Crimes digitais e a discussão sobre (in) adequação dos tipos penais

Gabriel Alves de Oliveira, Centro Universitário Integrado, Brasil, Gabrielalvesol@outlook.com

Luisa Araújo Sartori Pereira, Centro Universitário Integrado, Brasil, E-mail: luisa.aspereira@hotmail.com

Caroline Bittencourt da Silveira, Centro Universitário Integrado, Brasil, caroline.silveira@grupointegrado.br

RESUMO: Este estudo tem como objetivo realizar uma discussão sobre (in) adequação dos tipos penais nos crimes digitais. Utilizando uma abordagem metodológica qualitativa, de natureza dedutiva, foram examinados livros, artigos e jurisprudências relevantes sobre o tema. As conclusões indicam que, embora existam leis relacionadas aos crimes cibernéticos, a aplicabilidade do tipo penal é divergente em diversos delitos, pois enquanto o legislador, por muitas vezes, se socorre às leis para tentar dar uma resposta à sociedade, esta paga um enorme preço, seja pela morosidade com que as atitudes são tomadas, seja porque as leis editadas não acabam resultando em efetiva proteção aos bens jurídicos e aplicabilidade diversa do tipo penal, pois nos crimes cibernéticos desse estudo, aplicar o tipo penal adequado é um grande desafio, já que a inclusão dos crimes praticados na internet foi posterior à criação do tipo penal. Assim, adequar para melhor aplicação acaba por tornar a tipicidade aplicada de maneira inadequada em crimes cibernéticos, por não haver um tipo específico para determinada conduta.

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

ABSTRACT: The aim of this study is to discuss the (in)adequacy of criminal types in digital crimes. Using a qualitative, deductive methodological approach, relevant books, articles and case law on the subject were examined. The conclusions indicate that, although there are laws related to cybercrime, the applicability of the criminal type is divergent in various offenses, because while the legislator often uses laws to try to give society an answer, society pays a huge price, either because of the slowness with which action is taken, or because the laws enacted do not end up resulting in effective protection of legal assets and different applicability of the criminal type, because in the cybercrimes of this study, applying the appropriate criminal type is a major challenge, since the inclusion of crimes practiced on the internet was after the creation of the criminal type. Thus, adapting for better application ends up making the typicity inadequately applied in cybercrime, because there is no specific type for a given conduct.

Keywords: Criminal Law. Cybercrimes. Criminal Typicality.

INTRODUÇÃO

Segundo o Instituto Brasileiro de Geografia e Estatística (2023), 90% dos domicílios brasileiros possuem internet, constatando assim que a cada dez residências, 9 navegam pelo ciberespaço, seja por acesso por meio de computadores ou por meio de celulares ou tablets. Nessa vertente, houve um elevado crescimento de crimes que são praticados por meio do uso da tecnologia, de forma específica, a internet. Segundo uma pesquisa realizada pela Norton Cyber Security (2023),

aproximadamente 71 milhões de brasileiros foram vítimas de algum tipo de crime cibernético nos últimos 12 meses.

A internet é uma importante ferramenta de interação social, trabalho e estudo, tudo tem relação direta com a internet, tornando difícil a dissociação entre o mundo real e o virtual. Até mesmo conflitos que antes eram gerados somente por meio físico, atualmente são gerados no meio social, seja por publicações, troca de mensagens, redes sociais diversas, resultado esse do alcance a nível mundial que as informações alcançam (PINHEIRO, 2009).

Nesse contexto, tem crescido o número de estudos sobre a utilização da internet relacionados à prática de diversos crimes que ocorrem no ambiente virtual, de diversas naturezas. Deste modo, com a utilização de redes sociais, ampliou-se a liberdade de expressão dos indivíduos, assim como o posicionamento das pessoas sobre vários temas, surgindo diversos conflitos, resultado da exposição dessas opiniões, e ainda se tornou um local de cometimento de vários tipos penais. Para isso, o judiciário, diante dessa demanda, também precisou aplicar de forma efetiva a legislação para combater esses crimes (CASTRO, 2003).

Dessa forma, a problemática que se busca responder com esse estudo é: os tipos penais possuem aplicabilidade adequada para punir os crimes digitais? Para tanto, esse estudo objetiva realizar uma discussão sobre (in) adequação dos tipos penais nos crimes digitais.

MÉTODO

Para o desenvolvimento do estudo, faz-se mister abordar o problema central: sobre os crimes digitais e a discussão sobre (in) adequação dos tipos penais, visando elucidar o tema proposto, utilizar-se-á da pesquisa qualitativa, bem como da pesquisa bibliográfica, consultando artigos de periódicos, dissertações de mestrado, teses de doutorado, recursos disponíveis na Internet e outros materiais relacionados a diversas áreas de conhecimento, para se formar o entendimento teórico a despeito das (in) aplicabilidades da lei penal no âmbito digital.

O método dedutivo foi utilizado, pois foi possível partir da premissa geral sobre os crimes digitais e obter ao término do estudo conclusões particulares, ou seja, há presença de leis para combate aos crimes digitais, mas existe uma falha em relação a aplicabilidade do tipo penal, constatando em vários casos concretos a falta de um tipo penal adequado para melhor punição do delito praticado.

RESULTADOS E DISCUSSÕES

1 DIREITO PENAL E SUA APLICABILIDADE

O Direito Penal é ramo do direito público e possui várias funções, tais como a função de garantia, destinada a salvaguardar a sociedade de arbitrariedades governamentais, a função de controle social, que o usa para manter a ordem pública, e a proteção dos bens jurídicos, que é como a principal (Prado, 2003).

Assim, surge na doutrina contemporânea o conceito de "Funcionalismo", cujo objetivo principal é examinar a verdadeira função do direito penal. Duas tendências funcionalistas se sobressaem nestes estudos: o funcionalismo moderado, também conhecido como teleológico, e o funcionalismo radical (Coelho, 2003).

Já o funcionalismo radical, liderado por Günther Jakobs, sustenta que a finalidade do direito penal é a salvaguarda da norma em si. Sofre diversas críticas, principalmente porque é daí que surge o Direito Penal do Inimigo, teoria frequentemente rejeitada no Brasil.

Do outro lado, desenvolvido por Claus Roxin, o funcionalismo moderado acredita que a função do direito penal: “é assegurar bens jurídicos, assim considerados aqueles valores indispensáveis à convivência harmônica em sociedade, valendo-se de medidas de política criminal” (Cunha, 2015, p. 34).

Carneiro (2020, p. 01) complementa ainda que:

> O estabelecimento do Direito Penal como ramificação de utilização subsidiária da estrutura jurídica não é por menor justificada inadequadamente, caso haja em sua esfera argumentativa o fato de ser este o modo mais colérico no que tange a essência do ser humano quanto a sua dignidade e liberdade, visto que, o Direito Penal é a modalidade mais agressiva de reprovação de condutas, correção comportamental e, por conseguinte, sistematização das penas cominadas.

No entendimento de Claus Roxin, o funcionalismo moderado acredita que a função do direito penal “é assegurar bens jurídicos, assim considerados aqueles valores indispensáveis à convivência harmônica em sociedade, valendo-se de medidas de política criminal” (Cunha, 2015, p. 34).

