabo comum[3]. Outros engenhos que revolucionaram a experiência do internauta foram o *Wi-fi* e as redes móveis dos celulares, cuja utilização de fios para se conectar à rede é dispensável.

Recentemente, as redes móveis vivenciam sua quinta geração. O 5G promete, dentre outros benefícios, conectar mais dispositivos, sendo compatível com automóveis e eletrodomésticos, por exemplo; além de elevar a velocidade de conexão e reduzir o tempo de resposta[4]. A conexão 5G passou a funcionar no Brasil em meados do ano de 2022, inicialmente nas cidades de Belo Horizonte, Brasília, João Pessoa, Porto Alegre e São Paulo e tem gerado expectativas na população que aguarda pela expansão da área de cobertura do sinal 5G para que possam aderir à novidade.

Da mesma forma que a Internet tem se aprimorado, o mesmo sucedeu com os equipamentos eletrônicos disponíveis no mercado. A datar da criação do ENIAC, o primeiro computador do mundo, no ano de 1946, a informática vem evoluindo até que, nos anos 10, houve a explosão dos produtos inteligentes, como é o caso dos *smartphones*[5]. De acordo com Barros (2011), o *smartphone* é uma junção entre o computador e o celular, permitindo que o seu operador disponha de serviços como o acesso à Internet, as trocas de mensagens

---

[3] HP Inc. As 10 principais vantagens das conexões de Internet de fibra óptica. **HP**. 25 jan. 2022. Disponível em: <https://www.hp.com/br-pt/shop/tech-takes/principais-vantagens-das-conexoes-de-internet-de-fibra-optica#:~:text=A%20velocidade%20da%20Internet%20de%20fibra%20%C3%B3ptica%20%C3%A9%20cerca%20de,mais%20r%C3%A1pida%20que%20a%20DSL.> Acesso em 09 nov. 2022

[4] SBRISSIA, Helena. 1g, 2g, 3g, 4g e 5g: entenda a evolução da internet móvel. **Tecmundo.** 12 mai. 2021. Disponível em: <https://www.tecmundo.com.br/5g-no-brasil/217230-1g-2g-3g-4g-5g-entenda-evolucao-internet-movel.htm> Acesso em 09 nov. 2022

[5] GARRETT, Filipe. Dia da Informática: veja a evolução dos PCs ao longo das décadas. Relembre as máquinas rústicas dos anos 1970 e os PCs de hoje que você pode até levar no bolso. **TechTudo.** 15 ago. 2019, Informática. Disponível em: <https://www.techtudo.com.br/noticias/2019/08/dia-da-informatica-veja-a-evolucao-dos-pcs-ao-longo-das-decadas.ghtml> Acesso em 10 nov. 2022

instantâneas, o sistema de posicionamento global, o *e-mail*, dentre outras funcionalidades, bastando apenas um toque em sua tela[6].

Em conformidade com o site oficial do Governo Federal, um levantamento de dados realizado pela PNAD Contínua e o pelo IBGE mostra que, no ano 2021, 9 (nove) a cada 10 (dez) domicílios brasileiros participantes da pesquisa dispunham de acesso à Internet, havendo um acréscimo nas proporções de domicílios conectados em relação à última pesquisa, realizada em 2019, quando o número era de 8,4 (oito vírgula quatro) a cada 10 (dez) entrevistados[7]. O mesmo levantamento demonstra que os celulares são os meios mais comuns usados para o acesso.

Outrossim, a 33ª edição da Pesquisa Anual sobre o Mercado Brasileiro de TI e Uso nas Empresas, realizada pela FGV e divulgada em maio de 2022, enuncia que a quantidade de dispositivos digitais em operação no país ultrapassa o marco de 447 (quatrocentos e quarenta e sete) milhões, em outras palavras, já são mais de 2 (dois) aparelhos eletrônicos por habitante no Brasil[8]. Noutro giro, segundo estudo realizado pela NordVPN, empresa provedora de serviços de conexão, observando os hábitos dos brasileiros, foi constatado que, das 168 (cento e sessenta e oito) horas que compõem uma semana, em média, 91 (noventa e uma) dessas horas foram despendidas navegando na Internet, o que implica em 13 (treze) horas *online* por dia, aproximadamente[9].

Tais estatísticas reforçam a noção de que a Internet tem ocupado, paulatinamente, mais espaço no cotidiano do brasileiro, sendo desfrutada para estudos, trabalho, recreação, dentre

---

6 BARROS, Thiago. O que é smartphone e para que serve? **TechTudo.** 28 dez. 2011, Informática. Disponível em: <https://www.techtudo.com.br/noticias/2019/08/dia-da-informatica-veja-a-evolucao-dos-pcs-ao-longo-das-decadas.ghtml> Acesso em 10 nov. 2022

7 BRASIL. Governo Federal. Internet chegou a 90% dos domicílios brasileiros no ano passado. Em relação a 2019, houve aumento de seis pontos percentuais, quando 84% dos domicílios tinham acesso à rede mundial de computadores. [Brasília]: Governo Federal, 19 set. 2022. Disponível em: <https://www.gov.br/pt-br/noticias/educacao-e-pesquisa/2022/09/internet-chegou-a-90-dos-domicilios-brasileiros-no-ano-passado#:~:text=Em%202021%2C%20a%20internet%20j%C3%A1,de%20Domic%C3%ADlios%20(PNAD)%20Cont%C3%ADnua.> Acesso em 15 nov. 2022

8 FGV. Pandemia acelerou processo de transformação digital das empresas no Brasil, revela pesquisa. De acordo com o levantamento, essa antecipação do processo de Transformação Digital foi o equivalente ao esperado para o período de um a quatro anos. **FGV.** 26 mai. 2022. Disponível em: <https://portal.fgv.br/noticias/pandemia-acelerou-processo-transformacao-digital-empresas-brasil-revela-pesquisa?utm_source=portal-fgv&utm_medium=fgvnoticias&utm_campaign=fgvnoticias-2021-05-26> Acesso em 15 nov. 2022

9 RAMOS, Guilherme. Brasileiros passam mais da metade de suas vidas na Internet, estima pesquisa. Companhia de cibersegurança mensurou o tempo médio online dos brasileiros; plataformas de entretenimento e redes sociais ocupam maior tempo no dia a dia digital. **TechTudo**. 06 mai. 2022, Internet. Disponível em: <https://www.techtudo.com.br/noticias/2022/05/brasileiros-passam-mais-da-metade-de-suas-vidas-na-internet-estima-pesquisa.ghtml> Acesso em 25 nov. 2022

outros fins. Os avanços tecnológicos têm fomentado a praticidade e a simplicidade na vida das pessoas. É possível realizar, virtualmente, desde tarefas simples, como comprar algum produto ou pagar um boleto, a tarefas mais complexas como, por exemplo, abrir um *e-commerce* ou fazer um curso de graduação, bastando ter um computador ou um celular com acesso à Internet.

O fato é que as tecnologias foram capazes de encurtar distâncias e permitir uma nova forma de socialização dentro do meio cibernético. Entretanto, por mais que tais mecanismos tecnológicos sejam extremamente vantajosos, é imprescindível reconhecer que também subsistem malefícios. Um desses malefícios é a cibercriminalidade, isto é, a ocorrência de crimes no ciberespaço. Passemos a discorrer sobre os delitos virtuais no tópico a seguir.

3. A PROBLEMÁTICA DOS CRIMES CIBERNÉTICOS

3.1 A origem dos crimes cibernéticos até os dias atuais

É controverso na literatura quando exatamente se deram os primeiros casos de crimes cibernéticos no mundo. Consoante com o site oficial da Câmara dos Deputados, na década de 60 já se falava em uso de computadores para sabotagem e espionagem[10]. Crespo (2011), ao abordar a formação da "Sociedade da Informação", aduz que a década de 70 foi marcada pelos crimes de invasão de computadores, aparecendo a figura dos chamados *"hackers"*[11].

Já a década de 80, de acordo com o autor, caracterizou-se pela disseminação das práticas de pirataria de programas informáticos e de fraude de cartões magnéticos (CRESPO, 2011, p. 14). Por fim, o autor expõe que, a partir da década de 90 manifesta-se a chamada "Sociedade da Informação". Esse período foi caracterizado por uma valorização da informação e pela convergência entre a informática e as telecomunicações, de forma que estas

---

10 BRASIL. Câmara dos Deputados. Conheça a evolução dos crimes cibernéticos. [Brasília]: Câmara dos Deputados. 23 ago. 2008. Disponível em: <https://www.camara.leg.br/noticias/89137-conheca-a-evolucao-dos-crimes-ciberneticos#:~:text=Os%20primeiros%20crimes%20relacionados%20%C3%A0,delitos%20como%20sabotagens%20e%20espionagem> Acesso em 01 dez. 2022

11 *Hacker* é uma palavra oriunda da língua inglesa e, de acordo com o dicionário virtual Pearson-Longer designa "alguém que obtém informações secretamente no sistema de computador de outra pessoa para que possam ver, usar ou alterá-lo." Disponível em: <https://www.ldoceonline.com/dictionary/hacker> Acesso em 10 dez. 2022. De acordo com o Dicionário *Online* de Português, uma definição informal dada à palavra *hacker* é "pessoa com um vasto conhecimento na área informática, excessivamente proficiente em programar ou usar computadores." Disponível em: <https://www.dicio.com.br/hacker/> Acesso em 12 dez. 2022

se tornaram ainda mais cruciais na sociedade (CRESPO, 2011, p. 14). De imediato, Crespo (2011) fez um alerta. Para ele, o proveito das tecnologias de maneira indevida é uma ameaça a nível global, razão pela qual a segurança informática deve ser uma prioridade (CRESPO, 2011, p. 14).

Segundo Jesus e Milagre (2016), os casos iniciais de crimes cibernéticos na nação brasileira datam do final da década de 90, período em que os autores já questionavam o papel da Internet como geradora de novos delitos ou como novo meio de execução de crimes já existentes (JESUS; MILAGRE, 2016, p. 10). Um exemplo emblemático foi noticiado pelo jornal Folha de São Paulo, em 1995. Em abril do referido ano, houve um ataque cibernético[12] em que os criminosos tiveram acesso aos arquivos computacionais da faculdade Unicamp e da Embrapa e os destruíram[13]. Tem-se que, desde os anos 90, o número de crimes cibernéticos no país têm crescido consideravelmente, atingindo altos patamares na atualidade.

Vale ressaltar que em junho de 1997 foi criado o CERT.br, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, cujo objetivo é de fornecer respostas aos incidentes de segurança cibernética que procedem no país. O CERT.br possui um relatório contendo estatísticas dos incidentes que lhe são reportados desde o ano de 1999 até o ano de 2020. Como consta neste relatório, no primeiro ano de registro, foram reportados pouco mais de 3 (três) mil incidentes. Em 2014, os registros ultrapassaram a marca de 1 (um) milhão. Em 2020, último ano registrado, foram mais de 665 (seiscentos e sessenta e cinco) mil incidentes reportados[14].

A realidade é que tem sido mais fácil adquirir um dispositivo virtual e contratar serviços de provedoras de Internet, viabilizando a circulação de pessoas no mundo digital. Nesta senda, os criminosos viram a Internet como uma grande oportunidade para cometerem seus crimes, principalmente pela quantidade de vítimas que podem ser impactadas em um curto espaço de tempo.

