UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS I – CAMPINA GRANDE
CENTRO DE CIÊNCIAS JURÍDICAS
CURSO DE BACHARELADO EM DIREITO

RAFAELLE BEATRIZ SOARES PEREIRA

CRIMES CIBERNÉTICOS: PANORAMA HISTÓRICO DA NORMATIZAÇÃO NO ORDENAMENTO JURÍDICO BRASILEIRO

CAMPINA GRANDE - PB
2022

RAFAELLE BEATRIZ SOARES PEREIRA

CRIMES CIBERNÉTICOS: PANORAMA HISTÓRICO DA NORMATIZAÇÃO NO ORDENAMENTO JURÍDICO BRASILEIRO

Trabalho de Conclusão de Curso apresentado à Coordenação do Curso de Direito da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Bacharel em Direito.

Área de concentração: Ciências Criminais e Novas Tecnologias.

Orientador: Prof.ª Dr.ª Ana Alice Ramos Tejo Salgado

CAMPINA GRANDE - PB
2022

P435c Pereira, Rafaelle Beatriz Soares.

Crimes cibernéticos [manuscrito] : panorama histórico da normatização no ordenamento jurídico brasileiro / Rafaelle Beatriz Soares Pereira. - 2022.

36 p.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Estadual da Paraíba, Centro de Ciências Jurídicas , 2022.

"Orientação : Profa. Dra. Ana Alice Ramos Tejo Salgado , Coordenação do Curso de Direito - CCJ."

1. Crimes cibernéticos. 2. Novas tecnologias. 3. Impactos jurídicos. 4. Ambiente digital. I. Título

21. ed. CDD 345

Elaborada por Kênia O. de Araújo - CRB - 15/649 BSCCJ/UEPB

RAFAELLE BEATRIZ SOARES PEREIRA

CRIMES CIBERNÉTICOS: PANORAMA HISTÓRICO DA NORMATIZAÇÃO NO ORDENAMENTO JURÍDICO BRASILEIRO

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Jurídicas, Universidade Estadual da Paraíba – Campus I, como requisito parcial para a obtenção do título de Bacharel em Direito.

Área de Concentração: Ciências Criminais e Novas Tecnologias.

Aprovada em: 02 / 08 /2022

BANCA EXAMINADORA

Ana Alice Ramos Tejo Salgado

Prof.ª Dr.ª Ana Alice Ramos Tejo Salgado. (Orientadora)

Universidade Estadual da Paraíba (UEPB)

Esley Porto

Prof. Me. Esley Porto

Universidade Estadual da Paraíba (UEPB)

Rosimeire Ventura Leite

Prof.ª Dr.ª Rosimeire Ventura Leite

Universidade Estadual da Paraíba (UEPB)

AGRADECIMENTOS

Grata, em primeiro lugar, a Deus, pelo privilégio de nossa reaproximação e por sua intercessão e amor inesgotáveis, que me dão forças para continuar. Aos meus pais, pelos ensinamentos e gestos de amor e confiança, vocês tornaram essa graduação possível. A Rebeca, minha irmã e maior orgulho, que me prova diariamente que nossas diferenças nos tornam mais próximas, minha gratidão por se fazer presente mesmo com tantas obrigações a cumprir. A Flávio, meu cunhado, que pelo amor e companheirismo a Rebeca se tornou família. E a minhas avós, Helena e Beatriz (*in memoriam*), a quem dedico esta produção.

Aos amigos, em especial a Caio, por sempre se fazer presente, sua amizade e zelo são graça em minha vida. A Ana Luiza, companheira de jornada, pela confiança e parceria. A Ianca, prova de que amizade não se limita à proximidade física. A Yago, usado tantas vezes por Deus para me trazer esperança nos últimos anos. E aos demais, que torcem por mim e foram apoio durante essa caminhada.

Ainda, aos professores e demais profissionais, fonte de inspiração. Em especial a Ana Alice, por sua competência e orientação na construção deste trabalho.