Os bens jurídicos podem ser definidos como: “valores ético-sociais selecionados pelo direito com o objetivo de assegurar a paz social, e colocados sob sua proteção para que não sejam expostos a perigo de ataque ou a lesões efetivas” (Toledo, 2002, p. 16).

Portanto, é possível entender a extensão do âmbito do direito penal e sua responsabilidade na proteção dos bens jurídicos protegidos, além de sua função secundária, intervindo apenas como última opção nas dinâmicas sociais. Outros campos jurídicos disponíveis podem resolver controvérsias, deixando o direito penal apenas para situações onde não há outra opção jurídica apropriada disponível.

1.1 TIPO PENAL

São todos os elementos que se enquadram um delito, e cada tipo de delito possui um tipo penal, ou seja, cada tipo tem as suas características e elementos próprios que os distinguem uns dos outros. É classificado por Busato (2013) como a descrição de um fato ilícito, que violou uma lei penal, e que se enquadra em um fato típico, antijurídico e culpável, e seu estudo é denominado tipologia criminal. É o que

classifica o tipo de crime cometido, para cada delito há um tipo penal especifico e descrito.

A função precípua é a descrição de modo objetivo um comportamento proibido pelo Direito Penal, limitando e individualizando as condutas relevantes. Todos os elementos que compõem a descrição de um comportamento abstrato proibido pelo Direito Penal formam o tipo. Já a tipicidade resulta da análise de uma conduta realizada no plano concreto e de seu posterior enquadramento na previsão abstrata de um comportamento descrito no tipo (Toledo, 2002).

> A função pode ser ainda sistemática, dogmática e político-criminal. A função sistemática traduz o compêndio de elementos que permitem a identificação de qual tipo se trata, na função político-criminal, também denominada função de garantia, está associada ao princípio de legalidade, recortando o âmbito da incriminação somente para aquilo que define o tipo; já na função regulatória dos limites do erro relevante para a imputação e uma função dogmática, consistente na descrição dos elementos sobre os quais deve incidir o dolo (Busato, 2013, p. 308).

Os componentes do tipo são impessoais, pois não dependem da vontade do agente. Por outro lado, os elementos subjetivos se referem à vontade e à intenção do indivíduo, sendo o dolo e a culpa componentes subjetivos do tipo. Uma ação pode ser vista como criminosa se estiver em conformidade com a tipicidade e a antijuridicidade. O elemento subjetivo especial do tipo está presente em certos tipos objetivos, determinando ou fundamentando a ilicitude do ato. É visto como um componente subjetivo do tipo objetivo, independentemente do dolo (Cunha, 2015).

Portanto, a tipologia criminal é fundamental para a aplicação do Direito Penal, pois cada delito possui suas características específicas que o definem, sendo necessário que cada elemento seja analisado para que haja a efetiva aplicação da Lei, de forma que os princípios penais sejam respeitados, trazer segurança jurídica à sociedade.

1.2 PROTEÇÃO DOS BENS JURÍDICOS

O direito penal, segundo o princípio da intervenção mínima, é o direito de “ultima ratio”. Nesse sentido, compreende-se os motivos pelos quais o Direito Penal pode intervir prioritariamente como garantidor da proteção dos bens jurídicos, contudo, quando nenhuma outra área do Direito oferece solução adequada, desse modo, aplicando-se apenas como último recurso. (Prado, 2003). Para tanto, no ordenamento jurídico-penal somente pode:

> [...] se legitimar materialmente se estiver consoante tais princípios. Princípios estes de raízes constitucionais, expressa ou tácita, mas de obrigatória observância para o modelo constitucional adotado pelo país, qual seja o modelo de Estado Democrático de Direito. Tais princípios servem ao mesmo tempo de limite à intervenção estatal no

> âmbito do Direito Penal e de legitimação de tal intervenção (Serretti, 2009, p. 01).

Ocorre que, sua atuação é limitada pela intervenção mínima e fragmentariedade: intervém para proteger bens jurídicos, mas quando os demais ramos do direito falharam (intervenção mínima); e para criminalizar somente as condutas mais graves, que atentam contra bens jurídicos penalmente relevantes (fragmentariedade) (Prado, 2003).

Sobre esse aspecto, Luiz Régis Prado (2011, p. 148) afirma que a: "*ultima ratio* é um princípio informador do Direito Penal dotado de grande carga ética, filosófica e jurídico-político, apresenta-se como verdadeira ciência dos delitos e das penas".

Conforme Lopes (2006), a violação de um bem jurídico gera para o prejudicado o direito a ser ressarcido ou, no âmbito penal, para a vítima e/ou o Estado o direito/obrigação de ver uma penalidade aplicada, que pode assumir várias formas (privação de liberdade, restrição de direitos ou penalidade pecuniária).

Não apenas isso, é necessário que exista uma previsão legal que seja anterior ao ato delituoso. Afinal, ninguém pode ser penalizado por um ato que, no momento em que foi realizado, não estava tipificado como crime na lei.

Deste modo, conclui-se que o Direito Penal age de acordo com o princípio da intervenção mínima, que restringe sua atuação apenas aos casos em que há condutas graves e outros ramos do Direito não são suficientes para coibir o ato, além disso, atua com o princípio da legalidade, punindo apenas as condutas que já estavam previstas em Lei.

2 CRIMES CIBERNÉTICOS

A internet é uma importante ferramenta de interação social, trabalho e estudo, assim torna-se difícil a dissociação entre o mundo real e o virtual. Até mesmo conflitos que antes eram gerados somente por meio físico, atualmente são gerados no meio social, seja por publicações, troca de mensagens, redes sociais diversas, resultado esse do alcance a nível mundial que as informações alcançam (Corrêa, 2010).

Nesse contexto, tem crescido o número de estudo sobre a utilização da internet relacionado à liberdade de expressão e aos diversos discursos de ódio que tem acontecido com o advento da tecnologia, sendo um fato que muitos desses discursos se constituem crime. Dessa forma, com a utilização das redes sociais, ampliou-se a liberdade de expressão dos indivíduos, assim como o posicionamento das pessoas sobre vários temas, surgindo assim diversos conflitos, resultado da exposição dessas opiniões (Ramos et al., 2011).

Notavelmente a internet apresenta inúmeras vantagens e benefícios para as pessoas, vez que reduziu as distâncias entre as mesmas, possibilitando a realização de relações sociais e comerciais entre as pessoas e nações que estão conectadas a rede, o que, de fato, possibilitou um imenso crescimento econômico dos países que estão conectados à internet (Nascimento, 2016).