Cabe pontuar que, a partir do ano de 2020, o planeta passou a experienciar uma nova realidade. A pandemia de COVID-19 foi uma propulsora ao desenvolvimento e intensificação

---

[12] De acordo com o glossário, um ataque cibernético é uma tentativa de desabilitar computadores, roubar dados ou usar um sistema de computador violado para lançar ataques adicionais. Disponível em: <https://www.unisys.com/pt/glossary/what-is-cyber-attack/> Acesso em 20 jan. 2023

[13] JORDÃO, Francisco. "Invasores" ameaçam arquivos da Unicamp. **Folha de São Paulo**. 30 abr. 1995, Cotidiano. Disponível em: <https://www1.folha.uol.com.br/fsp/1995/4/30/cotidiano/36.html> Acesso em 13 jan. 2023

[14] Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Estatísticas dos Incidentes Reportados ao CERT.br. **CERT.br.** 16 mar. 2022. Disponível em: <https://www.cert.br/stats/incidentes/> Acesso em 13 jan. 2023

do uso de tecnologias, principalmente no Brasil. Neste contexto, o país figurou como um dos principais alvos de ataques cibernéticos, como veremos adiante.

3.2 A ocorrência de crimes cibernéticos no contexto de pandemia de COVID-19

No ano de 2020, os principais veículos de comunicação mundiais anunciaram a pandemia de COVID-19. Para a contenção da propagação do coronavírus e, consequentemente, da taxa de pessoas infectadas, a OMS propôs uma série de recomendações. Sendo uma doença transmissível por vias aéreas, os Estados tiveram de tomar providências para promover o distanciamento entre pessoas, como por exemplo, o isolamento social; o fechamento dos comércios; as restrições nos horários de funcionamento e de lotação máxima dos estabelecimentos; além de cuidados básicos como a utilização de máscaras, a higienização das mãos e o uso do álcool em gel.

Ante as circunstâncias, atividades antes exercidas presencialmente migraram para o remoto, até mesmo as práticas ilícitas. De acordo com o sítio eletrônico da Security Report um relatório do FortiGuard Labs, laboratório de inteligência de ameaças da empresa de soluções e serviços em cibersegurança Fortinet, tomando por base dados coletados nos seis primeiros meses do ano de 2022, o Brasil sofreu cerca de 31,5 (trinta e um vírgula cinco) bilhões de tentativas de ataques cibernéticos, sendo a segunda nação que mais sofreu tentativas na América Latina[15]. Esse número implica em um aumento de 94% (noventa e quatro por cento) com relação ao mesmo período no ano de 2021. Já uma reportagem do Profissão Repórter, programa jornalístico da Rede Globo apontou que o número de golpes cometidos pela Internet ampliou em 175% (cento e setenta e cinco por cento) durante a pandemia.[16]

Ademais, como alude o sítio eletrônico da FDR, em 2021, os criminosos virtuais geraram um prejuízo de 6 (seis) trilhões de dólares, conforme o relatório Atividade Criminosa

---

15 REDAÇÃO. Brasil é o segundo país que mais sofre ataques cibernéticos na América Latina. Laboratório registrou 31,5 bilhões de tentativas de invasão no país no primeiro semestre do ano, quase o dobro reportado no mesmo período de 2021. **Security Report**. 23 ago. 2022. Disponível em: https://www.securityreport.com.br/overview/brasil-e-o-segundo-pais-que-mais-sofre-ataques-ciberneticos-na-america-latina/#.Y3WNPHbMK5d> Acesso em 17 jan. 2023

16 PROFISSÃO REPÓRTER. Crimes virtuais crescem no Brasil; veja flagrante e histórias de vítimas com o Profissão Repórter. O número de golpes cometidos pela internet sofreu um aumento de 175% durante a pandemia e nossa equipe conversou com vítimas de fraude financeira e stalking, além de acompanhar uma operação policial contra a pornografia infantil. **Profissão Repórter**. 27 jul. 2022 Disponível em: <https://g1.globo.com/profissao-reporter/noticia/2022/07/27/crimes-virtuais-crescem-no-brasil-veja-flagrante-e-historias-de-vitimas-com-o-profissao-reporter.ghtml> Acesso em: 17 jan. 2023

Online do Brasil desenvolvido pela Axur, empresa de monitoramento, reação e remoção de riscos e ameaças digitais na Internet.[17] Além de prejuízos financeiros, os crimes virtuais também podem ocasionar desconfortos emocionais.

Em sintonia com o estudo elaborado pela empresa de cibersegurança Symantec, é possível afirmar que os traumas decorrentes de crimes virtuais equiparam-se aos "tradicionais". É mencionado que é comum entre as vítimas desses crimes a sensação de frustração e descrença quanto à eficiência do Judiciário.[18]

Somado a isto, pode-se dizer que o temor perante as ameaças que existem na *web* suscita a insegurança no uso da Internet. É o que demonstra um levantamento realizado pela empresa de segurança digital Psafe em que os pesquisados declararam preocupação em terem seus dados roubados (44,27%), em sofrerem golpes (24,88%) e em terem suas redes sociais invadidas (21,59%)[19].

É bem verdade que a pandemia contribuiu para uma era ainda mais digital em um curto espaço de tempo. Por outro lado, como bem demonstram os dados acima, nem todos os usuários das redes fazem bom uso delas, já que as aproveitam para fins ilícitos. Um dos fatores que contribuem para a ocorrência dos crimes cibernéticos é o anonimato, isto é, a condição em que o usuário interage na *web* sem ter sua identidade identificada. Baseado nisso, os criminosos podem agir sem temer serem descobertos.

Um outro elemento que pode propiciar a ocorrência dos crimes virtuais é o comportamento das próprias vítimas, na visão de Sydow (2015):

> Destarte, a grande maioria dos internautas vaga por endereços virtuais sem ser capaz de ponderar quão seguro está e o quanto é prudente permanecer se embrenhando em tais sítios. Também, quando abordado por e-mail, mensagem de rede social ou até mesmo por SMS, vê no interlocutor mal-intencionado a aparência neutra, quiçá a mesma de seus contatos, conhecidos, amigos etc. (...) Para o que se quer chamar a atenção, nesta sociedade de risco, é o fato de que, se por um lado a tecnologia dá aos usuários ampla liberdade e máxima

---

[17] AMORIM, Paulo. Crimes cibernéticos causaram prejuízo de US$6 trilhões em 2021. **FDR**. 10 fev. 2022. Disponível em: <https://fdr.com.br/2022/02/10/crimes-ciberneticos-causaram-prejuizo-de-us-6-trilhoes-em-2021/> Acesso em: 18 jan. 2023

[18] CORREIO BRAZILIENSE. Crimes na web causam traumas tão sérios quanto no mundo real, diz pesquisa. 29 nov. 2010, Tecnologia. Disponível em: <https://www.correiobraziliense.com.br/app/noticia/tecnologia/2010/11/29/interna_tecnologia,225250/crimes-na-web-causam-traumas-tao-serios-quanto-no-mundo-real-diz-pesquisa.shtml> Acesso em: 18 jan. 2023

[19] ANDRION, Roseli. Metade dos brasileiros se sente insegura ao navegar na web, aponta estudo. **TechTudo**. 09 fev. 2022, Segurança. Disponível em: <https://canaltech.com.br/seguranca/metade-dos-brasileiros-se-sente-insegura-ao-navegar-na-web-aponta-estudo-208747/> Acesso em: 19 jan. 2023

> igualdade individual, por outro lado ela lhes retira a habilidade de distinguir as pessoas com as quais se relacionam virtualmente, além de lhes restringir a capacidade de diferenciar a sensação de segurança da ideia de segurança como realidade. (SYDOW, 2015, p. 17)

O ponto que o autor Sydow (2015) quis frisar é que muitos daqueles que usufruem dos dispositivos informáticos são leigos no quesito de segurança virtual, a ponto de não possuírem a expertise exigida para diferenciar quais informações são verdadeiras e quais seriam possíveis golpes sendo aplicados pelos delinquentes. A carência de uma educação para os meios digitais, facilita que os transgressores obtenham êxito em seus intentos.

Para corroborar com a referida tese, temos uma pesquisa realizada pela empresa de *softwares* de segurança virtual Kaspersky que expôs que o Brasil foi o país com o maior número de casos de *phishing* no ano de 2020[20]. Conforme doutrinam Wendt e Jorge (2021, p. 61) "o termo *phishing* é originado da palavra inglesa *fishing*, que significa pescar, ou seja, é a conduta daquele que pesca informações sobre o usuário de computador". É o exemplo de *links* maliciosos enviados pelos golpistas por meios eletrônicos para que as pessoas forneçam seus dados bancários aos criminosos. Verifica-se ainda que a grande quantidade de golpes aplicados é um reflexo da vulnerabilidade a que estão expostos os internautas em razão da insuficiência de domínio em perceber a veracidade das informações que recebem.

Percebe-se, por conseguinte, que os crimes cibernéticos são uma realidade no nosso país há, pelo menos, duas décadas. Defronte tal conjuntura, os juristas têm se dedicado a elaborar legislações e discutir o tema, aprimorando e aplicando o Direito Penal Informático.

No próximo tópico, abordaremos, então, os principais conceitos e classificações dos crimes virtuais.

4. CONCEITOS E CLASSIFICAÇÕES DOS CRIMES CIBERNÉTICOS

4.1 Conceito de Crime

Em primeiro plano, antes de iniciarmos a exposição acerca dos conceitos de crimes cibernéticos, é válido elucidarmos as características do que é considerado crime nos moldes do ordenamento jurídico brasileiro. Não há na legislação interna uma definição precisa do que

---

[20] FERNANDES, Rodrigo. Brasil é líder mundial em golpes de phishing; saiba se proteger. Um em cada cinco brasileiros sofreu pelo menos uma tentativa de ataques do tipo em 2020; crimes cresce mais de 120% na pandemia. **TechTudo**. 06 mai. 2021, Segurança. Disponível em: <https://www.techtudo.com.br/noticias/2021/03/brasil-e-lider-mundial-em-golpes-de-phishing-saiba-se-proteger.ghtml> Acesso em 24 jan. 2023

é crime. Nesse sentido, Bittencourt (2021) faz uma breve crítica ao art. 1º da Lei de Introdução do Código Penal e da Lei das Contravenções Penais (Decreto-Lei n° 3.914 de 09 de dezembro de 1941) expressando que o legislador não se atentou a definir "crime" e "contravenção penal", sendo que apenas os diferencia apoiando-se no critério da penalidade aplicável a cada um, *in verbis:*

> Art 1º - Considera-se crime a infração penal que a lei comina pena de reclusão ou de detenção, quer isoladamente, quer alternativa ou cumulativamente com a pena de multa; contravenção, a infração penal a que a lei comina, isoladamente, pena de prisão simples ou de multa, ou ambas, alternativa ou cumulativamente.