RESUMO

A rede mundial de computadores, responsável por estreitar relações e facilitar a execução de tarefas, impôs novos desafios no tocante à segurança dos usuários. Nesse contexto, os riscos no ambiente digital avançam nas mais diversas áreas, entre elas, o aumento de condutas delituosas executadas através da Internet. Nesse sentido, o presente artigo possui como objetivo estudar os impactos jurídicos oriundos da revolução tecnológica que relacionam-se aos crimes cibernéticos, identificando a legislação existente sobre o tema no ordenamento jurídico brasileiro, em especial as definidoras de tipos penais no âmbito virtual. É uma pesquisa bibliográfica, com caráter exploratório e utilização do método dedutivo. O objeto de estudo se limitou à análise das disposições relacionadas à temática: Lei n.º 12.737, de 30 de novembro de 2012, Lei n.º 13.964, de 24 de dezembro de 2019, Lei n.º 13.968, de 26 de dezembro de 2019, Lei n.º 14.132, de 2021 (Lei de Stalking), Lei n.º 14.155, de 27 de maio de 2021, entre outras. Conclui-se que há avanços na adequação dos diplomas legais aos crimes virtuais, no entanto, se identifica a necessidade de maior especificidade da estrutura legal brasileira no tratamento destes delitos.

Palavras-Chave: Crimes cibernéticos. Novas Tecnologias. Impactos jurídicos. Ambiente digital.

ABSTRACT

The global computer network, responsible for strengthening relationships and facilitating the execution of multiple tasks, also imposed new challenges regarding the safety of users. In this context, the risks in the digital environment advance in diverse areas, among them, the increase of criminal conduct carried out through the Internet. In this discussion, this article aims to study the legal impacts arising from the technological revolution that relate to cybercrimes, identifying the existing legislation on the subject in the Brazilian legal system, especially the definitions of criminal types in the virtual environment. It is a bibliographical research, with an exploratory character and use of the deductive method. The object of the study was limited to the analysis of legislations related to the theme: Law n.º 12.737/ 2012, n.º 13.964/2019, n.º 13.968/2019, n.º 14.132/2021 (Stalking), n.º 14.155/2021, among others. It is concluded that there are advances in the adequacy of legal diplomas for virtual crimes; however, the need for greater specificity of the Brazilian legal structure in the treatment of these crimes is identified.

Keywords: Cybercrimes. New technologies. Legal impacts. Digital environment.

SUMÁRIO

1 INTRODUÇÃO

O presente trabalho de conclusão de curso possui como objetivo geral estudar os impactos jurídicos oriundos da revolução tecnológica que relacionam-se aos crimes cibernéticos, identificando a legislação existente sobre o tema no ordenamento jurídico brasileiro, em especial as definidoras de tipos penais no âmbito virtual. Para isto, o estudo pautou-se em analisar as principais alterações legislativas relacionadas às novas tecnologias, além de pontuar as normas definidoras de tipos penais enquadrados nos crimes cibernéticos, investigando o arcabouço legal existente.

Faz-se mister, portanto, compreender o desenvolvimento histórico que acompanha o surgimento dos crimes virtuais, a fim de que seja possível analisar sua presença no ordenamento jurídico.

A partir da década de 1970, caracterizada por revoluções nas áreas de telecomunicações e informática, tornou-se possível a definição de novas bases econômicas, pautadas na disseminação da informação e no desenvolvimento tecnológico, potencializado com o advento da Internet, responsável por democratizar o acesso à informação e, por consequência, possibilitar avanços digitais em maiores proporções.

Somados a tais acontecimentos, a popularização de ferramentas tecnológicas e dos equipamentos para a conexão, como computadores e *smartphones* – que se tornaram acessíveis a um percentual significativo da população, com o passar dos anos –, são pontos essenciais no processo de compreensão da importância da Internet atualmente. Relevante, ainda, observar a dimensão que esta rede conquistou durante a pandemia da COVID-19, situação que ocasionou um crescimento exponencial da utilização de tecnologia em atividades cotidianas.

Com a proibição de aglomerações, surgiu a necessidade de que fossem encontrados novos meios para a realização de práticas essenciais para a vida social, tendo sido a Internet a ferramenta principal para a concretização deste ideal. Dessa forma, com a adaptação de funções laborais e educacionais para o modelo remoto (*online*), o tempo de utilização de equipamentos eletrônicos foi intensificado.

Portanto, se antes dos protocolos de isolamento social e da adoção do sistema de atividades remotas já se discutia acerca de temas como a proteção de dados e privacidade, com o aumento da utilização deste espaço virtual, multiplica-se

a necessidade de que sejam estabelecidos debates acerca dos riscos inerentes ao ambiente digital, de modo a alertar os usuários a respeito das ameaças às quais estão suscetíveis.