O posicionamento dos Tribunais acerca da matéria tem sido:

> **APELAÇÃO CRIMINAL - CONDENAÇÃO PELOS DELITOS TIPIFICADOS NOS ARTS. 241-A, CAPUT, E 241-B, CAPUT, DO ESTATUTO DA CRIANÇA E DO ADOLESCENTE - PRELIMINARES - ARGUIÇÃO DE NULIDADE DA BUSCA E APREENSÃO E DAS PROVAS OBTIDAS POR TER SIDO DECRETADA POR JUÍZO INCOMPETENTE** - REJEIÇÃO – INVESTIGAÇÃO INICIAL DESTINADA A APURAR CRIMES CIBERNÉTICOS ENVOLVENDO PORNOGRAFIA INFANTO-JUVENIL NA REDE MUNDIAL DE COMPUTADORES, CUJA COMPETÊNCIA PARA PROCESSAMENTO É DA JUSTIÇA FEDERAL NOS TERMOS DO RECURSO EXTRAORDINÁRIO Nº 628.624 DO SUPREMO TRIBUNAL FEDERAL, COM REPERCUSSÃO GERAL - APENAS POSTERIORMENTE QUE SE AVERIGUOU QUE O CRIME IMPUTADO AO ACUSADO ENVOLVIA A TROCA DE E-MAILS ENTRE INDIVÍDUOS NACIONAIS, AFASTANDO A TRANSNACIONALIDADE DO DELITO - CIRCUNSTÂNCIA POSTERIOR QUE NÃO MACULA A BUSCA E APREENSÃO, EIS QUE NO MOMENTO DECRETADA O JUÍZO ERA COMPETENTE E OS ATOS FORAM POSTERIORMENTE RATIFICADOS - ARGUIÇÃO DE NULIDADE DO PROCESSO POR NÃO TER SIDO DISPONIBILIZADO ACESSO INTEGRAL À DEFESA DO INQUÉRITO POLICIAL - EXCEPCIONALIDADE DA SITUAÇÃO EM APREÇO QUE POSSIBILITA O ACESSO APENAS ÀS PROVAS QUE INTERESSEM AO ACUSADO - INVESTIGAÇÃO SIGILOSA, COM DILIGÊNCIAS AINDA EM ANDAMENTO, ENVOLVENDO INÚMEROS INVESTIGADOS EM TODO O TERRITÓRIO BRASILEIRO, **ARQUIVOS DE IMAGEM E 91 (NOVENTA E UM) ARQUIVOS DE VÍDEO COM CONTEÚDO COM CARACTERÍSTICAS DE PORNOGRAFIA INFANTOJUVENIL OU IMAGENS DE NUDEZ NO HD PERTENCENTE AO APELANTE - MANUTENÇÃO DA CONDENAÇÃO COMO MEDIDA QUE SE IMPÕE - COMO CONSEQUÊNCIA, INCABÍVEL A FIXAÇÃO DO REGIME ABERTO OU ENCAMINHAMENTO DOS AUTOS A OFERECIMENTO DE PROPOSTA DE SUSPENSÃO CONDICIONAL DO PROCESSO -** RECURSO CONHECIDO E DESPROVIDO. (TJPR, 2021).

As redes sociais são importantes ferramentas de contato interpessoal, democratização da informação, troca de informações e também de venda de produtos e serviços, estes que se utilizam das mídias para atrair novos clientes (Johnson,2013).

Nota-se que as redes estão cada vez mais abrangentes e grandiosas, muitas empresas nunca obtiveram contato pessoal com seus clientes ou viram seus consumidores pessoalmente, somente se comunicam por meio de mensagens e os dados que possuem destas pessoas são informações disponibilizadas por elas nas redes, dependendo do serviço prestado (Ramos et. al, 2011).

Verifica-se que o ambiente virtual é fundamental para as relações sociais e comerciais, porém tem sido também um ambiente para cometimento de inúmeros crimes e assim foi necessário a criação de leis para responsabilizar os autores de crimes cometidos no ambiente virtual, pois não havia previsão na lei.

3 SIMBOLISMO E OS CRIMES DIGITAIS

Conforme exposto no tópico anterior, foi necessário a criação de leis para combater os crimes digitais, no entanto nem todos os delitos cometidos no ambiente virtual apresentam a tipicidade adequada.

Não são poucos os exemplos existentes na legislação brasileira de falta de tipificação. O mais famoso provavelmente seja o delito contido na lei nº 7.643, de 18 de dezembro de 1987 que proíbe a pesca e o molestamento de cetáceo, *in verbis:*

> Art. 1º Fica proibida a pesca, ou qualquer forma de molestamento intencional, de toda espécie de cetáceo nas aguas jurisdicionais brasileiras. Art. 2º A infração ao disposto nesta lei será punida com pena de 2 (dois) a 5 (cinco) anos de reclusão e multa de 50 (cinquenta) a 100 (cem) Obrigações do Tesouro Nacional – OTN, com perda da embarcação em favor da União, em caso de reincidência.

A presente lei surgiu num período em que havia grande comoção social em torno da preservação das baleias, ameaçadas de extinção. Especificamente acerca do molestamento intencional de cetáceo, Maíra Zapater relata a forma curiosa como foi introduzida:

> Reza a lenda (assim me refiro ao episódio por já tê-lo ouvido de mais de um professor de Direito Penal, de gerações diferentes, sem contudo jamais ter conseguido localizar uma fonte escrita que confirmasse a história oral) que na ocasião uma baleia teria encalhado nas areias de uma praia famosa do Rio de Janeiro (Leblon? Ipanema? Copacabana? A localização exata varia ao gosto de quem conta o conto) e, enquanto ativistas tentavam devolver o animal às águas, um garotinho teria introduzido um palito de picolé no espiráculo (uma salva de palmas para o Google, que nos dá o nome certo para aquele orifício por onde os cetáceos respiram), causando, a um só tempo, a morte da baleia e uma grande comoção em torno do caso. O ocorrido teria inspirado o deputado a incluir o “molestamento intencional de cetáceo” na redação do tipo penal.

Seja ou não verídico tal episódio, questiona-se: Com que frequência tal conduta ocorre no país e qual a probabilidade de ocorrer novamente? Ainda que o Brasil seja cercado por um oceano e que, de fato, animais possam encalhar nas areias nacionais, qual a aplicabilidade prática de tal lei?

Se analisarmos sob o enfoque da Criminologia (ciência empírica e interdisciplinar que tem por objetos de estudo o crime, o criminoso, a vítima e o controle social), mais precisamente da visão de Shecaira (2020), são necessários alguns critérios para que um fato possa, efetivamente, ser considerado como crime no meio

social, são eles: incidência massiva na população; incidência aflitiva; persistência-espaço temporal; e consenso sobre a sua etiologia e técnicas de intervenção.

A incidência massiva, ou seja, para ser considerado crime, não deve tratar-se de um fato isolado, mas sim que ocorra com alguma frequência (ou ao menos haja possibilidade concreta de tal ocorrência). A incidência aflitiva consiste em conduta que cause alguma dor na vítima, ou seja, condutas que não tenham relevância social não podem ser consideradas crimes. O terceiro critério, persistência espaço-temporal, estipula que para ser considerado crime, o fato deve ser distribuído pelo território nacional, e por um período de tempo. Por fim, o quarto elemento seria o consenso sobre a etiologia do crime e as técnicas para sua intervenção, ou seja, para ser considerado crime, a conduta deve ser repudiada por grande parte da população (Cunha, 2020).