Diante da lacuna legislativa, a doutrina se consagrou em tentar elaborar tal definição, sobrevindo divergências entre os autores. A respeito do conceito analítico de delito, há duas correntes doutrinárias preponderantes: a teoria tripartida e a teoria bipartida de crime. A primeira, defendida por autores como Nucci (2022) e Greco (2022), define crime como um fato típico, antijurídico e culpável. Já a segunda, compartilhada entre autores como Jesus (2020) e Capez (2021), a culpabilidade não é um pressuposto essencial do crime, sendo uma mera "régua" que o juízo recorre para majorar ou atenuar a pena, restando como elementos caracterizadores do delito apenas a tipicidade e a ilicitude. Nesse ponto, vejamos as lições de Capez (2021):

> Na culpabilidade afere-se apenas se o agente deve ou não responder pelo crime cometido. Em hipótese alguma será possível a exclusão do dolo e da culpa ou da ilicitude nessa fase, uma vez que tais elementos já foram analisados nas precedentes. Por essa razão, culpabilidade nada tem que ver com o crime, não podendo ser qualificada como seu elemento. (CAPEZ, 2021, p. 159)

Registra-se que o Código Penal brasileiro adotou a Teoria Bipartida de crime. Prova disto é a determinação do art. 59, *caput*, que designa a culpabilidade como um critério para a fixação da pena:

> Art. 59 - O juiz, atendendo à culpabilidade, aos antecedentes, à conduta social, à personalidade do agente, aos motivos, às circunstâncias e conseqüências do crime, bem como ao comportamento da vítima, estabelecerá, conforme seja necessário e suficiente para reprovação e prevenção do crime: (...)

Logo, podemos dizer que o fato criminoso é caracterizado pela tipicidade que, segundo Bitencourt (2021), seria a circunstância do fato praticado estar em conformidade com o tipo penal previsto em lei; e pela ilicitude, também denominada antijuridicidade, a qual, Bitencourt (2021) define como a contradição existente entre o fato praticado pelo agente infrator e o ordenamento jurídico.

4.2 Conceitos de Crimes Cibernéticos

No tocante aos crimes cibernéticos, Jesus e Milagre (2016, p. 20) listam outras nomenclaturas utilizadas para destiná-los como “crimes de computador”, “delito informático”, “crimes virtuais”, “crimes digitais”, “crimes eletrônicos”, dentre outras terminologias.

Nascimento (2019) aponta que o termo “cibercrime” foi aludido pela primeira vez no final da década de 90 após uma reunião do Grupo do Lyon, composto por Estados Unidos, Japão, Alemanha, Reino Unido, França, Itália, Canadá e Rússia, quando tais nações empregaram o termo para designar práticas ilícitas cometidas por meio da Internet.

A doutrina tem elaborado diversos conceitos e classificações para estes tipos de crimes. Kerr (2011, p. 23), menciona que, de acordo com a moderna criminalística, o delito informático seria “toda a ação típica, antijurídica e culpável, praticada contra ou através da transmissão, processamento e armazenamento automático de dados”.

Já Jesus e Milagre (2016, p. 20) definiram os cibercrimes como “(...) o fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação”, e completam: “(...) no crime informático, a informática ou é o bem ofendido ou o meio para a ofensa a bens já protegidos pelo Direito Penal”.

Detecta-se que entre as definições dadas acima há certas divergências com relação à teoria do crime adotada e ao bem jurídico tutelado. Uma definição mais recente é apresentada por Wendt e Jorge (2021), que compreendem os crimes virtuais como aqueles que são praticados utilizando dispositivos informáticos que podem ou não estar conectados à internet.

4.3 Classificação dos Crimes Cibernéticos

Uma classificação mais antiga dos crimes digitais é apresentada por Vianna (2001). O escritor, partindo do pressuposto de que o bem jurídico tutelado pela norma penal é a inviolabilidade de dados, classifica os crimes cibernéticos em delitos informáticos impróprios; delitos informáticos próprios; e delitos informáticos mistos.

Para Vianna (2001), os delitos informáticos impróprios são caracterizados pela utilização do computador como instrumento de execução do delito, sem que haja ofensa à inviolabilidade de dados. Seria o caso de um crime contra a honra, como calúnia, difamação ou injúria (arts. 138, 139 e 140, do CP), cometido por meio de envio de um e-mail, como bem exemplifica o autor.

Já os delitos informáticos próprios, para Vianna (2001) seriam aqueles em que há a violação da inviolabilidade de dados, como é o caso da interceptação legal em que os dados são capturados durante sua transferência de um sistema computacional para outro, tipificado no art. 10 da Lei n. 9.296/1996, que regula a interceptação telefônica.

Por fim, os delitos informáticos mistos, segundo o doutrinador, visa proteger além da inviolabilidade de dados outro bem jurídico de natureza diversa, e exemplifica com o art. 67, inciso VII, da Lei n. 9.100/1995 que tipificou como crime eleitoral a obtenção ou tentativa de obtenção indevida de acesso a sistema de tratamento automático de dados utilizados pelo serviço eleitoral, para fins de alteração da apuração ou contagem de votos.

Wendt e Jorge (2021) expõem uma forma de categorização mais atual. Os autores classificam os crimes cibernéticos em “crimes cibernéticos abertos” e “crimes exclusivamente cibernéticos”. Para eles, os crimes cibernéticos abertos “são aqueles que podem ser praticados da forma tradicional ou por intermédio de dispositivos informáticos” (WENDT; JORGE, 2021, p. 40). Entende-se que é possível a prática dos crimes com ou sem os dispositivos informáticos, sendo tais dispositivos apenas um dos meios pelos quais os criminosos podem se utilizar para agirem. É o caso dos crimes de extorsão e de estelionato tipificados, respectivamente, nos arts. 158 e 171, do CP, como bem ilustram.

Por outro lado, no que tange aos crimes “exclusivamente cibernéticos”, Wendt e Jorge (2021) lecionam não é possível que esses sejam praticados sem a utilização de dispositivos informáticos, tratando-se de meio indispensável para o cometimento do delito. Um exemplo citado pelos doutrinadores é o crime tipificado no art. 244-B, parágrafo 1º do ECA em que emprega-se meios eletrônicos, incluindo salas de bate-papo virtuais para corromper ou facilitar a corrupção de menor de 18 anos, com ele praticando infração penal ou induzindo-o a praticá-la.

Wendt e Jorge (2021) abordam também sobre as “ações prejudiciais atípicas":

> são aquelas condutas, praticadas por intermédio de dispositivos informáticos, que causam algum transtorno e/ou prejuízo para a vítima, porém não existe uma previsão penal, ou seja: o indivíduo causa algum problema para a vítima, mas não pode ser punido, no âmbito criminal, em razão da inexistência de norma penal com essa finalidade. (WENDT; JORGE, 2021, p. 39-40)

À vista disso, considerando o princípio da legalidade o qual impõe que não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal, nos termos do art. primeiro do CP, mesmo que um indivíduo cause malefícios a outro recorrendo-se dos dispositivos informáticos, se não houver previsão legal que vede a conduta praticada, restará

prejudicada a configuração de crime, por ausência do elemento essencial da tipicidade. Sem embargo, Wendt e Jorge (2021) acentuam que, apesar deste indivíduo não poder ser condenado criminalmente, nada impede que responda civilmente pelos danos gerados.

Em resumo, verifica-se que para Wendt e Jorge (2021), a classificação dos crimes em abertos ou exclusivamente cibernéticos, irá depender se o delito pode ser ou não cometido sem a utilização de um dispositivo digital, enquanto que, na forma de classificação de Vianna (2001), os crimes serão categorizados em próprios ou impróprios a depender se houve ou não ofensa à inviolabilidade de dados.

Partindo das considerações desenvolvidas até o momento, evidencia-se que o cerne deste trabalho é o de proceder com uma breve análise do ordenamento jurídico pátrio no que se refere aos crimes cibernéticos, o que será feito a seguir.

5. A LEGISLAÇÃO

Há uns anos não raramente ouvia-se que “a Internet é terra sem lei” ou “a Internet é terra de ninguém”. Tais frases expressam uma falsa perspectiva de que o ciberespaço não possui regras e que os usuários são completamente livres para explorá-lo como bem entenderem, sem que houvesse qualquer tipo de consequência de seus atos. Contudo, não é bem assim. Apesar de os internautas terem certa liberdade para usufruírem da Internet, estes podem ser sim responsabilizados pelas atitudes que tomam no ambiente virtual, especialmente na esfera criminal, na hipótese de ocorrência de algum delito. A errônea ideia de "impunidade na Internet"[21] é um combustível para que pessoas má intencionadas ajam ilicitamente, o que deve ser desencorajado.

Entende-se que o Direito, enquanto conjunto de normas que regularizam a conduta humana, deve acompanhar as mudanças sociais, estando sempre atualizado com relação às novas realidades que emergem. Nesse sentido, Venosa (2022, p. 6; p. 12) leciona: “Em Direito não há dogmas, mas princípios, normas e leis que podem e devem ser alterados de acordo com as necessidades sociais” e completa: “O Direito busca, portanto, a adequação da sociedade, sua melhor convivência, embora cada sistema possa usar métodos diversos”.

---

[21] Do ponto de vista subjetivo, a impunidade consiste na sensação compartilhada entre os membros de uma sociedade no sentido de que a punição de infratores é rara e/ou insuficiente. Disso deriva uma cultura marcada pela ausência de punição ou pela displicência na aplicação de penas. LUPO, Fernando Pascoal. Criminalidade e Impunidade. Regresso Social. Disponível em: <http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/MFN%3D49310.pdf> Acesso em 01 fev. 2023

Em uma configuração social caracterizada por intenso uso da Internet e alarmantes cifras de crimes cometidos virtualmente, os operadores do Direito não podem manter-se inertes. Com relação ao Direito Penal ensina Estefam e Gonçalves (2021):

> Cuida-se do ramo do Direito Público, que se ocupa de estudar os valores fundamentais sobre os quais se assentam as bases da convivência e da paz social, os fatos que os violam e o conjunto de normas jurídicas (princípios e regras) destinadas a proteger tais valores, mediante a imposição de penas e medidas de segurança. (ESTEFAM; GONÇALVES, 2021, p. 22)

Neste norte, cabe ao Direito Penal, principalmente o Direito Penal Informático, área criada a partir da eclosão da Sociedade da Informação com vistas a estudar e regular acerca dos crimes cibernéticos, oferecer respostas às demandas, na medida de sua esfera de atuação, garantindo a proteção aos bens jurídicos mais relevantes.

Filho (2004) evidencia a existência de certa resistência em termos da necessidade de serem formuladas novas legislações direcionadas à punição de crimes praticados em ambientes desmaterializados, questionando-se se as normas penais existentes já bastavam por si só na incriminação dessas condutas. Todavia, como bem pontuado pelo autor, no ambiente virtual, surgiram novas posturas criminosas que já não se relacionavam com os tipos penais correntes.

Ademais, a ausência de leis específicas alimentava o sentimento de "isenção de responsabilidade" dos cibercriminosos e poderia até mesmo, de certa forma, contribuir para a atuação destes infratores, como assinalado por Jesus e Milagres (2016):

> A criminalização dos abusos do domínio da informática sempre foi objeto de controvérsias. Não restam dúvidas que a ausência de leis específicas, somada a ultrapassadas práticas investigativas, era (ou é) elemento que influenciava o criminoso digital no seu intento, amparado por quatro paredes e o suposto anonimato proporcionado pelo seu computador. (JESUS; MILAGRES, 2016, p. 35)

Apoiado nisso, foram idealizados os primeiros projetos de lei com o propósito de sistematizar os crimes cibernéticos. Nesta ocasião, manifestaram-se uma série de propostas legislativas que logo vieram a ser transformadas em lei promulgada. Destarte, a partir da década de 10, surgiram as legislações internas iniciais relativas ao assunto.