Sendo assim, são consideradas práticas ilícitas em ambientes digitais (crimes cibernéticos) aquelas já tipificadas no Código Penal, desde que possam ser cometidas através de um dispositivo ou sistema informático. Além destas, consideram-se também aquelas tipificadas em leis específicas, por serem executadas exclusivamente através de equipamentos ou redes digitais.

Diante dessa discussão, se questiona a evolução histórica da regulamentação legal dos crimes cibernéticos. Nesse sentido, é possível encontrar diplomas legais referentes a esta modalidade de delito, a exemplo da Lei n.º 12.737, de 30 de novembro de 2012, popularmente conhecida como Lei Carolina Dieckmann, e a mais recente Lei n.º 14.155, de 27 de maio de 2021 cuja origem possui relações com o aumento dos casos durante a pandemia de COVID-19, entre outros diplomas legais. Este fato exemplifica a necessidade de que a ciência jurídica esteja em constante aperfeiçoamento, adequando-se às dinâmicas sociais, visando acompanhá-las.

De todo modo, ainda que a criação dos instrumentos supracitados caracterize-se como um importante avanço no combate aos crimes cibernéticos, inúmeros desafios permanecem carentes de solução, seja na identificação e tipificação de novas condutas, na investigação pelas autoridades policiais ou na conscientização dos usuários, como combate preventivo.

Assim sendo, a escolha do tema justifica-se a partir de reflexões estimuladas pela observação da nova realidade imposta pelo corona vírus, que se tornou parte da rotina da população mundial. Somado a isto, o reconhecimento do aumento de casos criminais que recorrem à Internet ou a utensílios tecnológicos como meio para a sua execução, veiculados nos meios de comunicação, despertou o interesse pelo estudo.

Pretende-se, portanto, através deste trabalho, oferecer bases para a análise do arcabouço jurídico existente no contexto dos crimes cibernéticos, não existindo, de toda forma, a pretensão de esgotamento do tema, por sua complexidade e atualização diária. Tendo como público-alvo os operadores do Direito e a sociedade em geral, busca-se, a partir da obtenção dos resultados, ofertar uma visão geral acerca das regulamentações atuais e da possível necessidade da criação de novos

textos legais, alertando, ainda, a comunidade acadêmica e local dos perigos ligados ao ambiente virtual.

O desenvolvimento do tema proposto realizar-se-á em três partes. A primeira seção será responsável por abordar a relação entre a tecnologia e sociedade, identificando a presença das ferramentas tecnológicas durante a história do homem e seu papel na atualidade, além de identificar os impactos jurídicos oriundos deste fenômeno. Na segunda parte, o estudo dedicar-se-á ao estudo dos crimes virtuais e aspectos gerais a estes relacionados. Por fim, a terceira seção apresentará as previsões relacionadas aos crimes cibernéticos encontradas na legislação brasileira, organizadas de modo cronológico, além de abordar a discussão acerca da criação de lei específica.

2 TECNOLOGIA E SOCIEDADE

O homem, como ser social, possui como característica intrínseca a busca por evolução, seja com fim pessoal ou comunitário. A partir da observação das dinâmicas presentes nas sociedades mais antigas, pode-se reconhecer a tendência a uma formação de grupos que trabalham de modo a facilitar a execução de atividades essenciais, tornando-as mais práticas, a exemplo da divisão de grupos responsáveis pela caça, segurança e alimentação, como pode ser observado nas civilizações do período paleolítico.

A divisão de tarefas e a atribuição de responsabilidades a diferentes membros de determinada coletividade estende-se pela história da humanidade, estando presente, do mesmo modo, na sociedade atual. Para além dessa estratégia, o homem buscou munir-se de utensílios que o auxiliassem na obtenção de seus objetivos e melhoria de práticas, atitude esta que promoveu alguns dos mais importantes feitos da raça humana, tais como a criação de lâminas, da roda, dos veículos, etc.

Existe, naturalmente, uma tendência a considerar tecnológico apenas aquilo que se relaciona aos séculos mais recentes e à informática, de todo modo, a tecnologia e a sociedade estiveram relacionadas durante todo o processo evolutivo. Pode-se concluir dessa forma ao reconhecer como sendo tecnologia tudo aquilo que visa expandir a independência dos seres, podendo ser conceituada como “um sistema através do qual a sociedade satisfaz as necessidades e desejos de seus membros”. (SILVA, 2003, p. 53).