Assim sendo, analisando os critérios apontados por Shecaira (2020), questiona-se se a elaboração do tipo penal acima aludido preenche os requisitos para ser considerado, sob o prisma criminológico, como crime. Sabe-se que o fato que ensejou a elaboração da lei ocorreu tão somente uma vez, não havendo, portando, persistência espaço-temporal. Pode-se considerar que preencheria o requisito de incidência aflitiva, visto que pode causar a morte de animais, atingindo assim o meio ambiente, bem como pode-se considerar que a preservação ambiental e proteção dos animais seria de interesse coletivo. Contudo, nitidamente, tal conduta não preenche o primeiro critério apontado, qual seja, a incidência massiva na população. Ora, tratou-se de um fato isolado do qual o legislador se apropriou para demonstrar uma aparente preocupação. Shecaira (2020, p. 65) aponta as críticas, inclusive citando o mesmo exemplo do crime acima:

> Nem se pretende fazer a crítica do verbo utilizado para descrever a conduta praticada por aquele agente, mas tão somente destacar a impropriedade de, por ocorrência única no País, promover aquele fato à condição de crime.

Portanto, em que pese os conceitos de crime para a Criminologia e para o Direito Penal sejam distintos, deve-se considerar que ambas ciências caminham em um mesmo sentido. Desta feita, é nítido que a conduta acima apresentada não tem aplicabilidade prática, tratando-se tão somente de uma norma editada com o fim de acalmar os anseios sociais e transmitir uma falsa sensação de segurança pública.

No dizeres de Cunha (2020, p. 40):

> Esquecendo a real missão do direito Penal, o legislador atua pensando (quase que apenas) na opinião pública, querendo, com novos tipos penais e/ou, aumento de penas e restrições de garantias, devolver para a sociedade a (ilusória) sensação de tranquilidade. Permite a edição de leis que cumprem função meramente representativa, afastando-se das finalidades legítimas da pena.

Embora o exemplo supracitado seja antigo, atualmente o Brasil se depara com normas editadas sob o crivo do Direito Penal Simbólico. Em 2018, houve um clássico

erro legislativo, na tentativa de promover um Direito Penal Simbólico o que acabou resultando em impunidade.

Foi editada a Lei 13.654/2018 que alterou os crimes de furto e roubo (art. 155 e 157, respectivamente, ambos do Código Penal). Contudo, na alteração, o legislador acabou suprimindo a majorante para o delito de roubo praticado com emprego de arma branca. Inicialmente, o delito de Roubo previa, no §2º, I, o acréscimo de 1/3 (um terço) até metade para o delito, se praticado com emprego de arma, sem especificar qual o tipo. Com a edição da lei 13.654/2018, na tentativa de aumentar a pena para o delito, se praticado com emprego de arma de fogo, foi acrescido ao delito do Art. 157 o §2º-A, I, prevendo um acréscimo de 2/3 (dois terços) na pena. No entanto, tal dispositivo não mencionou o emprego de arma branca e, não obstante, a referida lei revogou o inciso I do §2º, causando uma *novatio legis in mellius*, ou seja, além de impedir o acréscimo de pena dos delitos de roubo praticado com emprego de arma branca, a partir da vigência da referida lei, tal medida ainda beneficiou as condutas praticadas anteriormente, visto a exceção contida no princípio da irretroatividade, ou seja, aplicação retroativa da lei que beneficia o réu, ainda que trate-se de decisão transitada em julgado (Assunção, 2021).

Assim, na tentativa de simbolizar uma proteção maior aos bens jurídicos e transmitir uma sensação de segurança à população, o legislador acabou por causar maior impunidade, diminuindo a proteção dos bens jurídicos (Da Silva, 2015).

Para sanar tal irregularidade, a Lei 13.964/2019, popularmente conhecida por Pacote Anticrime, acrescentou o inciso VII ao §2º do Art. 157, prevendo novamente o acréscimo de 1/3 à metade da pena em caso de emprego de arma branca. Salienta-se, contudo, que as condutas praticadas antes da vigência desta referida lei, não são passíveis de acréscimo.

Embora os exemplos citados sejam de fácil percepção, a legislação brasileira é recheada de demonstrações de Direito Penal Simbólico que exigem um conhecimento um pouco mais aprofundado. Como exemplo podemos citar o artigo 492, I, do Código de Processo Penal, o qual prevê que, nos procedimentos de competência do Júri, em caso de condenação a pena superior a 15 anos, o presidente (juiz togado) determinará a execução provisória da pena (Assunção, 2021).

Ocorre que no julgamento das ADCs 43, 44 e 54, o STF decidiu ser inconstitucional a execução provisória da pena. Assim, para seu cumprimento, mister se faz o trânsito em julgado da sentença penal condenatória.

Em que pese os questionamentos acerca dos verdadeiros motivos de tais decisões e, ainda que as decisões tomadas pelo STF não vinculem a atividade típica do Poder Legislativo, é nítido que o artigo 492, I, do CPP afronta a referida decisão, que é vigente, e, por conseguinte, ofende a Constituição Federal (Da Silva, 2015).

Assim sendo, ainda que editada com a melhor das intenções, a legislação demonstra-se tão somente simbólica, pois está em vias de ser declarada inconstitucional, denotando o mal emprego da verba pública, levando em consideração que o tempo dos congressistas fora desperdiçado com a edição da presente lei (Assunção, 2021).

O caso de demonstração de Direito Penal Simbólico ocorreu em 2021, com a edição da lei 14.245, de 22 de novembro de 2021, popularmente conhecida como Lei Mari Ferrer.

Mariana Ferrer é uma influenciadora digital que alegou ter sido vítima de estupro, ocasião em que o acusado foi absolvido em primeira e segunda instância. O caso gerou grande repercussão nacional, devido às diversas *Fake News* espalhadas acerca do suposto argumento utilizado para absolvição. Outro ponto que repercutiu muito acerca do caso foi a forma completamente desrespeitosa com que o advogado de defesa agiu para com a vítima, expondo-a de forma vexatória (Assunção, 2021).

Diante disso, fora editada então a lei supracitada, que visa coibir a prática de atos atentatórios à dignidade da vítima e de testemunhas durante o processo, causando alterações no Código de Processo Penal, no Código Penal e na Lei de Juizados Especiais (Lei 9.099/95).

Após a edição da referida lei, durante a audiência de instrução de julgamento, ou durante a instrução em plenário, veda-se a manifestação sobre circunstâncias ou elementos alheios aos fatos objetos de apuração nos autos, bem como a utilização de linguagem, de informações ou de material que ofendam a dignidade da vítima ou de testemunhas (Da Silva, 2015).

Analisando a primeira vedação, nota-se que nada mudou em relação a forma como o processo era conduzido antes da edição da lei. Ora, o juiz sempre tivera o poder-dever de obstar as manifestações que fossem estranhas ao processo.

Quanto a segunda vedação, esbarra num problema um pouco mais complexo. É evidente que o advogado deve agir com o máximo respeito possível para com todos os sujeitos do processo. Contudo, em se tratando de um processo por crime contra a dignidade sexual, que por sua essência, na maioria das vezes, é praticado em local isolado e longe de qualquer testemunha ou outra prova, a palavra da vítima encontra-se como único elemento para se estabelecer o nexo causal. Desta forma, como poderia o advogado de defesa questionar a vítima acerca dos fatos, que são sempre constrangedores e remetem a vítima ao trauma sofrido, sem que isso lhe ofenda a dignidade? E como poderia restar provado se o fato é verídico ou se é uma falsa acusação, sem que seja inquirida aquela pessoa que, em muitos casos, é a única que presenciou o fato?