Muitas destas leis objetivaram tipificar condutas. Na concepção de Zaffaroni e Pierangeli (1998, p. 421), "o tipo penal é um instrumento legal, logicamente necessário e de natureza predominantemente descritiva, que tem por função a individualização de condutas humanas penalmente relevantes". A importância da tipificação reside no fato de que a tipicidade é elemento essencial para caracterização do crime, sem o qual as condutas não

poderão ser reprimidas pelo Direito Penal. Algumas legislações também se debruçaram a apresentar orientações pertinentes à investigação criminal, facilitando a operacionalização das autoridades no enfrentamento dos crimes cibernéticos.

Passemos à análise das principais legislações nos subtópicos a seguir.

5.1 Lei n° 12.965 de 23 de abril de 2014: Marco Civil da Internet

Conforme consta no seu projeto de lei, o Marco Civil da Internet (MCI) surge de uma proposta da Secretaria de Assuntos Legislativos do Ministério da Justiça, em parceria com o Centro de Tecnologia e Sociedade da Escola de Direito da FGV do Rio de Janeiro que objetivava a criação de um texto que estabelecesse princípios, garantias, direitos e deveres relacionados ao uso da Internet no país, tanto para os usuários quanto para os provedores de conexão, além de outras providências. Descreve o Projeto de Lei n. 2126/2011:

> No âmbito legislativo, diversos projetos de lei tramitam desde 1995, ano do início da oferta comercial de conexões no país. No entanto, passados quinze anos, ainda não existe um texto de lei específico para o ambiente cibernético que garanta direitos fundamentais e promova o desenvolvimento econômico e cultural. (BRASIL, 2011, p. 8)

Os autores da proposta legislativa aduzem ainda que a ausência de uma legislação que padronize as relações virtuais ensejam diversos transtornos como a violação aos direitos dos usuários, as contradições na jurisprudência e até mesmo omissões nas políticas públicas.

Registra-se que o debate acerca do anteprojeto do MCI contou com a participação pública da própria Internet: no final do ano de 2009 e começo do ano de 2010 realizaram-se discussões sobre a proposta por meio de um *blog* disponibilizado na plataforma Cultura Digital e por meio do Twitter, obtendo mais de 2 (dois) mil comentários:

> A dinâmica adotada teve como meta usar a própria Internet para, desde já, conferir mais densidade à democracia. Por meio da abertura e da transparência, permitiu-se a franca expressão pública de todos os grupos sociais, por meio de um diálogo civilizado e construtivo. (BRASIL, 2011, p. 10)

Por fim, os autores do anteprojeto do MCI destacam que a legislação representa um passo inicial por meio do qual será possível, futuramente, posicionar-se de forma mais adequada com relação à relevantes temas atinentes à Internet, inclusive quanto aos crimes cibernéticos.

O texto sofreu algumas alterações durante a sua tramitação na Câmara dos Deputados e no Senado e, após sua aprovação, foi transformado em lei, sancionada pela Presidente da

República à época, Dilma Rousseff. Trata-se da Lei n° 12.965 de 23 de abril de 2014 a qual teve o prazo de 60 dias para entrada em vigor, nos termos do seu art. 32.

Ressalta-se que, de acordo com Fiorillo e Conte (2016), o texto foi aprovado rapidamente pela chefe do Poder Executivo como uma reação do governo às denúncias que ocorriam na época de que autoridades e empresas brasileiras estariam sendo espionadas pela NSA, Agência de Segurança Nacional dos Estados Unidos. Além disso, segundo Jesus e Milagres (2016), a aprovação do MCI representou um verdadeiro triunfo para os brasileiros que clamavam por uma "carta de direitos dos internautas" e que, aliás, ficou conhecida como a "Constituição da Internet".

Constata-se que o MCI é uma legislação majoritariamente principiológica, não prevendo qualquer tipo de crime cibernético, entretanto, não deixa de ser um importante instrumento para o estudo do Direito Penal Informático. Dentre os princípios enumerados em seu art. 3° temos a garantia da liberdade de expressão; a proteção da privacidade e dos dados pessoais; a preservação e a garantia da neutralidade de rede e a responsabilização dos agentes de acordo com suas atividade, conforme incisos I, II, III, IV e VI.

Nesta toada, ressalta-se as críticas feitas ao MCI no sentido de questionar se este de fato apresentou mudanças substanciais ao ordenamento jurídico, conforme discorre Filho (2016). Do ponto de vista do autor, a redação final dada ao MCI é redundante ao reproduzir dispositivos já consagrados pela Constituição Federal. É o que acontece, por exemplo, no art. 7º, inciso I, em que fica estabelecido o direito à inviolabilidade da intimidade e da vida privada e a garantia de indenização pelo dano decorrente de sua violação, sendo a mesma previsão constante no art. 5º, inciso X, da Carta Magna. Sobre isso, Fiorillo e Conte (2016) entendem que o reconhecimento pelo MCI de direitos fundamentais já consagrados por meio de outras normativas como uma pretensão de se reforçar a proteção dada a estes direitos no ambiente digital.

Na esfera criminal, há alguns pontos do MCI que merecem a nossa atenção. Ao longo de sua regulamentação, foram determinados prazos nos quais os provedores de aplicações de Internet e administradores de sistemas autônomos terão a responsabilidade de preservação dos dados de acesso, sob sigilo, o qual pode ser rompido mediante autorização judicial. Tais dados têm a serventia de auxiliar na identificação de autores de delitos, além de servirem como meio de prova em sede processual criminal. Pode, inclusive, as autoridades policiais ou administrativas ou o Ministério Público requerer, de maneira cautelar, que tais registros sejam mantidos por prazo superior ao previsto em lei, conforme previsão do art. 13 e do art. 15 do MCI. Neste ponto, comenta Fiorillo e Conte (2016):

> O Marco Civil da Internet teve por objetivo, nesse aspecto, solucionar um dos grandes impasses no tocante à responsabilidade sobre o conteúdo postado e, principalmente, na contribuição com investigações criminais sobre crimes cibernéticos. Ocorre que, até então, a responsabilidade pelo armazenamento dos dados dos usuários não era regulamentada por lei e cada empresa fazia, quando fazia, a seu modo. (FIORILLO; CONTE, 2016, p. 73)

Tais artigos são uma novidade trazida pelo legislador, visto que ainda não havia sido positivado a determinação da manutenção destes registros pelos provedores e administradores. A manutenção é elementar frente à facilidade com que essas informações podem ser perdidas. Sobre isso, transmitem Dorigon e Soares (2020):

> De modo geral, as evidências deixadas pelos crimes cibernéticos são extremamente instáveis, motivo pelo qual, em razão de seu caráter volátil, podem ser facilmente apagadas, alteradas ou perdidas, devendo o investigador agir com cautela para não corromper evidência alguma que possa ser relevante para a solução da investigação. (DORIGON; SOARES, 2020, p. 2)

Frise-se que essa colaboração entre os provedores e as autoridades contribui para buscar soluções para um antigo impasse existente na persecução penal de crimes cibernéticos: a comprovação de indícios de autoria e de materialidade do delito. Historicamente, os investigadores têm encontrado obstáculos que dificultam a produção desse conjunto probatório como, por exemplo, a questão do anonimato e a do acesso à Internet por via de redes de conexão abertas. Entretanto, pode ser que a partir dessa nova determinação do MCI, os responsáveis pela investigação dos delitos, tendo acesso às informações armazenadas pelos provedores e administradores consiga certificar a ocorrência da infração penal e seu(s) autor(es) para que então se desenrole o processo penal.

Alguns apontamentos quanto à redação dada aos arts. 13 e 15 do MCI são feitos pelos autores. Segundo Fiorillo e Conte (2016), a lei não é clara em informar o marco inicial da contagem do prazo de manutenção, o que pode gerar dificuldades de interpretação do dispositivo. Já Filho (2016) menciona que os referidos prazos teriam sido definidos sem um critério. Além do mais, o art. 13, parágrafo segundo, inciso II, do Decreto n° 8.771 de 11 de maio de 2016, estipula que os registros mantidos pelos provedores devem ser excluídos com o decurso do prazo legal, o que pressiona as autoridades à acelerarem o ritmo da investigação para que seja finalizada antes que os dados sejam eliminados.

Outro dispositivo suscitado pelo MCI que vale a pena sondar é o art. 21, a saber:

> Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.
>
> Parágrafo único. A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

Via de regra, o MCI definiu em seu art. 18 que o provedor de conexão à Internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros. No entanto, o art. 21 é uma exceção à essa regra, prevendo hipóteses de responsabilização subsidiária . De acordo com Néris (2019):

> (...) a lei nascia com uma regra específica de responsabilidade dos provedores de aplicação na Internet para os casos de imagens íntimas não consensuais (NCII), visando a incentivar as plataformas a remover o conteúdo o quanto antes, sem obrigar a vítima a cumprir formalidades, constituir advogado, ou buscar a Justiça.” (NÉRIS, 2019, n.p)

A autora alude que durante as discussões sobre o projeto de lei do MCI ocorreram eventos drásticos que colocaram em pauta a questão levantada pelo art. 21, como os casos das adolescentes Giana Fabi e Julia Rebeca, que tiveram fotos e vídeos íntimos divulgados na Internet e que em vista da situação vexatória que passaram, resolveram tirar as próprias vidas.[22] Na opinião de Sydow (2015), o legislador poderia ter abarcado mais circunstâncias ao art. 21, o que poderia aumentar a proteção dada aos bens jurídicos.

Em resumo, Sydow (2015) interpreta que o Marco Civil da Internet ainda carece de maturidade, sendo questionável a sua eficácia. Entretanto, continua dizendo que:

> A inserção desse importante normativo dá início a uma política legislativa que respeita a urgente necessidade de o Brasil regrar o segmento do direito informático, gerando princípios, garantias e diretrizes, decretando valores sociais e individuais e apresentando importantes definições e formas de obtenção e guarda de dados com alguma segurança jurídica. (SYDOW, 2015, p. 129)

---

[22] COISSI, Juliana. Garotas foram encontradas enforcadas após fotos e vídeos publicados na internet. **Folha de São Paulo.** 01 dez. 2013, Cotidiano. Disponível em: <https://m.folha.uol.com.br/cotidiano/2013/12/1379103-garotas-foram-encontradas-enforcadas-apos-fotos-e-videos-publicados-na-internet.shtml> Acesso em 04 fev. 2023

Ante o exposto, apesar de tratar-se de uma legislação civil, é inegável a sua relevância para inaugurar as discussões acerca do Direito Penal Informático, abordando conceitos iniciais e princípios que devem ser observados nas relações digitais.

5.2 Lei n° 13.709 de 14 de agosto de 2018: Lei Geral de Proteção de Dados

A Lei n° 13.709 de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD) é uma legislação brasileira que teve inspiração na *General Data Protection Regulation* (GDPR), regulamentação originada em 2018 com o intuito de promover a proteção dos dados na União Europeia. Em vista da preocupação com a segurança virtual, a LGPD veio a complementar os ditames já existentes acerca da proteção de dados, definindo dados pessoais e designando como devem ser tratados. A propósito:

> Art. 1º - Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

De acordo com o art. quinto, inciso I da LGPD, dado pessoal é qualquer informação relacionada a pessoa natural identificada ou identificável como nome, número de telefone, endereço, etc. A proteção dos dados pessoais é primordial para a garantia da privacidade e para evitar que criminosos tenham acesso a estas informações, utilizando-se destas de maneira indevida. Assim, a LGPD impacta diretamente na forma como empresas e Estado manejam os dados pessoais, os quais devem se adaptar às normas previstas nesta lei, sob pena de responsabilização.