Importante reconhecer, de todo modo, que a importância e a presença dos resultados de tais empenhos modificaram-se durante o transcorrer do tempo, de modo que, na sociedade atual, a tecnologia ocupa um patamar essencial ao desenvolvimento, tornando-se tarefa de difícil execução a separação entre o progresso e aquela. Por essa razão, justificam-se os imponentes investimentos nesse campo, no cenário político e econômico mundial, tendo em vista a necessidade de que os países utilizem de modo eficaz a tecnologia, a fim de destacarem-se no plano global.

Pensando, portanto, na melhoria das qualidades de vida, do bem-estar e das oportunidades de crescimento da população, as ferramentas tecnológicas sofreram um crescimento exponencial nos últimos anos, possibilitando o cumprimento de

grande parte das atividades cotidianas através de instrumentos informáticos. Interessante ressaltar, ainda, que foi este um ponto crucial para a manutenção de setores essenciais para a sociedade durante a pandemia da COVID-19, que atingiu a população mundial desde o início de 2020, impossibilitando o transcorrer normal de funções laborais, educacionais e de lazer.

Pelo uso da tecnologia, foi possível que aulas e empregos fossem adaptados à realidade pandêmica, viabilizando as reuniões de forma remota, através da utilização de computadores e *smartphones*, instrumentos frutos da expansão informática. De modo especial, ao considerar o cenário global, atenta-se para o papel da Internet na propagação em grande escala de informações e na execução de diversas atividades, expandindo os modos de uso dos dispositivos e possibilitando uma comunicação expressiva em escala globalizada.

Estas razões apontam para o alcance, pela Internet, do “patamar de uma das invenções mais importantes da contemporaneidade” (REIS; VIANA, 2021, p. 1.609). De todo modo, o uso emergencial desta ferramenta por grande parte da população mundial de uma só vez não apenas se relaciona a benefícios e à praticidade, sendo necessário, por este motivo, estabelecer discussões acerca dos perigos pertinentes ao seu uso.

2.1 Internet e ferramentas informáticas

As transformações sociais e os modos de organização da comunidade global resultam na criação de diversas ferramentas que possuem como fim a facilitação da execução de atividades, visando a praticidade e o bem-estar da população envolvida. Diante desta afirmação, torna-se válido refletir acerca de uma das maiores revoluções na comunicação e economia mundial: a Internet.

Capaz de se sobrepor a fronteiras geográficas, esta rede mundial de computadores promove troca de informações facilitadas, tendo surgido com o propósito de servir como um sistema para o compartilhamento de informações, de modo a facilitar as estratégias de guerra, a partir de linhas de comunicação que, segundo Turner e Muñoz (2002) “poderiam ser estruturadas de forma que permanecessem intactas ou pudessem ser recuperadas em caso de um ataque nuclear”. (*apud* ABREU, 2009, p. 2).

De toda forma, ainda que tal nascimento tenha datado durante a guerra fria, em 1957, apenas nos anos 90 a Internet se proliferou no cenário mundial, a partir da criação do navegador *World Wide Web* (www), responsável por expandir as possibilidades de uso da rede mundial de computadores, tornando-a popular globalmente. A esse respeito, explica Pinheiro (2013, p. 39):

> Na década de 90, a Internet passou por um processo de expansão sem precedentes. Seu rápido crescimento deve-se a vários de seus recursos e facilidade de acesso e transmissão, que vão desde o correio eletrônico (*e-mail*) até o acesso a banco de dados e informações disponíveis na *World Wide Web* (WWW), seu espaço multimídia.

Ao reconhecer esta tecnologia e sua evolução como um marco histórico profundo, a forma de sua utilização apresenta-se como ponto a ser tratado com devida atenção, ao passo que se torna essencial para a definição dos limites da interferência na vida dos usuários. Afinal, com o fenômeno da popularização dos computadores e *smartphones*, que se tornaram acessíveis a parcela considerável da população global, o ambiente digital permanece ao alcance do usuário diariamente.