O Art. 7ª da Lei 8906/94, Estatuto da OAB, prevê que o advogado tem o direito de exercer com liberdade a profissão em todo o território nacional, bem como prevê a imunidade profissional, não consistindo injuria ou difamação as manifestações irrogadas em juízo. Assim sendo, questiona-se se a lei Mari Ferrer, ao estabelecer tais vedações, não acabaria por dificultar a atuação do advogado e, consequentemente estaria cerceando o direito de defesa do réu (Brasil, 1994).

Portanto, mostra-se com os exemplos acima aludidos a manifestação do Direito Penal Simbólico que, na prática, pouco – ou nada – contribuem para a redução da criminalidade e proteção dos bens jurídicos, embora na teoria sejam apresentados como a grande solução dos problemas globais. Nota-se também que em alguns casos, a manifestação do Direito Penal Simbólico não apenas não contribui para a redução

da criminalidade, como acaba tornando os bens jurídicos ainda mais desprotegidos (Da Silva, 2015).

Não obstante, em vários momentos, percebe-se que a edição de leis sob a finalidade simbolismo jurídico, não só causa um inflacionamento na legislação nacional, como ofende diversos princípios penais. É o caso, por exemplo, da primeira lei citada, que tipifica a conduta de molestar cetáceo. Evidentemente tal ato poderia ser abrangido por outra área do direito, vide a administrativa, caracterizando, portanto, violação ao princípio da fragmentariedade, que assevera que o Direito Penal deve se preocupar tão somente com os bens jurídicos tidos por mais importantes. Também ofende o princípio da intervenção mínima, pelo qual o Direito Penal somente deve intervir na coletividade quando outros ramos do direito se demonstrarem insuficientes Shecaira (2020).

A manifestação do Direito Penal Simbólico, portanto, além de não causar uma efetiva proteção aos bens jurídicos, ainda dão azo para uma desproteção dos bens jurídicos. Além dos casos em que diretamente acaba por prejudicar a proteção, indiretamente também podem causar este efeito. Ao contrariar princípios penais que, em sua maioria, são constitucionais, as leis editadas com simbolismo vivem em constantes questionamentos acerca de suas constitucionalidades. Não obstante, o legislador parece ainda não ter compreendido que o encarceramento, por si só, não é um meio eficaz de combater a criminalidade. Ocorre que o poder judiciário parece já ter compreendido isto e, paulatinamente, vem buscando interpretações que acarretem em menor restrição de liberdade (Cunha, 2020).

4 INADEQUAÇÃO DOS TIPOS PENAIS EM RELAÇÃO AOS CRIMES DIGITAIS

As discussões e os debates acerca dos crimes cibernéticos vêm aumentando, uma vez que o tema é relevante, de extrema complexidade e muito corriqueiro atualmente, sendo possível notar que os tipos penais atuais não se adequam às especificidades dos crimes cometidos no ambiente digital (Da Silva, 2015).

O primeiro ponto dessa inadequação é em relação aos novos crimes que vão surgindo na internet, devido a evolução rápida da tecnologia, o que faz com que as legislações não sejam capazes de acompanhar essas novidades, dificultando a tipificação de crimes que não estavam previstos no momento da criação das leis (Galli, 2017).

Outro ponto é em relação à natureza dos crimes. Grande parte dos delitos acontece por intermédio da invasão de dispositivos e fraudes online, não se enquadrando adequadamente no tipo penal dos delitos comuns, que possuem contexto direto e físico. Dessa forma, a virtualidade e a globalização tornam complexa a aplicação dos tipos penais existentes (Da Silva, 2015).

Diante das novas práticas criminosas, os tribunais tem se manifestado sobre hackeamento de contas do Instagram, em que as vítimas impulsionam o judiciário para buscar indenização de valores e prejuízos causados por esse tipo de crime. Vejamos:

> RECURSO INOMINADO. REDE SOCIAL (INSTAGRAM). **CONTA HACKEADA. FALHA NO SISTEMA DE SEGURANÇA DIGITAL.** DANOS MORAIS CONFIGURADOS NO CASO CONCRETO EM RELAÇÃO AO AUTOR QUE TEVE A CONTA INVADIDA. **EXCLUDENTE DE RESPONSABILIDADE DE CULPA EXCLUSIVA DA CONSUMIDORA E DE TERCEIROS APLICÁVEL EM RELAÇÃO À CO-AUTORA QUE EFETUOU PIX SEGUNDO DADOS INFORMADOS EM OUTRO PERFIL DE INSTAGRAM,** QUE TERIA SIDO INDICADO PELOS FALSÁRIOS QUE INVADIRAM A CONTA DO REQUERENTE. PREJUÍZO MATERIAL QUE NÃO DECORREU DE FORMA DIRETA E IMEDIATA NA INVASÃO HACKER AO PERFIL DO PROMOVENTE. **FALTA DE CAUTELA NA CONCLUSÃO DE INVESTIMENTO PELA PARTE PROMOVENTE. INDENIZAÇÃO POR DANOS MATERIAIS AFASTADA**. SENTENÇA REFORMADA. RECURSO EM PARTE PROVIDO (TJPR, 2023).

Assim no caso acima da jurisprudência, verifica-se que não consegue a lei brasileira apontar o nexo de causalidade de forma adequada entre a conduta e o dano causado pela conta hackeada.

Seja analisado o julgado abaixo, que retrata o caso de uma conta hackeada da rede social Instagram:

> RECURSO INOMINADO. **MATÉRIA RESIDUAL. APLICATIVO INSTAGRAM. PRELIMINAR DE ILEGITIMIDADE PASSIVA. INOCORRÊNCIA.** PLATAFORMA EM QUE SE ENCONTRA HOSPEDADO O PERFIL QUE VIABILIZOU O GOLPE É DE RESPONSABILIDADE DA RÉ. MÉRITO RECURSAL. PROVAS QUE INDICAM QUE O PERFIL DE UM COLEGA DO AUTOR FOI HACKEADO. FRAUDADORES QUE UTILIZARAM O PERFIL PARA APLICAR GOLPES. **FALHA NA PRESTAÇÃO DO SERVIÇO CARACTERIZADA. AUTOR QUE FOI PREJUDICADO FINANCEIRAMENTE PELO GOLPE, POIS TRANSFERIU VALORES PARA OS ESTELIONATÁRIOS ACREDITANDO SER PARA SEU COLEGA. FRAUDE PERPETRADA MEDIANTE A INSEGURANÇA DO SISTEMA DA RÉ.** PROCEDÊNCIA DO PEDIDO DE INDENIZAÇÃO POR DANO MATERIAL. DANO MORAL CONFIGURADO. SITUAÇÃO QUE ULTRAPASSA O MERO DISSABOR COTIDIANO. SENTENÇA REFORMADA. RECURSO CONHECIDO E PROVIDO (TJPR, 2023).

Fica demonstrado que sempre há ambiguidade e generalidade quando busca-se aplicar os tipos penais que são vagos e imprecisos, o que causa dificuldade na aplicação prática, levando à insegurança jurídica, tanto para vítimas, quanto para os acusados (Da Silva, 2015).