Sobre isso, apesar da LGPD ter entrado em vigor em 2018, somente no ano seguinte é que foi criada a Autoridade Nacional de Proteção de Dados (ANPD), autoridade responsável por, dentre outras atribuições, fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento às normas, nos termos do art. 55-J, inciso IV, da Lei n° 13.853/2019. Ainda, destaca-se que as referidas sanções administrativas previstas nos arts. 52 a 54, só começaram a ser aplicadas em 1 de agosto de 2021, nos termos do art. 20 da Lei n° 14.010/2020.

Em que pese a LGPD tenha significado um importante passo para a cibersegurança nacional, de acordo com a empresa brasileira de tecnologia Flowti, os criminosos digitais

descobriram uma brecha para cometimento de delitos por meio da LGPD[23]. Conforme elucida a referida empresa, os cibercriminosos invadem os sistemas de empresas e tomam posse de dados pessoais de colaboradores, clientes e parceiros, e, em posse dessas informações, servem-se de chantagem contra essas empresas para conseguirem vantagens financeiras pelo resgate dos dados extraviados. Dessa forma, por vezes, os empresários preferem ceder às extorsões dos criminosos em troca da recuperação dos dados, do que pagarem as altas multas previstas na LGPD.

Nesta conjuntura, compreende-se a notoriedade das empresas e do Estado brasileiro se adequarem às normas enunciadas na LGPD para a resguarda de ataques cibernéticos. Porém, a realidade atual é que tal adequação ainda está em um patamar longe do ideal, dado que em conformidade com a Pesquisa de Privacidade e Proteção de Dados realizada pelo grupo Daryus Consultoria e Treinamentos apenas 20% (vinte por cento) das companhias no Brasil estão completamente adequadas à LGPD.[24]

5.3 Lei n. 12.737 de 30 de novembro de 2012: Lei de Crimes Cibernéticos ou Lei Carolina Dieckmann

A Lei n. 12.737/2012 de 30 de novembro de 2012 ficou popularmente conhecida por "Lei Carolina Dieckmann". Tal instrumento normativo é uma resposta a um famoso episódio ocorrido com a atriz global Carolina Dieckmann que teve seu computador invadido, em maio de 2011, e o invasor teve acesso às suas fotos pessoais de cunho íntimo. Detendo posse das fotografias, o invasor exigiu o pagamento de uma quantia de dinheiro à atriz. Com a recusa da artista, as imagens foram compartilhadas na Internet, expondo a intimidade da vítima.

A grande repercussão do incidente aqueceu os debates quanto à criminalização dessa prática. Nisto, foi elaborado o Projeto de Lei 2.793/2011 o qual, após a sua ligeira aprovação, foi transformado na Lei n. 12.737/2012, a Lei de Crimes Cibernéticos ou Lei Carolina Dieckmann. Esta lei modificou o Código Penal, alterando a redação dada ao art. 266 que refere-se à interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública e ao art. 298 que refere-se à falsificação de

---

[23] FLOWTI. A importância da LGPD no combate aos cibercrimes. 12 nov. 2021. Disponível em: <https://flowti.com.br/blog/a-importancia-da-lgpd-no-combate-aos-cibercrimes> Acesso em 29 jan. 2023

[24] PIGNATI, GIOVANA. 80% das empresas no Brasil ainda não se adequaram à LGPD. **Canaltech**. 07 dez. 2022, Mercado. Disponível em: <https://canaltech.com.br/mercado/80-das-empresas-no-brasil-ainda-nao-se-adequaram-a-lgpd-232255/> Acessi em 29 jan. 2023

documento particular. Porém, a legislação ganhou notoriedade mesmo em decorrência da tipificação do crime de invasão de dispositivo informático, por meio da inclusão dos arts. 154-A e 154-B ao CP:

> 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.
> §1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º , aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.
>
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Após anos em vigência, o artigo que previu o crime de invasão de dispositivo informático foi alterado pela Lei n° 14.155 de 27 de maio de 2021, sobre a qual iremos discorrer futuramente neste trabalho.

Reina (2022, n.p) comenta que a Lei n. 12.737/2012 foi alvo de críticas em razão de seu "texto vago e carente de aspectos técnicos", apontando como uma falha favorável aos cibercriminosos a falta de precisão em saber os tipos de dispositivos nos quais poderiam ocorrer a invasão. Nesse mesmo sentido, agregam Jesus e Milagres (2016, p. 16): "Não temos

um glossário na Lei n. 12.737/2012, o que pode gerar interpretações distintas para o termo "dispositivo informatizado"".

Da perspectiva de Sampei (2015), a Lei Carolina Dieckmann apresenta lacunas já que deixou de abarcar diversas situações no tipo penal de invasão de dispositivo informático. Isso porque, segundo a autora, não é criminalizado, por exemplo, o ato de invadir o dispositivo eletrônico e ver as fotografias presentes nele, já que não necessariamente haverá a "obtenção, adulteração ou destruição" dos dados, condutas necessárias para a configuração do crime.

Outro exemplo citado por Sampei (2015) é quando o agente acessa as redes sociais de alguém sem que haja a violação do computador, o que também não seria considerado crime. Os apontamentos da autora encaminham-se no sentido de que condutas capazes de causar danos poderiam ter sido criminalizadas e, consequentemente, punidas na esfera do Direito Penal, caso o legislador tivesse atentado-se a incluí-las no texto legal, mas não o fizeram.

Lado outro, do ponto de vista de Reina (2022, n.p), é possível afirmar que a Lei Carolina Dieckmann é um "marco inicial para a proteção de dados pessoais dos cidadãos contra os criminosos virtuais", visto que antes de sua promulgação não havia previsão que tipificasse a invasão de sistemas.

Apesar das ressalvas, é inegável que a Lei n. 12.737/2012 contribuiu para colocar em evidência a pauta dos crimes cibernéticos no país, abrindo espaço para elaboração de novas leis.

5.4 Lei n. 12.735 de 30 de novembro de 2012: Lei Azeredo

No mesmo dia da publicação da Lei de Crimes Cibernéticos, também foi promulgada a Lei n. 12.735 de 30 de novembro de 2012, conhecida por Lei Azeredo. A Lei Azeredo oriunda com o Projeto de Lei n. 84 de 1999. Explica Filho (2004) que o projeto de lei tentou criar novas tipificações, além de aumentar o âmbito de incidência de crimes já previstos no CP, abarcando os fenômenos que decorrem no meio desmaterializado.

Contudo, o Projeto de Lei n. 84/99 foi bastante polêmico e, como resultado, à época da aprovação da Lei n. 12.735/2012 a maioria de seus artigos tinham sido vetados. De acordo com Lemos et al (2008), as disposições constantes no Projeto de Lei n. 84/99 apresentavam problemas quanto ao seu âmbito de abrangência e quanto à sua precisão, o que poderia conduzir a interpretações equivocadas[25].

[25] LEMOS, Ronaldo; BOTTINO, Thiago, et al. Comentários e Sugestões sobre o Projeto de Lei de Crimes Eletrônicos (PL n. 84/99). Centro de Tecnologia e Sociedade. Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas. 2008, p. 1-21. Disponível em:

A legislação aprovada em 2012 alterou o Código Penal, o Código Penal Militar e a Lei de Crimes Raciais. O seu art. 5° deu nova redação ao art. 20, parágrafo terceiro, inciso II da Lei de Crimes Raciais prevendo a possibilidade do juiz, em caso de crime de prática, indução ou incitação a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional, e ouvido o Ministério Público ou a pedido deste, antes mesmo do inquérito policial, determinar a cessação das transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio.

O ponto chave da Lei Azeredo recai nas determinações do seu artigo quarto. Restou positivado que os órgãos de polícia judiciária deverão estruturar setores e equipes especializadas no combate à ação delituosa em redes de computadores, dispositivo de comunicação ou sistema informatizado. Neste ponto, o legislador ponderou no tocante à imprescindibilidade de se ter instituições e profissionais qualificados para a tomada de diligências que a investigação de crimes virtuais exige. Nisto, exterioriza Barreto (2018):

> Não obstante a criação de delegacias especializadas contribuírem, de forma significativa, na resolução de fatos de difícil elucidação, como homicídios ou ataques a instituições financeiras, a seara dos crimes informáticos é bastante distinta, não dependendo, pois, de apenas um setor com expertise, e sim da polícia como um todo, com capacidade de buscar e materializar a evidência eletrônica. (BARRETO, 2018, n.p)

Ademais, o autor recomenda uma releitura da Lei Azeredo de forma a propiciar que tais delegacias e setores especializados se encarreguem apenas dos crimes próprios e de maior complexidade. Tais medidas evitariam uma sobrecarga destes setores e uma atuação mais eficiente. Ainda sobre o assunto, Crespo (2015) disserta:

> A medida é salutar, mas depende do Poder Público a ela prover a concretude necessária, investindo na especialização da Polícia com treinamentos e equipamentos. Ainda não se pode dizer que as delegacias que foram criadas estão plenamente aptas a prover o atendimento adequado às vítimas de crimes digitais. (CRESPO, 2015, n.p)

Destarte, depreende-se que a Lei Azeredo é decorrente de um projeto que visava explorar de maneira vasta a temática dos crimes virtuais mas que, após sofrer numerosas reduções, foi aprovada com poucas inovações normativas, cuja eficiência subordina-se aos esforços advindos do Poder Público.

<https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/2669/Estudo_CTS_FGV_PL_crimes_eletronicos.pdf> Acesso em 10 fev. 2023

Ademais, reafirma-se que, indo ao encontro dos raciocínios estabelecidos acima, a atuação da Administração Pública para a construção de uma estrutura investigativa capaz de apurar os delitos digitais vão além da criação de órgãos especializados, englobando também a preparação de profissionais para trabalharem na área; uma política criminal bem estruturada; a destinação de recursos financeiros; a disponibilização de todos os equipamentos necessários para que as autoridades possam exercer o seu papel, dentre outros fatores.

5.5 Lei n. 14.155 de 27 de maio de 2021

Faz-se mister salientar que a Lei Carolina Dieckmann foi questionada quanto às suas punições, em virtude do entendimento que o crime de invasão de dispositivo informático é um crime de menor potencial ofensivo, não sendo possível a fixação de penas restritivas de liberdade. É o que evidencia Sampei (2015):

> Estamos diante de uma Lei Penal fraca ante o grande avanço tecnológico que vivenciamos. Como já mencionado, as penas são muito fracas em relação ao tipo de crime cometido, seria necessário uma punição maior de seus agentes. Pena máxima de dois anos considera o crime como de menor potencial ofensivo. Tamanho estrago na vida da vítima não deve ser considerado crime de menor potencial ofensivo. (SAMPEI, 2015, n.p)

Nestas circunstâncias, a Lei n. 14.155 de 27 de maio de 2021 encarregou-se de rever esta e outras questões provocando modificações no Código Penal e no Código de Processo Penal. A nova legislação retirou a necessidade de violação indevida de mecanismo de segurança para a configuração do crime de invasão de dispositivo informático, além de ter majorado as penas inicialmente cominadas.