Esta aproximação é a responsável pela tendência da migração de serviços essenciais para o mundo virtual, a exemplo dos Bancos e instituições financeiras cujas comodidades podem ser acessadas através dos equipamentos citados. De todo modo, ao passo que a sociedade se beneficia com maior praticidade e rapidez na execução de tarefas, deve-se considerar a existência de usuários mal-intencionados, que podem usar os equipamentos com fins maculados.

Por esta razão, faz-se necessário atentar para o enfrentamento a tais condutas cometidas no ambiente informático, conhecendo-as e conscientizando os usuários da rede acerca de sua existência. Ainda, é essencial compreender que a reflexão acerca dos riscos inseridos na utilização da Internet e dos dispositivos informáticos é determinante para a diminuição do número de vítimas de condutas delituosas cujo meio de ação é o ambiente virtual.

Partindo deste pressuposto, torna-se possível observar a influência das transformações sociais em diversos aspectos, ao passo que o modo de vida passa a influir no modo de agir, pensar e decidir acerca de temáticas inerentes ao próprio convívio. Assim, pode-se notar que, com a multiplicação da utilização das tecnologias, o modo de comunicar-se e até mesmo de laborar sofreram gradativas mudanças, com a criação de aplicativos de mensagens instantâneas e de funções de trabalho remoto.

Estas adaptações, para além disso, possuem reflexos também no mundo jurídico, fazendo surgir a necessidade de que exista um arcabouço legal eficiente frente às novas formas de relação social e seus desafios. Desse modo, atenta-se para o impacto das transformações tecnológicas no Direito, fenômeno que pode ser percebido pela gradual transformação das normas jurídicas, consequência direta da construção social atual.

Assim, pode-se observar este fenômeno a partir da inclusão de previsões relacionadas ao mundo tecnológico no texto constitucional e em normas infraconstitucionais, do surgimento de discussões doutrinárias e em sede de Tribunais, para a formação de posicionamentos e, além disso, na criação de dispositivos legais que tipificam condutas delituosas cometidas no âmbito virtual, ao considerar sua reprovabilidade e alcance expandido, que serão alvo de estudo no presente trabalho.

2.2 Dos impactos jurídicos da era tecnológica

As transformações sociais refletem no ordenamento jurídico como decorrência do dinamismo do direito, característica essa capaz de promover uma constante mutação das normas, a fim de que exista uma adequação entre a teoria e a realidade social. A nível exemplificativo acerca deste fenômeno adaptativo, pode ser apontada a Lei n.º 11.106, de 28 de março de 2005, responsável por trazer alterações ao Código Penal, descriminalizando certas condutas e modificando tipos penais, de modo a melhor adequar o diploma legal à realidade social brasileira (SOUZA, 2005, *online*).

Dessa forma, cita-se a retirada da previsão do crime de sedução, cuja disposição encontrava bojo nos termos do artigo 217 do Código Penal, tendo sido excluído do ordenamento após a percepção de que não mais cabia a proteção jurídica à perda da virgindade, considerando a mudança de paradigmas entre a data da criação da norma (que refletia a sociedade dos anos 30) e o período atual, tendo a disposição perdido sua eficácia. Nesse sentido, afirma Miguel Reale (1996, p. 132):

> Há um trabalho, por assim dizer, de desgaste ou de erosão das normas jurídicas, por força do processo vital dos usos e costumes. O hábito de viver vai aos poucos influindo sobre as normas jurídicas, mudando-lhes o sentido, transformando-as até mesmo em seus pontos essenciais, ajustando-se às

> necessidades fundamentais da existência coletiva. (*apud* JARDIM, 2019, p. 161)

A este respeito, vale salientar que a hermenêutica jurídica oferece bases para o aprofundamento desta relação apontada entre as dinâmicas sociais e seus reflexos no mundo jurídico, especialmente através da chamada “interpretação progressiva”. Também denominada adaptativa ou evolutiva, possui como objetivo a adaptação da lei às necessidades e concepções do presente, conforme as transformações sociais, científicas e jurídicas atuais (SILVA, 2013).

Diante disso, torna-se possível atentar para que a evolução do direito permite tanto a exclusão de determinadas disposições quanto a criação de dispositivos legais específicos, voltados para as novas necessidades sociais, fazendo nascer discussões legais acerca da realidade fática, promovendo o dinamismo na ciência jurídica. Nesse cenário, podem ser identificadas questões como a dos crimes cibernéticos, cuja recorrência fez surgir para o direito a necessidade da inclusão de dispositivos que tratam dessa matéria, a fim de garantir a tutela dos bens jurídicos expostos a riscos pela via virtual.