A questão da inadequação do tipo penal para o crime de invasão de dispositivo eletrônico faz com que, mesmo que pessoas já tenham sido denunciadas e processadas pela prática deste crime, não haja diferenciação dos tipos de invasão, resultando em penas desproporcionais ou insuficientes para a gravidade do crime, o que na prática acarreta na impunidade e na insegurança jurídica. Mostra-se, portanto,

a necessidade de existir legislação que especifique e diferencie crimes cibernéticos, de forma que os tipos penais sejam adaptados à realidade digital (Galli, 2017).

Um dos grandes desafios da jurisdição é que o ambiente virtual ultrapassa as fronteiras, o que complica a aplicação da lei em um único país. Assim, a falta de acordos internacionais dificulta para punição e localização dos criminosos que operam em muitas jurisdições (Jesus; Milagre, 2016).

Um caso real de inadequação do tipo penal em crimes relacionados ao hackeamento de contas de Instagram ocorreu no Brasil em 2020, fato que foi apelidado como “Caso dos Influenciadores”. Neste caso, um grupo de criminosos invadiu a contas dos influenciadores digitais, trocou senhas e se passou por eles, aplicando golpes em seus seguidores. Verifica-se que o artigo 154-A do Código Penal (acesso não autorizado a sistema informático) poderia ser aplicado, mas é muito complexo e dificultoso conseguir demonstrar que de fato houve a violação do sistema e especificar a intenção criminosa, especialmente nos casos onde as vítimas não notam a invasão de maneira imediata (Assunção, 2021).

Este fato se assemelha aos crimes de furto mediante fraude e estelionato, mas caso fossem assim tipificados, estaria inadequado, pois a forma como os bens foram obtidos, ou seja, sem contato físico com a vítima causa inúmeros debates sobre a devida tipificação (Costa, 2023).

Dessa forma, o entendimento jurisprudencial sobre o crime cibernético tem sido:

> Habeas Corpus. “**Operação Token”.** Crimes de organização criminosa (art. 2º, caput, da Lei 12.850/2013 – 1º fato[1]), furto qualificado mediante fraude (art. 155, § 4º, inciso II, do CP – 2º e 3º fatos[2]), furto qualificado mediante fraude tentado (art. 155, § 4º, inciso II c.c. art. 14, inciso II, ambos do CP – 4º fato[3]) e lavagem de dinheiro (art. 1º, caput, da lei n. 9613/1998 – 5º, 6º, 7º, 8º, 9º, 10º, 11º, 12º, 13º e 14º fatos[4])[5], **todos praticados no âmbito dos crimes cibernéticos**. Medidas cautelares diversas da prisão impostas em substituição à prisão preventiva. Pleito de revogação das medidas de recolhimento domiciliar noturno e proibição de se ausentar da comarca sem autorização do Juiz. Indeferimento pelo Juízo a quo. Alegação de não mais existirem motivos para sua manutenção. Descabimento. Decisão corretamente fundamentada diante da necessidade da garantia da ordem pública, conveniência da instrução penal e aplicação da lei penal. Fundamentação sucinta que não se confunde com ausência de fundamentação. Admissibilidade de fundamentação sucinta e/ou per relationem. Necessidade da manutenção das medidas cautelares presente. Contexto fático que autoriza a manutenção das medidas cautelares diversas da prisão. Ordem denegada. “2. A fundamentação sucinta não se confunde com a ausência de motivação do ato (HC nº 111.127/DF, Primeira Turma, Rel. Min. Luiz Fux, DJe de 10/5/13)” - [HC 201179 AgR, Relator(a): DIAS TOFFOLI, Primeira Turma, julgado em 17/08/2021, PROCESSO ELETRÔNICO DJe-177 DIVULG 03-09- (STF, 2021).

Em suma, ao levar em consideração a realidade vivida atualmente, um cenário demasiadamente digital, faz-se imprescindível a reformulação da legislação brasileira no âmbito dos crimes cibernéticos, uma vez que os tipos penais existentes não são capazes de calcular a gravidade dos delitos virtuais. Com a edição de Leis compatíveis com a atualidade, certamente haverá mais justiça e proteção jurídica em relação aos bens jurídicos vitimados.

5 LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados, surgiu como resultado da má utilização dos dados eletrônicos e da falta da segurança das informações, ocorrendo vazamentos de dados. A Lei nº 13.709/2018 tem por objetivo garantir maior segurança e proteção aos dados pessoais aos mais diversos meios, principalmente os meios eletrônicos,

> De acordo com a LGPD, os dados pessoais são informações capazes de identificar alguém e o tratamento desses representa qualquer operação que os envolvem, como a sua coleta, uso e transmissão. A Lei representa o esforço mundial para que se tenha maior segurança sobre as informações e privacidade de dados. O seu objetivo é permitir que o cidadão tenha mais controle sobre o tratamento de suas informações pessoais (Alecrim, 2020, s.p).

Demonstrando assim que foi criada para estabelecer regras mais precisas e claras sobre como deve ser o tratamento de dados pessoais, a LGPD tem como foco gerar maior *accountability*[1] e transparência para os agentes de tratamento de dados, podendo ser pessoa jurídica ou física, de direito privado ou público, e por meio dessa lei, deve ser assegurado práticas seguras e transparentes. Dessa forma, está alicerçada em cinco eixos principais, quais sejam: a) generalização e unidade para aplicabilidade da Lei; b) legitimar o tratamento de dados (hipóteses autorizativas); c) direitos e princípios do titular; d) obrigações que os agentes são sujeitos no tratamento dos dados; e) responsabilização dos agentes (Doneda; Mendes, 2018).

O direito à proteção de dados pessoais além de necessário, está diretamente vinculado ao direito à privacidade e sua análise é complexa. Por esse fato, não há como negar a relação direta existente entre a proteção de dados e o direito à privacidade. Enquanto este se caracteriza principalmente pela dicotomia entre as esferas pública e privada, aquele abarca uma gama de proteção ainda maior, pois não se caracteriza apenas como um direito que reflete de forma negativa, mas também como um direito de liberdade, ou seja, seu titular tem controle sobre os dados e uma grande variedade de proteção ainda mais extensa, em relação aquele que se confere ao direito da privacidade (Doneda, 2006).

Na maioria dos casos, quando ocorre a violação Lei de Proteção de Dados, verifica-se a seguinte situação conforme a descrita abaixo:

> INDENIZATÓRIA. IMPROCEDÊNCIA NA ORIGEM. INSURGÊNCIA DO AUTOR. DADOS DO AUTOR VINCULADOS A PROCESSO

[1] De acordo com o dicionário Aurélio significa responsabilidade.

> CRIMINAL POR ERRO DE AGENTE ESTATAL. CASO DE HOMÔNIMO. FALHA NA PRESTAÇÃO DO SERVIÇO PÚBLICO. SÃO NOTÓRIOS OS RISCOS INERENTES À ATRIBUIÇÃO DE AÇÃO PENAL. SENTIMENTOS DE TEMOR, ANGÚSTIA E ANSIEDADE DE SE VER ENVOLVIDO EM PROCESSO CRIMINAL. VIOLAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD). A INSERÇÃO ESPÚRIA DO NOME DO AUTOR DE MODO ESPÚRIO EM BANCO DE DADOS CRIMINAL VIOLA A LGPD. DANO MORAL CARACTERIZADO NO CASO CONCRETO. DEVER DE INDENIZAR. SENTENÇA REFORMADA. RECURSO PROVIDO (TJ-SC, 2022).