No tocante a primeira mudança, Jorio e Boldt (2021, n.p) comentam que novos fatos poderão ser enquadrados no tipo penal, além de ter se tornado mais fácil identificar a prática do crime: “Mas o fato é que uma elementar típica objetiva que restringia as hipóteses de configuração do crime foi retirada, o que, por óbvio, acabará facilitando o reconhecimento da sua prática.”

A segunda mudança demonstra a intenção do legislador em melhor repreender o crime, perante as críticas de que as penas antes impostas eram brandas. Com o aumento da pena do *caput* de 3 (três) meses a 1 (um) ano e multa para 1 (um) a 4 (quatro) anos e multa, a pena também foi alterada de reclusão para detenção. Esclarece Ganem (2022):

> Na prática, isso significa que, se preso em flagrante, o autor do delito será submetido a lavratura de auto de prisão em flagrante e não mero

> termo circunstanciado de ocorrência, como anteriormente se admitia. O delito sai da alçada do Juizado Especial Criminal (rito sumaríssimo) e não mais admite transação penal. Contudo, como sua pena não excede a 4 anos, ainda é possível o arbitramento de fiança pelo Delegado de Polícia; a suspensão condicional do processo, prevista no art. 89 da Lei nº 9.099/95; o acordo de não persecução penal (art. 28-A do CPP) e a interceptação telefônica, salvo a captação ambiental, admitida apenas para delitos com pena superior a 4 anos de reclusão. (GANEM, 2022, n.p)

Também foram majorados os limites da causa de aumento de pena do parágrafo segundo de ⅓ (um terço) para ⅔ (dois terços); e a pena qualificadora do parágrafo terceiro para de 2 (dois) a 5 (cinco) anos e multa, nos termos dos parágrafos segundo e terceiro, respectivamente.

Ainda dentro do CP, a Lei n. 14.155/2021 tornou mais grave o crime de furto, nos casos em que é praticado mediante fraude cometida por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo, nos termos do parágrafo 4°-B, adicionado ao art. 155, do CP. As penas serão ainda maiores, caso o crime seja praticado mediante a utilização de servidor mantido fora do território nacional ou caso crime seja praticado contra o idoso ou vulnerável, como definido no parágrafo 4º-C.

Para Jorio e Boldt (2021) há um grande equívoco na elaboração deste artigo. Segundo os autores, o crime de furto presume a subtração de coisa alheia móvel e os dados obtidos em meio virtual não poderiam ser considerados “coisa” em razão de não constituírem matéria:

> Como os dados do mundo digital não constituem matéria, não possuem massa, tecnicamente falando, não podem ser subtraídos, mas apenas copiados, alterados ou apagados de um mundo virtual, composto de ideias, informações e conceitos. Por isso, a imensa maioria das situações em que alguém se servir de fraudes eletrônicas para obter vantagem econômica indevida em prejuízo alheio constituirá estelionato (atualmente, sob a modalidade da novel “fraude eletrônica” – art. 171, § 2º-A, CP). (JORIO; BOLDT, 2021, n.p)

Por conseguinte, conforme Jorio e Boldt (2021) o artigo seria pouco aplicado na prática, incidindo apenas no casos em que os criminosos, por meio da fraude eletrônica, conseguissem distrair suas vítimas ou desativar mecanismos de segurança para, então, subtrair coisa alheia móvel.

Ademais, a Lei n. 14.155 de 27 de maio de 2021, incluiu a fraude eletrônica e o estelionato contra idoso ou vulnerável. Diferente do artigo anterior, criminaliza-se a utilização

dos meios eletrônicos para obtenção de vantagem ilícita, em prejuízo alheio, por meio de indução ou manutenção de alguém em erro. Do ponto de vista de Jorio e Boldt (2021), a tipificação da fraude eletrônica mostrou-se louvável, entretanto, haveria um exagero na pena aplicável, que é de 4 (quatro) a 8 (oito) anos, e multa, de acordo com o parágrafo 2º-A do art. 171, do CP, sem contar com as majorantes estipuladas nos parágrafos subsequentes:

> O legislador brasileiro, em um show de inconstâncias, descarrega toda a fúria punitivista sobre a fraude eletrônica, que, tendo em vista a realidade empírica do mundo moderno, informatizado, cibernético, não tem nada de mais grave ou reprovável do que qualquer outra fraude que se leve adiante por meio de engodos que não envolvam internet, aplicativos ou dispositivos informáticos. (JORIO; BOLDT, 2021, n.p)

Por fim, com relação à mudança ocorrida no art. 70 do CPP para definir que, em crimes de estelionato que envolvam depósito, emissão de cheque sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência para julgar e processar as ações serão definidas pelo local de domicílio da vítima, ou pelo critério da prevenção em caso de pluralidade de vítimas, Jorio e Boldt (2021) entendem que a nova previsão leva a uma superação das súmulas n. 244 do Superior Tribunal de Justiça e n. 521 do Supremo Tribunal Federal que previam que a competência seria regida pelo local onde se deu a recusa do pagamento pelo sacado.

5.6 Lei n. 11.829 de 25 de novembro de 2008

Sublinha-se que os operadores do Direito se dedicaram a reforçar a tutela dada à dignidade e à liberdade sexual no ambiente virtual. A pretexto dos casos de pedofilia na Internet, a Lei n. 11.829 de 25 de novembro de 2008 alterou o Estatuto da Criança e do Adolescente (ECA) para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outas condutas relacionadas à pedofilia na Internet.

Foram acrescentadas ao ECA as novas redações para os artigos 240, 241, 241-A, 241-B, 241-C, 241-D e 241-E, de forma a criminalizar, dentre outras condutas, a produção e a venda de registros que contenham cena de sexo explícita ou pornográfica envolvendo criança ou adolescente, cuja pena cominada foi a de reclusão, de 4 (quatro) a 8 (oito) anos, e multa (art. 240 e art. 241).

Puniu-se a distribuição e/ou a publicação, dentre outras condutas, deste material com a pena de reclusão de 3 (três) a 6 (seis) anos e multa (art. 241-A), e a aquisição, a posse e/ou o

armazenamento dos registros com a pena de reclusão de 1 (um) a 4 (quatro) anos, e multa (art. 241-B).

Criminalizou-se a prática de simular a participação de criança ou adolescente em cena de sexo explícitoou pornográfica por meio de representação visual, sob pena de reclusão de 1 (um) a 3 (três) anos, e multa (art. 241-C); e a prática de aliciar, assediar, instigar ou constranger criança, por qualquer meio de comunicação, com o fim de com ela praticar ato libidinoso, sob pena de reclusão de 1 (um) a 3 (três) anos e multa (art. 241-D).

No que concerne aos pontos polêmicos da Lei n. 11.829/2008, Cruz e Franco (2016) discutem acerca da aplicabilidade desta normativa na responsabilização de empresas com relação a materiais com conteúdo de pornografia infantil armazenados em seus dispositivos eletrônicos pelos empregados e quais medidas poderiam ser adotadas para a repressão deste comportamento sem que houvesse a violação ao direito à privacidade dos funcionários.

No mesmo sentido, discutem acerca da responsabilidade de provedores de serviços de internet, *lan houses*, comunidades *on-line*, dentre outros, com relação aos seus usuários. Observa-se que esta lei antecedeu o Marco Civil da Internet e que este ponto sobre a responsabilização dos provedores veio a ser regulamentado pelo MCI em 2014, como exposto no tópico 5.1. deste trabalho. Sobre isso, Cruz e Franco (2016) opinam:

> Acompanhando a opinião de parte da doutrina, entendemos que a empresa é responsável por todos os dados e imagens visualizados ou baixados pelos usuários em seus equipamentos e que a presença de menores deve ser monitorada conforme dispõem portaria dos juizados especiais. Ainda, os usuários de equipamentos em empresas prestadoras de serviços de informática, principalmente os menores, não podem basear-se no direito à privacidade e à intimidade para praticar atos ilegais. (CRUZ; FRANCO, 2016, p. 80)

Apesar das divergências doutrinárias existentes sobre os pontos críticos acima mencionados, os autores destacam que a Lei n. 11.829/2008 é o principal avanço existente no ordenamento jurídico brasileiro dos últimos anos no combate a pornografia infantil, devido ao fato de ter criado novos crimes para reprimir condutas ilegais antes não tipificadas.

5.7 Lei n. 13.718 de 24 de setembro de 2018 e Lei n. 13.772 de 19 de dezembro de 2018

Em continuidade ao raciocínio traçado no tópico anterior, é pertinente realçar que as Lei n. 13.718 e Lei n. 13.772, ambas de 2018, também tiveram por objeto de tutela a dignidade e a liberdade sexual, mormente no meio virtual. A Lei n. 13.718/2018 incluiu o art.

218-C que versa sobre o crime de divulgação de cena de estupro ou cena de estupro de vulnerável, de cena de sexo ou de pornografia, a saber:

> Art. 218-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia.

A pena é de reclusão de 1 (um) a 5 (cinco) anos, se o fato não constituir crime mais grave. De acordo com o parágrafo primeiro do art. 218-C, a pena será aumentada de ⅓ (um terço) a ⅔ (dois terços) caso o delito seja praticado por agente que mantenha ou tenha mantido relação íntima de afeto com a vítima ou com o fim de vingança ou humilhação.

Essa previsão de majoração de pena é fruto de uma reinvidicação social pela criminalização da *revenge porn* ou pornografia de vingança. Isso porque a Internet possibilitou o vazamento de conteúdos sexuais, essencialmente por ex-companheiros, após o término do relacionamento, com fins de causar desconforto à vítima. Esse tipo de atitude pode gerar danos sérios à pessoa que teve sua intimidade exposta, o que justificou o surgimento deste dispositivo legal, como apontado por Advogados (2020):

> O vazamento de conteúdo íntimo traz diversas consequências à vítima. Já foram registrados vários casos de jovens que não aguentaram a exposição e cometeram suicídio. Quando não leva a atitudes extremas, o *revenge porn* deixa marcada a reputação de quem foi exposto. Isto quando não leva a problemas ainda mais sérios, que ultrapassam a esfera da moral, chegando a casos de agressões físicas e assédio sexual. (ADVOGADOS, 2020, n.p)

Antes da Lei n. 13.718/2018 os crimes de *revenge porn* eram julgados como crimes contra a honra, cuja pena era muito menor e a ação penal era privada, ou seja, dependia da iniciativa do ofendido. A Lei n. 13.718/2018 destaca-se ainda pela tipificação do crime de importunação sexual, além de ter definido que todos os delitos contra a liberdade sexual e delitos sexuais contra vulnerável fossem processados mediante ação pública incondicionada, e não mais por meio de ação pública condicionada à representação.

De igual forma, a Lei n. 13.772/2018 acrescentou o art. 216-B ao CP que tipificou o crime de registro não autorizado da intimidade sexual, que consiste em:

> Art. 216-B. Produzir, fotografar, filmar ou registrar, por qualquer meio, conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado sem autorização dos participantes.