Assim, na busca pela garantia da segurança jurídica dos usuários da rede mundial de computadores, surge para o direito a necessidade de refletir acerca da oferta de soluções legais às situações delituosas relacionadas a este ambiente cada vez mais presente na realidade mundial. Portanto, pode ser observado um processo de adequação das disposições legais, em especial no âmbito penal, a partir da tipificação condutas ilícitas no ambiente digital, de modo a consolidar as transformações sociais através da positivação de normas adequadas às dinâmicas atuais.

3 CRIMES VIRTUAIS

Com o crescimento da utilização da Internet, impulsionado pelo fenômeno da globalização, novas ligações passaram a existir no cenário global, sendo a rede mundial de computadores a responsável pela diminuição das distâncias entre as nações. Em termos simplificados, uma rede consiste na união entre dois ou mais computadores (equipamentos) com o fim de compartilhar informações, sendo este o seu princípio.

Tornou-se, portanto, cada vez mais comum defrontar-se com condutas cometidas no campo cibernético com o fim de obter vantagens, na maior parte das vezes econômicas, considerando o valor e a importância destas informações – também chamadas “dados” – compartilhadas diariamente. Por esta razão, os sistemas jurídicos mundiais iniciaram uma cruzada para a elaboração ou atualização de suas leis, adaptando-as à nova realidade. (PINHEIRO, 2014, p. 35).

A partir disso, torna-se possível identificar a necessidade de adaptação do Direito às novas dinâmicas sociais, em especial das legislações relacionadas ao Direito Penal e Processual Penal, promovendo uma especificidade dos tipos legais, adequando-os ao meio cibernético pela previsão de condutas cometidas neste ambiente e na cominação de penas proporcionais, de modo a “adequar a legalidade das ações com a realidade mundial, integrando os objetivos de prevenção e repressão da criminalidade, além da busca de uma maior eficiência por parte dos Estados.”. (BEZERRA; AGNOLETTO, 2020, p. 21).

Perante o exposto, cabe-nos pontuar que os crimes virtuais, inclusive, podem receber variadas nomenclaturas, tais como: crimes digitais, crimes cibernéticos ou cibercrimes. Em que pese a diversidade e a falta de consenso dos estudiosos e doutrinadores acerca de suas nomenclaturas e conceituações, o ponto de convergência encontra-se na existência de um dispositivo tecnológico para a realização das condutas ilícitas. (ASSUNÇÃO, 2018, p. 6).

Acerca de seu conceito, os crimes informáticos são considerados por Jesus e Milagres (2016) como sendo fatos típicos e antijurídicos cometidos por meio da ou contra a tecnologia da informação, podendo esta ser a informática, um sistema, um dispositivo ou uma rede.

Podem ser divididos entre crimes próprios e impróprios, sendo os primeiros aqueles que necessitam ter como meio de execução um sistema ou equipamento

informático. Por sua vez, os crimes virtuais impróprios são condutas comuns, executadas através de dispositivos conectados à Internet, porém que possuem também a alternativa de serem praticados por outros meios.

Torna-se válido, pois, compreender a ampla variedade de condutas que podem ser praticadas pela via digital, visto que não apenas estão em discussão as condutas já previstas no Código Penal, mas sim a estas somadas as novas práticas, descobertas dia após dia, no ambiente informático. Por esta razão, considerando a tendência de aumento da utilização e importância da tecnologia na vida da população mundial, faz-se necessário atentar para a necessidade de enfrentamento a tais atos ilícitos, visando a proteção dos bens jurídicos e dos próprios usuários da rede mundial de computadores.

4 DOS CRIMES CIBERNÉTICOS NA LEGISLAÇÃO BRASILEIRA

Ao passo que as legislações de todo o mundo iniciaram um processo de adaptação dos textos legais à atual realidade, o Brasil promulgou leis para tratar da regulamentação da *web*, visando proteger assuntos essenciais, tais como a proteção de dados pessoais, comércio eletrônico, direitos autorais digitais, entre outros. (PINHEIRO, 2014, p. 35).