Ao realizar análise da LGPD é importante destacar que dados e informação têm conceituação diferente, mesmo sendo abordados e tratados como sinônimo na LGPD. Enquanto dados se referem a fatos brutos ou não processados[2], a informação é o tratamento desses dados, a fim de se compreender o seu resultado (Alecrim, 2020).

O autor também considera que é importante entender a diferença entre dado e informação:

> [...] o dado é um conjunto de letras, números ou dígitos que, tomado isoladamente, não transmite nenhum conhecimento, ou seja, não contém um significado claro. A informação é todo o dado trabalhado ou tratado. Pode ser entendida como um dado com valor significativo atribuído ou agregado a ele e com um sentido natural e lógico para quem usa a informação (Rezende, 2008, p. 08).

Neste sentido, nota-se que a tecnologia de informação está presente no cotidiano de todas as pessoas sejam pessoas físicas ou pessoas jurídicas, todos fazem uso da troca de informação e precisam armazenar dados o tempo todo, como fotos, vídeos, mensagens, uma quantidade de itens extensa, motivos pelos quais a população brasileira viu necessidade em garantir maior controle e proteção sobre seus dados, o que foi possível, até certo ponto, com a edição da Lei Geral de Proteção de Dados.

7 LEGISLAÇÃO ESTRANGEIRA E COOPERAÇÃO NOS CRIMES CIBERNÉTICOS BRASILEIROS

A sugestão para aplicabilidade correta do tipo penal em crimes cibernéticos no Brasil é a cooperação internacional, uma vez que em vários países já existem inúmeras leis de crimes cibernéticos. É importante ressaltar que muitos crimes são cometidos por hackers de outras nacionalidades, então a cooperação internacional seria de suma importância. Vejamos algumas leis internacionais.

[2] Qualquer atividade realizada com dados pessoais e dados pessoais sensíveis é chamada de tratamento, desde a coleta, utilização, transmissão, armazenamento, até a eliminação. Antes de realizar o tratamento, é imprescindível identificar a base legal, isto é, a hipótese prevista na LGPD que autoriza o tratamento do dado pessoal.

Nos Estados Unidos existe: a Lei de Proteção à Infância na Internet (COPPA, 1998); a Lei de Fraude e Abuso de Computadores (CFAA, 1986), a Lei de Privacidade de Comunicações Eletrônicas (ECPA, 1986) e a Lei de Segurança de Dados (Data Security Law).

Na União Europeia, existem: Diretiva sobre Crimes Cibernéticos (2013/40/UE); Regulamento Geral sobre Proteção de Dados (GDPR, 2016/679) e Diretiva sobre Segurança de Redes e Informações (NIS, 2016/1148).

Existe ainda, a Convenção contra o crime cibernético, também chamada de Convenção de Budapeste, é uma ferramenta legal destinada a fomentar a colaboração global no enfrentamento aos delitos digitais. A Convenção incorpora regras de Direito Penal e Processo Penal, fornecendo conceitos e procedimentos. Além disso, ressaltamos que a Convenção tem natureza obrigatória (e não meramente facultativa), uma vez que foi promulgada e incorporada ao nosso sistema jurídico pelo Decreto Presidencial no 11.491/23 (Alburquerque, 2023).

A Convenção de Budapeste, oficialmente chamada de Convenção sobre Cibercrime, é um acordo internacional destinado a enfrentar o crime virtual e fomentar a colaboração entre nações na apuração e no combate a infrações digitais. Firmada em 2001, esse tratado é visto como um ponto crucial na legislação relacionada aos delitos cibernéticos.

Em 2012, o Brasil integrou a convenção ao seu sistema jurídico ao aderir ao tratado. A implementação da Convenção de Budapeste no país abrange diversas áreas como da legislação, pois o Brasil tem se empenhado em modernizar suas normas para se adequar às diretrizes globais definidas pela convenção, como a Lei Carolina Dieckmann (Lei nº 12.737/2012), que define e pune delitos relacionados à internet (Carvalho Ramos, 2023).

O acordo promove a colaboração entre as autoridades do Brasil e nações estrangeiras na luta contra os crimes cibernéticos. Essa cooperação é realizada por meio da troca de informações e conhecimentos, bem como do suporte recíproco em investigações (Jesus; Milagre, 2016).

O Brasil tem promovido o treinamento de profissionais da segurança pública e do sistema judiciário para enfrentar os desafios impostos pelo cibercrime, adotando orientações e práticas recomendadas pela convenção (Galvão, 2020).

A nação tem implementado iniciativas voltadas para fortalecer a segurança na internet, salvaguardar informações pessoais e informar a população sobre os perigos e medidas preventivas associadas ao mundo digital (Carvalho Ramos, 2023).

A implementação adequada da Convenção de Budapeste apresenta um desafio persistente, devido à rápida transformação da tecnologia e às novas modalidades de crimes cibernéticos. Entretanto, a inclusão do Brasil no tratado evidencia um engajamento em lidar com essas dificuldades de maneira colaborativa e integrada.

Para o Brasil, a Lei de Segurança de Dados pode ser considerada uma referência, pois trata-se de um conjunto de leis e normas destinadas a garantir a segurança e a privacidade dos dados. São alguns aspectos fundamentais desta lei:

aviso de violação de dados – as empresas são obrigadas a informar os clientes quando há uma violação de dados; proteção de dados delicados – as organizações precisam salvaguardar dados delicados, tais como dados financeiros e de saúde; proteção de dados – as organizações precisam adotar ações de segurança para salvaguardar informações e; responsabilidade – as empresas têm a obrigação de assegurar a proteção dos dados internet (Carvalho Ramos, 2023).

Para que a efetiva implementação da referida lei seja possível, existem mudanças necessárias a serem feitas na gestão dos fornecedores, como a realização de auditoria de segurança de dados, implementação de medidas de segurança para proteger dados, desenvolvimento de política de notificação de violação de dados, treinamento de funcionários sobre segurança de dados e, realização de avaliações de risco regulares (Jesus; Milagre, 2016).

A Lei de Segurança de Dados dos EUA serve de modelo para proteção da segurança e da privacidade dos dados. A LGPD brasileira segue princípios semelhantes e exige medidas de segurança para protege-los. Neste sentido, empresas que operam no Brasil devem implementar medidas de segurança e notificação de violação de dados para cumprir com a LGPD (Alburquerque, 2023).

As leis se assemelham com o aviso de violação de dados – a LGPD prevê o requerimento da comunicação de qualquer violação de dados em até 72 horas; e a defesa de informações sensíveis, que requerem uma proteção extra. E com relação a proteção de dados, a LGPD requer ações de segurança para salvaguardar informações. A Lei de Segurança de Dados dos Estados Unidos é válida apenas para empresas sediadas no país, enquanto a LGPD é aplicável a todas as empresas que recolhem e processam dados de cidadãos brasileiros. As penalidades por infringir a Lei de Segurança de Dados dos Estados Unidos são mais severas do que as previstas anteriormente (Carvalho Ramos, 2023).

Para tanto, a cooperação internacional será efetiva no combate aos delitos cibernéticos, uma vez que a globalização também abriu portas para que criminosos de qualquer país possa praticar delitos em qualquer parte do mundo, através da virtualidade. Além disso, este conjunto de esforços fará com que o Brasil possa espelhar-se nas normas de outros países, proporcionando um ambiente digital mais civilizado e seguro.