Sobre a redação dada ao *caput* do art. 216-B, Caramigo (2019) faz uma breve observação relativamente ao plural em "sem autorização dos participantes", evidenciando que a disposição não poderá ser aplicada àqueles que registrarem a intimidade sexual de alguém sem autorização em se tratando de uma única vítima:

> Ora, se o tipo fala em "participanteS", só se pode punir alguém pelo *caput* do artigo 216-B quando este alguém praticar a conduta em face de mais de uma pessoa envolvida, sob pena de atipicidade da conduta do referido artigo se assim não o for. O tipo penal é taxativo e não admite analogia *in malam partem.* (CARAMIGO; 2019, n.p)

A pena prevista para o crime de registro não autorizado da intimidade sexual é de detenção de 6 (seis) meses a 1 (um) ano e multa. Percebe-se que, em comparação com o art. 218-C do CP, incluído pela Lei n. 13.718/2018, a pena cominada é bem menor, o que evidencia o entendimento do legislador no sentido de que as condutas tipificadas neste artigo seriam "menos graves" do que as contidas no art. 218-C.

Na prática, é possível que o mesmo agente pratique ambos os crimes. Com base nisto, Cunha (2019) questiona se deve ser aplicado o princípio da consunção (quando o crime fim absorve o crime meio), impondo que o agente seja condenado apenas pelo delito mais gravoso, ou se deve haver o concurso de crimes (quando o agente comete dois ou mais delitos com uma ou mais ações), preceituando que o agente deva ser condenado tanto pelo art. 218-C quanto pelo art. 216-B.

Para a resolução deste dilema, Cunha (2019) aponta que tudo vai depender da situação e da intenção do criminoso. Se o autor do fato já produz o conteúdo com a intenção de divulgá-lo, aplica-se a consunção, mas, se a produção é para satisfação própria e, oportunamente, decide pela divulgação deste material, poderia ser aplicável a hipótese de concurso de delitos.

O parágrafo único do referido artigo estabelece que também poderá ser responsabilizado aquele que realiza montagem em fotografia, vídeo, áudio ou qualquer outro registro com o fim de incluir pessoa em cima de nudez ou ato sexual ou libidinoso de caráter íntimo.

5.8 Convenção de Budapeste

Na seara estrangeira, destaca-se a Convenção de Budapeste sobre crimes cibernéticos, o primeiro tratado internacional a explorar o tema, cujo objetivo é o de promover a

cooperação internacional entre os países na elaboração de procedimentos para o combate aos cibercrimes. Sobre a cooperação internacional, Fiorillo e Conte (2016) pronunciam:

> Desse modo, para combater uma praga transfronteiriça como a nova criminalidade, é imperativo ter-se em conta as vias de uma cooperação internacional, já que é indiscutível que uma parte da delinquência informática migrou para a Internet, face a essa nova realidade global. (...) Portanto, a globalização trouxe consigo a necessidade de aprimoramento de mecanismos de combate à criminalidade de natureza transnacional e, consequentemente, de repensar a Ciência Criminal, bem como despertou uma consciência mundial para a necessidade de estabelecimento de mecanismos de justiça supranacional. (FIORILLO; CONTE, 2016, p. 59-60)

Além de abordar a cooperação internacional, a Convenção de Budapeste instituiu normativas de direito penal material e de direito penal processual. O foco principal dos artigos que versam sobre normas de direito penal material voltou-se à responsabilização de condutas criminosas, submetendo os Estados signatários a adotarem medidas legislativas e demais que fossem necessárias para tanto. Nesta seção, discorreu-se acerca de infrações contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos (título 1); infrações relacionadas com computadores (título 2); infrações relacionadas a pornografia infantil (título 3) e infrações relacionadas a violação do direito de autor e dos direitos conexos (título 4).

Com relação à seção voltada às normas de direito penal processual, o enfoque recaiu em aspectos de investigação criminal e de produção de provas eletrônicas. Dentre os procedimentos tratados, destaca-se a adoção de medidas legislativas e outras que se fizerem necessárias para habilitação das autoridades competentes a proceder com busca e apreensão de dados informáticos armazenados em servidores nacionais ou internacionais (art. 19) e a promoção de auxílio mútuo entre as partes relativamente a poderes de investigação como, por exemplo, acesso a dados informáticos (art. 31).

Apesar da Convenção de Budapeste ter sido elaborada em 2001, somente duas décadas depois, em 15 de dezembro de 2021, foi firmada a adesão do Brasil ao referido instrumento. Sobre a adesão tardia, manifesta-se Pugliesi e Luiz (2022):

> Em suma, embora com atraso, o Brasil dá um importante passo na estratégia de repressão a crimes cibernéticos com a adesão à Convenção de Budapeste. Agora, inaugura-se uma oportunidade ímpar para que o Estado brasileiro empreenda discussões inadiáveis sobre a otimização da legislação nas matérias correlatas, com o objetivo de elevar sua atuação nesse campo no cenário internacional (PUGLIESI; LUIZ, 2022, n.p)

Tendo em mente que o mundo virtual ultrapassa fronteiras geográficas, aderir à Convenção de Budapeste revela-se um progresso rumo à maturação da legislação interna, baseando-se em padrões internacionais. Somado a isto, o apoio internacional em sede de investigação criminal e produção de provas pode ser decisivo para a identificação, o processamento e a responsabilização dos cibercriminosos, motivo pelo qual espera-se que a adesão à Convenção de Budapeste implique em avanços positivos para o Direito Penal Informático.

6. CONCLUSÃO

A presente monografia visou realizar uma breve abordagem da legislação brasileira com enfoque na problemática dos crimes cibernéticos no país. Para tanto, foi feita uma revisão bibliográfica de doutrinas e artigos científicos os quais analisaram criticamente as principais normativas relacionadas ao assunto, propiciando que fossem encontrados pontos positivos e pontos a serem melhorados no ordenamento nacional com fins de possibilitar a repressão dos crimes cibernéticos de maneira mais efetiva.

Verificou-se que os avanços tecnológicos ocorridos ao longo dos anos, principalmente, a criação e a popularização da Internet foram responsáveis por transformar o mundo, tornando-se item indispensável na sociedade atual. Todavia, como visto, toda essa revolução foi acompanhada pelo desenvolvimento de um grande problema: a cibercriminalidade. Isso se deve ao fato que os dispositivos informáticos possibilitaram novas formas de se cometer crimes e novas condutas criminosas. A facilidade que se tem para acessar a Internet e impactar pessoas por meio dessa ferramenta é um dos fatores que favorecem a ocorrência dos crimes cibernéticos.

Além disso, conforme foi retratado ao longo desta pesquisa, podemos citar o anonimato do agente, a sensação de impunidade e a carência de conhecimento das vítimas no manuseio das informações a que são expostas no mundo virtual como outros fatores que, do mesmo modo, são responsáveis por proporcionar um ambiente oportuno para que os infratores entrem em ação.

Vimos ainda que o episódio da pandemia de COVID-19 experienciado no início da década também foi caracterizado por um número alarmante de tentativas de ataques cibernéticos no país, o que é suficiente para voltarmos nossa atenção às discussões relacionadas à temática. Nota-se que se trata de um assunto de relevância singular, ante aos

impactos negativos dos crimes virtuais às vítimas e à economia, e considerando que a legislação pátria ainda é muito recente.

Baseando-se nas perspectivas doutrinárias apresentadas, podemos concluir que as atuais leis promulgadas no Brasil são frutos de um reconhecimento da necessidade de haver normativas específicas para o tratamento dos crimes virtuais. No entanto, como já abordado, os textos normativos em vigor, do ponto de vista doutrinário, detém omissões considerando a diversidade de situações que não foram abarcadas pelos tipos penais estabelecidos, além de possuírem redações vagas e imprecisas as quais dão margem a múltiplas interpretações.

Ante o exposto, depreende-se que a sociedade evolui rapidamente e que o Direito, em especial, o Direito Penal, busca incessantemente se adaptar às demandas que vão surgindo, visando proteger os bens jurídicos mais relevantes, por meio da criação legislativa com fins de tipificar condutas e majorar as penas. Porém, conclui-se que somente essas medidas não são hábeis a reprimir as condutas delituosas isoladamente.

Desta forma, também é necessário a criação e execução de políticas criminais efetivas; a preparação adequada de profissionais para operarem na área; a disponibilização de recursos financeiros e tecnológicos; a cooperação internacional entre Estados na elaboração de mecanismos de combate e prevenção aos delitos cibernéticos; a colaboração entre os todos os atores sociais envolvidos como, no caso das provedoras de serviços de conexão que mantém dados úteis às investigações criminais e à produção probatória; o incentivo à educação dos internautas para que se precavenham de serem vítimas dos criminosos digitais, dentre outras providências possíveis.

À vista disso, podemos afirmar que a legislação brasileira é incipiente na tratativa dos crimes cibernéticos no país, possuindo muitas lacunas a serem preenchidas. Ademais, somente com a união entre a dedicação dos legisladores em criarem normativas mais precisas e atuação dos responsáveis em colocar em prática as diligências expostas no parágrafo anterior é que será possível potencializar a repressão de crimes cibernéticos e a conter os altos índices de ocorrências destas condutas criminosas.

REFERÊNCIAS

ADVOGADOS, Marinho. O que é Revenge Porn ou Pornografia de Vingança e porque você deve saber como combater este tipo de ato. Divulgação de fotos e vídeos íntimos de ex-parceiros, como forma de vingança quando o relacionamento termina. **Jus Brasil**. 2020. Disponível em: <https://advocaciamarinho.jusbrasil.com.br/artigos/831302225/o-que-e-revenge-porn-ou-pornografia-de-vinganca-e-porque-voce-deve-saber-como-combater-este-tipo-de-ato> Acesso em 03 fev. 2023

BARRETO, Alessandro Gonçalves Barreto. Análise da Lei Azeredo: necessidade de criação de delegacias e setores especializados na repressão aos crimes informáticos. Migalhas. 11 abr. 2018, ISSN 1983-392X. Disponível em: <https://www.conjur.com.br/2022-jan-10/opiniao-desafios-brasil-adesao-convencao-budapeste> Acesso em: 26 jan. 2023

BITENCOURT, Cezar Roberto. **Tratado de direito penal*:*** Parte geral - arts. 1 a 120, v. 1, 27. ed. São Paulo: Saraiva Educação, 2021.