De todo modo, o tema é tido como controverso e/ou complexo por alguns doutrinadores, a exemplo de Damiani (2019), à medida que problemáticas cercam as discussões acerca dos crimes virtuais, a exemplo de qual seria o bem jurídico tutelado, além da necessidade de que sejam reconhecidos como novos delitos ou se há a possibilidade de que continuem a ser consideradas as condutas já tipificadas no Código Penal, apenas observando a possibilidade de serem praticadas através da Internet.

Embora não haja consenso acerca de todos os detalhes que cercam o tema, podem ser reconhecidas tentativas de adequação do ordenamento jurídico brasileiro à realidade da criminalidade digital. Num primeiro momento, em uma perspectiva histórica, pode ser apontada como pioneira a tratar sobre tecnologia a Lei n.º 9.609, de 19 de fevereiro de 1998, responsável por incluir na legislação brasileira inovações, ao passo que dispôs sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, entre outras providências. (BRASIL, 1998).

No Capítulo V, o texto da mencionada legislação dispôs sobre as infrações e penalidades, que se relacionam aos direitos de autoria e registro de programas virtuais. Por esta razão, o trecho contido no artigo 12 pode ser considerado como a primeira tipificação voltada aos crimes cibernéticos (ASSUNÇÃO, 2018, p. 23), possuindo a seguinte redação:

> Art. 12. Violar direitos de autor de programa de computador:
>
> Pena - Detenção de seis meses a dois anos ou multa.
>
> § 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente:
>
> Pena - Reclusão de um a quatro anos e multa.
>
> § 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de

> comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.
>
> § 3º Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo:
>
> I - quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público;
>
> II - quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo.
>
> § 4º No caso do inciso II do parágrafo anterior, a exigibilidade do tributo, ou contribuição social e qualquer acessório, processar-se-á independentemente de representação.

Em um segundo momento, a Lei n.º 9.983, de 14 de julho de 2000 foi responsável por alterar o Código Penal, adicionando, dentre outros, os delitos de inserção de dados falsos em sistemas de informações e de modificação ou alteração não autorizada de sistema de informações (artigos 313-A e 313-B).

Por esta razão, a legislação significou avanço na temática, ao passo que surgiu no momento de transição, no setor público, dos dados escritos para os virtuais, representando uma resposta legal à responsabilidade dos servidores públicos que passaram pelo processo de adequação para a utilização dos sistemas de informações e dos bancos de dados. Este fenômeno fez surgir, portanto, a necessidade de tutela destes bens jurídicos por parte do Estado, ocasionando a criação dos tipos penais mencionados, a fim de responsabilizar as condutas desviantes.

Posteriormente, foi aprovada pelo Congresso Nacional a Lei n.º 12.737, de 30 de novembro de 2012 – popularmente conhecida como Lei Carolina Dieckmann –, que promoveu alterações no Código Penal e possibilitou a tipificação de delitos virtuais como a invasão de dispositivo informático, a interrupção ou perturbação de serviços informáticos, telemáticos, entre outros.

Ainda que se reconheça a inovação trazida pela Lei Carolina Dieckmann à legislação brasileira, esta se mostrou insuficiente, possuindo termos que careciam de precisão técnica, a exemplo do que seria considerado “mecanismo de segurança”, trecho presente no artigo 154-A, essencial para o entendimento da configuração do tipo penal. Frente a isto, aponta-se a barreira da aplicabilidade relacionada aos usuários que não possuíssem as tais ferramentas nos seus equipamentos, independentemente do motivo, que restariam desprotegidos pela falta de existência do elemento de “violação indevida de mecanismo de segurança”,

necessário para a caracterização do tipo penal, conforme presente no caput, o que comprometeria a segurança jurídica desta parcela da população.

Situações como esta, portanto, fizeram surgir a necessidade de aprovação de novas normas jurídicas, a fim de que fossem definidas as expressões técnicas a serem utilizadas nos dispositivos legais e, por consequência, que uma maior quantidade de práticas delituosas cometidas virtualmente pudesse ser punida, maximizando a proteção legal oferecida.