CONSIDERAÇÕES FINAIS

Ao término do estudo, compreende-se que sobre o que trata o direito penal, ou seja, sua aplicabilidade como *ultima ratio*, no estudo em comento, constata-se que o aumento da propagação do uso de redes sociais e internet, novos crimes surgiram nesses ambientes e o Judiciário e Legislativo e tiveram a necessidade de atualização, com as normativas e leis para atender essa demanda. No entanto, verifica-se que, adequar ao tipo penal das novas leis de crimes realizados nesse ambiente é um desafio amplo e complexo, uma vez que, em vários casos de crimes cibernéticos a tipicidade penal do crime é inadequada.

Enquanto o legislador, por muitas vezes, se socorre às leis para tentar dar uma resposta à sociedade, esta paga um enorme preço, seja pela morosidade com que as atitudes são tomadas, seja porque as leis editadas não acabam resultando em efetiva proteção aos bens jurídicos.

Dessa forma, para solucionar esse problema é necessário edição de novas leis, em um sistema legislativo já inchado, como mecanismo único e suficiente para resolver o problema de segurança pública no país, é utópico, uma vez que criar novas leis penais sem a tipicidade correta, simplesmente aumentando as penas dos crimes já existentes ou simplesmente retirar o criminoso do meio social por um tempo determinado, por si só, não acaba com os altos índices de criminalidade.

É um desafio e uma tarefa complexa e árdua eliminar completamente a criminalidade digital, considerando a constante evolução das tecnologias e o aumento da complexidade das ameaças cibernéticas. Contudo, uma mescla de táticas legislativas, educacionais, tecnológicas e colaborativas pode diminuir consideravelmente a ocorrência de delitos digitais e aprimorar a segurança na internet, como Uma das estratégias mais eficientes para enfrentar a criminalidade digital é elaborar e melhorar leis que tratem especificamente dos delitos cibernéticos.

A desinformação acerca da segurança digital e do processo de crimes digitais representa uma das maiores fragilidades. Portanto, a educação e a sensibilização são ações fundamentais para diminuir a criminalidade digital.

REFERÊNCIAS

ALECRIM, Emerson. **O que você deve saber sobre a lei de proteção de dados pessoais no Brasil**. 2020. Disponível em: <https://tecnoblog.net/250718/lei-geral-protecao-dados-brasil/>. Acesso em: 13 out. 2024.

ANDREUCCI, Ricardo Antonio. **Manual de direito penal**. 12. ed. São Paulo: Saraiva Educação, 2018. Livro eletrônico. p.21-29.

ASSUNÇÃO, Mayume da Silva. **A tipicidade dos crimes cibernéticos no direito penal brasileiro: Um estudo sobre o impacto da Lei nº 12.737/2012 e a (des)construção de uma dogmática penal dos crimes cibernéticos.** GuanambiBA. 2021.

ÁVILA, Humberto. **Teoria dos Princípios:** da definição à aplicação dos princípios jurídicos. São Paulo: Malheiros, 2013.

BUSADO, Paulo César. **Direito Penal.** Parte Geral. 2ª Ed. São Paulo: Atlas, 2015. p.57-66.

BITTENCOURT, Cezar Roberto. **Tratado de Direito Penal:** Parte Geral 1. 16. Ed. São Paulo: Editora Saraiva, 2011. p.79-81.

BITENCOURT, Cezar Roberto. **Tratado de direito penal: parte geral.** 25. ed. São Paulo: Saraiva Educação, 2019. p.30-33.

BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial da União,** Brasília, DF, 5 out. 1988.

BECK, Francis Rafael; RITTER, Ruiz. A coleta de perfil genético no âmbito da Lei nº 12.654/12 e o direito a não autoincriminação: uma necessária análise. **Revista da AJURIS.** Vol. 42, n. 137, mar. 2015.

CARVALHO RAMOS, André de. **Curso de Direito Internacional Privado.** 3. ed. São Paulo: Saraiva, 2023.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e Seus Aspectos Processuais.** Rio de Janeiro, Lumen Júris, 2003. p.44-46.

CASTRO, Renato de Lima. Garantismo penal: uma ilusão? In: PRADO, Luiz Regis. (Org.). **Direito penal contemporâneo:** Estudos em homenagem ao Professor José Cerezo Mir. São Paulo: *Revista dos Tribunais*, 2007, p.12-14.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet.** Editora: SARAIVA JURIDICO. Ano de Edição: 2010. p.53-58.

COSTA, Amanda Maciel. **Regime disciplinar diferenciado:** aspectos históricos e críticos. 2013. Disponível em: < https://www.direitonet.com.br/artigos/exibir/8147/Regime-disciplinar-diferenciado-aspectos-historicos-e-criticos> Acesso em: 24 out. 2024.

DA SILVA, Patrícia Santos. **Direito e crime cibernético:** análise da competência em razão do lugar no julgamento de ações penais. Brasília: Vestnik, 2015. p.19.

DONEDA, Danilo; MENDES, Laura Schertel. Reflexões Iniciais sobre a Nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor,** São Paulo, v. 120, p. 469- 483, nov.-dez. 2018.

DOTTI, René Ariel. **Curso de Direito Penal:** Parte Geral. 2. ed. rev. atual. e ampl. Rio de Janeiro: Forense, 2005. p. 54.

GALVÃO, Fernando. **Teoria do crime da pessoa jurídica:** proposta de alteração do PSL nº 236/12. Belo Horizonte: D'Plácido, 2020. p. 90-95.

HOFFMANN-RIEM, Wolfgang. Autorregulação, autorregulamentação e autorregulamentação regulamentada no contexto digital. **Revista da AJURIS**, v. 46, n. 146, p. 529-554, 2019.

JESUS, Damásio de, e MILAGRE, José Antonio. **Manual de crimes informáticos.** São Paulo: Saraiva, 2016. p. 22-45.

LILLA, Paulo. **LGPD trouxe segurança aos pacientes, mas seu cumprimento ainda é complexo.** 2022. Disponível: < https://medicinasa.com.br/lgpd-cumprimento/#:~:text=%E2%80%9CA%20LGPD%20confere%20maior%20transpar%C3%AAncia,aspectos%20sens%C3%ADveis%20de%20sua%20personalidade.> Acesso em: 20 dez. 2022.

PINHEIRO, Patricia Peck. **Direito Digital.** 3. ed. São Paulo: Saraiva, 2009. p.45-50.

PIOVESAN, Flávia. **Direitos humanos e o direito constitucional internacional.** 4ed. São Paulo: Max Limonad, 2000. p. 98.

PRADO, Luiz Regis. **Curso de Direito Penal Brasileiro**: Parte Geral I, arts. 1º a 120. 6. ed. rev.atual e ampl. São Paulo: RT, 2006. p. 141.

PRADO, Luiz Regis. **Curso de Direito Penal Brasileiro**: Parte Geral I, arts. 1º a 120. 10. ed. rev.atual e ampl. São Paulo: RT, 2011. p.60-75.

QUEIROZ, Paulo. **Direito Penal.** Parte Geral. 4ª edição. 2008. p.133.