BRASIL. **Decreto n° 8.771, de 11 de maio de 2016.** Regulamenta a Lei n° 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Brasília, DF: Diário Oficial da União, 11 mai. 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm> Acesso em: 15 jan. 2023

BRASIL. **Decreto-Lei n° 2.848, de 07 de dezembro de 1940.** Código Penal. Rio de Janeiro, RJ: Diário Oficial da União, 31 dez. 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm> Acesso em: 10 jan. 2023

BRASIL. **Decreto-Lei n° 3.689, de 3 de outubro de 1941.** Código de Processo Penal. Rio de Janeiro, RJ: Diário Oficial da União, 3 out. 1941. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm> Acesso em 26 jan. 2023

BRASIL. **Lei n° 3.914, de 09 de dezembro de 1941.** Lei de Introdução do Código Penal (decreto-lei n. 2.848, de 7-12-1940) e da Lei das Contravenções Penais (decreto-lei n. 3.688, de 3 de outubro de 1941). Rio de Janeiro, RJ: Diário Oficial da União, 9 dez. 1941. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del3914.htm> Acesso em: 10 jan. 2023

BRASIL. **Lei n° 11.829, de 25 de novembro de 2008.** Altera a Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal metarial e outras condutas relacionadas à pedofilia na internet. Brasília, DF: Diário Oficial da União, 25 nov. 2008. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm> . Acesso em: 13 jan. 2023

BRASIL. **Lei nº 12.735, de 30 de novembro de 2012.** Altera o Decreto-lei n° 2.848, de 7 de Dezembro de 1940 – Código Penal, o Decreto-lei n° 1.001, de 21 de Outubro de 1969 – Código Penal Militar, e a Lei n° 7.716, de 5 de Janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Brasília, DF: Diário Oficial da União, 30 nov. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm>. Acesso em: 11 jan. 2023

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** *Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-lei n° 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências.* Brasília, DF: Diário Oficial da União, 30 nov. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em: 11 jan. 2023

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Diário Oficial da União, 23 abr. 2014 . Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 10 jan. 2023

BRASIL. **Lei n° 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados (LGPD). Brasília, DF: Diário Oficial da União, 14 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em: 13 jan. 2023

BRASIL. **Lei n° 13.718, de 24 de setembro de 2018.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar os crimes de importunação sexual e de divulgação de cena de estupro, tornar pública incondicionada a natureza da ação penal dos crimes contra a liberdade sexual e dos crimes sexuais contra vulnerável, estabelecer causas de aumento de pena para esses crimes e definir como causas de aumento de pena o estupro coletivo e o estupro corretivo; e revoga dispositivo do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). Brasília, DF: Diário Oficial da União, 24 set. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13718.htm>. Acesso em: 13 jan. 2023

BRASIL. **Lei n° 13.853, de 8 de julho de 2019.** Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Diário Oficial da União, 19 dez. 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13718.htm>. Acesso em: 13 jan. 2023

BRASIL. **Lei n° 14.010, de 10 de junho de 2020**. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19). Brasília, DF: Senado Federal, 8 set. 2020. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm> Acesso em 17 jan. 2023

BRASIL. **Lei n° 14.155, de 27 de maio de 2021.** Altera o Decreto-Lei n° 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais grave os crimes de violação de de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-LEI n° 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Brasília, DF: Diário Oficial da União, 14 ago. 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm> Acesso em 17 jan. 2023

BRASIL. **Projeto de Lei nº 2126/2011.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Congresso Nacional, 25 abr. 2011, p. 1-11 . Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=912989&filename=PL%202126/2011> Acesso em: 11 jan. 2023

CAPEZ, Fernando. **Curso de direito penal:** Parte geral – arts. 1º a 120, vol. 1, 25ª ed. São Paulo: Saraiva Educação, 2021.

CARAMIGO, Dênis. Registro não autorizado da intimidade. **Canal Ciências Criminais.** 2019. Disponível em: <https://canalcienciascriminais.jusbrasil.com.br/artigos/739512376/registro-nao-autorizado-da-intimidade-sexual> Acesso em 23 jan. 2023

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A Trajetória da Internet no Brasil**: Do surgimento das redes de computadores à instituição dos mecanismos de governança. Dissertação (Mestrado em Ciência de Engenharia de Sistemas e Computação) - Universidade Federal do Rio de Janeiro, Rio de Janeiro: 2006.

CASTELLS, Manuel. **A Galáxia da Internet:** Reflexões sobre a Internet, os negócios e a sociedade. Tradução de Maria Luiza X. de A. Borges. Revisão de Paulo Vaz. Rio de Janeiro: Zahar, 2003.

CRESPO, Marcelo. As Leis n° 12,735/2012 e 12.737/2012 e os crimes digitais: acertos e equívocos legislativos. **Jusbrasil**. 2015. Disponível em: <https://canalcienciascriminais.jusbrasil.com.br/artigos/201526971/as-leis-n-12735-2012-e-12737-2012-e-os-crimes-digitais-acertos-e-equivocos-legislativos> Acesso em 8 fev. 2023

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

CRUZ, Fernando Silvério da; FRANCO, Sueli da Consolação Silva. Pedofilia na Internet: A Lei n.° 11.829, de 25 de novembro de 2008 e sua efetiva aplicabilidade. Uberaba: Revista Inova Ciência & Tecnologia, n. 1, ano 2, jan./abr., p.73-84, 2016, ISSN 2447-598X. Disponível em: <https://periodicos.iftm.edu.br/index.php/inova/article/view/93/59> Acesso em 22 jan. 2023

CONSELHO DA EUROPA. **Convenção sobre o Cibercrime.** (Convenção de Budapeste). Budapeste, 23 XI. 2021. Disponível em: <https://rm.coe.int/16802fa428> Acesso em 02 jan. 2023

CUNHA, Rogério Sanches da. **Breves comentários às Leis 13.769/18 (prisão domiciliar), 13.771/18 (feminicídio) e 13.772/18 (registro não autorizado de nudez ou ato sexual).** p. 1-7, 2018. Disponível em: <https://s3.meusitejuridico.com.br/2018/12/9c20f715-breves-comentarios-as-leis-13769-18-prisao-domiciliar-13771-18-feminicidio-e-13772-18.pdf.> Acesso em: 02 fev. 2023

DORIGON, Alessandro; SOARES, Renan Vinicius de Oliveira. Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade. Teresina: Revista Jus Navidandi. n. 5342, ano 23, 15 fev. 2018, ISSN 1518-4862. Disponível em: <https://jus.com.br/artigos/63549/crimes-ciberneticos-dificuldades-investigativas-na-obtencao-de-indicios-da-autoria-e-prova-da-materialidade/2> Acesso em 02 fev. 2023

DURKHEIM, Émile. **As regras do método sociológico**. Tradução de Paulo Neves. Revisão da tradução de Eduardo Brandão. 3ª ed. São Paulo: Martins Fontes, 2007.

ESTEFAM, André; GONÇALVES, Victor Eduardo Rios. **Direito Penal:** parte geral. 10ª ed. São Paulo: Saraiva Educação, 2021.

FILHO, Demócrito Reinaldo. O projeto de lei sobre crimes tecnológicos (PL n° 84/99): Notas ao parecer do Senador Marcello Crivella. Teresina: Revista Jus Navigandi, n. 375, ano, 17 jul. 2004, ISSN 1518-4862. Disponível em: <https://jus.com.br/artigos/5447/o-projeto-de-lei-sobre-crimes-tecnologicos-pl-n-84-99> Acesso em: 10 jan. 2023

FILHO, Eduardo Tomasevicius. **Marco Civil da Internet:** uma lei sem conteúdo normativo. Scielo, 2016, Estudos Avançados 30, 86, p. 269-285, DOI: 10.1590/S0103-40142016.001000017. Disponível em: <https://www.scielo.br/j/ea/a/n87YsBGnphdHHBSMpCK7zSN/?format=pdf&lang=pt> Acesso em 10 jan. 2023

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

GANEM, Pedro. O combate aos cybercrimes e a nova Lei n.º 14.155 de 2021. **Canal Ciências Criminais.** 11 ago. 2022 Disponível em: <https://canalcienciascriminais.com.br/o-combate-aos-cybercrimes-e-a-nova-lei-n-o-14-155-de-2021/> Acesso em 21 jan. 2023

GRECO, Rogério. **Curso de Direito Penal:** Parte Geral: arts. 1º a 120 do Código Penal, vol 1, 24ª ed. Barueri: Atlas, 2022.

JESUS, Damásio de Jesus. **Direito Penal:** Parte Geral, vol 1, 37ª ed. São Paulo: Saraiva Educação, 2020.

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

JORIO, Israel Domingos; BOLDT, Raphael. Comentários à Lei 14.155/2021. **Jusbrasil.** 2021. Disponível em:

<https://raphaelboldt.jusbrasil.com.br/artigos/1227518895/comentarios-a-lei-14155-2021> Acesso em 28 jan. 2023

KERR, Vera Kaiser Sanches. **A disciplina, pela legislação processual penal brasileira, da prova pericial relacionada ao crime informático praticado por meio da Internet.** Dissertação (Mestrado em Engenharia Elétrica) - Escola Politécnica da Universidade de São Paulo, São Paulo, 2011.

LINS, Bernardo Felipe Estellita. A evolução da Internet: uma perspectiva histórica. Brasília: Cadernos ASLEGIS, n. 48, p. 11-46, jan./abr. 2013. Disponível em: <http://www.belins.eng.br/ac01/papers/aslegis48_art01_hist_internet.pdf> Acesso em 05 nov. 2022

NASCIMENTO, Samir de Paula. Cibercrime: Conceitos, modalidades e aspectos jurídicos-penais. **Âmbito Jurídico**. 03 set. 2019. Disponível em: <https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais/> Acesso em: 02 fev. 2023

NÉRIS, Natália. Conquistas e desafios na proteção da intimidade na Internet. **Interlab.** 10 abr. 2019, Desigualdades e Identidades. Disponível em: <https://internetlab.org.br/pt/especial/conquistas-e-desafios-na-protecao-da-intimidade-na-internet/> Acesso em: 24 jan. 2023

NUCCI, Guilherme de Souza. **Manual de Direito Penal**. 18ª ed. Rio de Janeiro: Forense, 2022.

PUGLIESE, Yuri Sashione; LUIZ, José Henrique Ballini. Os desafios da adesão à Convenção de Budapeste sobre o Crime Cibernético. Revista Consultor Jurídico, 10 jan. 2022, ISSN 1809-2829. Disponível em: <https://www.conjur.com.br/2022-jan-10/opiniao-desafios-brasil-adesao-convencao-budapeste> Acesso em: 23 jan. 2023

REINA, Eduardo. Lei Carolina Dieckmann completa 10 anos com necessidade de complementações. Revista Consultor Jurídico, 27 dez. 2022, . ISSN 1809-2829. Disponível em: <https://www.conjur.com.br/2022-jan-10/opiniao-desafios-brasil-adesao-convencao-budapeste> Acesso em: 22 jan. 2023

SAMPEI, Kamila Kayumi. Lei Carolina Dieckmann - A vida prática e a ineficácia da aplicação da pena. Lei 12.737 de 30 de novembro de 2012 - Insuficiência da pena ao punir o agente e a possível reparação à luz do Direito Civil. **Jusbrasil.** 2015. Disponível em: <https://kamilasampei.jusbrasil.com.br/artigos/189641302/lei-carolina-dieckmann-a-vida-pratica-e-a-ineficacia-da-aplicacao-da-pena#:~:text=Em%20suma%2C%20a%20lei%20trouxe,ou%20destruir%20dados%20ou%20informa%C3%A7%C3%B5es.> Acesso em 25 jan. 2023

SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas**. 2. ed. São Paulo: Saraiva, 2015.

VENOSA, Sílvio de Salvo. **Introdução ao estudo do direito**. 7ª ed. Barueri (SP): Atlas, 2022.

VIANNA, TÚLIO LIMA. **Do acesso não autorizado a sistemas computacionais:** fundamentos de Direito Penal Informático. Dissertação (Mestrado em Direito) - Universidade Federal do Minas Gerais, Belo Horizonte: 2001.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos:** Ameaças e procedimentos de investigação. 2ª ed. Rio de Janeiro: Brasport Livros e Multimídia Ltda, 2013.

ZAFFARONI, Eugenio Raúl; PIERANGELI, José Henrique. **Manual de Direito Penal Brasileiro.** São Paulo: Revista dos Tribunais, 1998.