Nesse sentido, pode-se apontar, seguindo a esteira temporal, a Lei n.º 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet, cuja relevância justifica-se por disciplinar o uso da Internet no território brasileiro, estabelecendo os princípios, garantias, direitos e deveres referentes à temática. (BRASIL, 2014, *online*). Acerca disso, posiciona-se Siqueira (2017, p. 126):

> A lei do Marco Civil foi criada para suprir as lacunas no sistema jurídico em relação aos crimes virtuais, num primeiro momento tratando dos fundamentos, conceitos para sua interpretação e objetivos que o norteiam, além de enumerar os direitos dos usuários, tratar de assunto polêmicos como por exemplo a solicitação de histórico de registros, a atuação do poder público perante os crimes virtuais e por último garante o exercício do direito do cidadão de usufruir da internet de modo individual e coletivo estando devidamente protegido.

Considerado um grande progresso legislativo do ordenamento brasileiro frente às inovações tecnológicas, possui o objetivo de garantir um contato com a internet pautado na qualidade e segurança oferecidas aos usuários. Entretanto, embora seja reconhecida a relevância deste texto normativo, críticas ao seu teor podem ser observadas, em especial quanto à característica de que suas normas, pois:

> não abrangem todo o campo de atuação dos criminosos da internet, ficando ainda algumas lacunas supridas por outras legislações, como por exemplo, a regulamentação usada para as compras feitas pela internet em que o comprador necessita de algum tipo de auxílio judiciário, seja por devolução do produto porque não gostou ou por algum defeito, regulamenta-se pelo código do consumidor. (SIQUEIRA, 2017, p. 126).

Assim, em momento posterior, observada a necessidade da criação de um texto legal com maior especificidade da temática, surge a Lei n.º 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), criada com o propósito de servir “como um sistema baseado em etiquetas, permissões ou proibições para o uso de informações específicas, que leva na devida conta os riscos objetivos potencializados pelo tratamento informatizado das informações pessoais”. (DONEDA, 2019, p. 50).

Dessa forma, a LGPD regulou o modo de tratamento dos dados dos usuários, alterando os artigos 7 e 16 do Marco Civil da Internet, buscando uma maior atualização legislativa. Nesse sentido, atentou para a existência de registros de alta importância, os chamados dados pessoais sensíveis, assim conhecidos por se referirem diretamente à pessoa do usuário, dentre os quais podem ser citados o nome completo, CPF, RG, nacionalidade, estado civil, profissão e escolaridade (CASTRO, 2019).

Portanto, ainda que a Lei Geral de Proteção de Dados não possua caráter criminal, em sua essência, as disposições nela encontradas são de grande importância na seara penal, ao passo que servem de referência para a valoração dos dados expostos no meio virtual e das formas pelas quais deve ocorrer o tratamento, armazenamento e transporte destes registros. Estas informações, por sua vez, são de grande serventia ao legislador, que pode utilizá-las de parâmetro quando da tipificação e determinação da pena de condutas delituosas relacionadas aos dados sensíveis.

4.1 Das recentes alterações legislativas no âmbito criminal

Ao compreender as inúmeras possibilidades de utilização da Internet, pode-se observar, de modo proporcional, as diversas situações capazes de expor os usuários e, principalmente, seus dados, a riscos de difícil reparação. Nesse sentido, a vastidão da rede mundial de computadores permite o surgimento constante de condutas que, por sua complexidade e periculosidade, não encontram amparo suficiente nas legislações gerais e, portanto, necessitam recorrer ao Direito Penal como *ultima ratio*, a fim de que sejam responsabilizados os agentes ativos pelos prejuízos causados aos bens jurídicos dos particulares tendo como meio a Internet.

Nesse sentido, passa-se à análise as recentes alterações legislativas no âmbito criminal, a exemplo da Lei n.º 13.964 de 2019, que aperfeiçoou a legislação penal e processual penal, Lei n.º 13.968 de 2019, que alterou o crime de incitação ao suicídio, Lei n.º 14.132 de 2021 — Lei de Stalking, Lei n.º 14.155 de 2021, que promoveu alterações nos delitos de violação de dispositivo informático, furto e estelionato, cometidos de forma eletrônica ou pela Internet e da Emenda Constitucional 115, que incluiu a proteção de dados pessoais no rol de direitos e

garantias fundamentais. Assim, a fim de compreender suas implicações, a exposição encontra-se organizada conforme o critério cronológico.

4.1.1 Lei n.º 13.964 de 2019 — Aperfeiçoamento da legislação penal e processual penal

Criada com o objetivo de aperfeiçoar a legislação penal e processual penal, a Lei n.º 13.964, de 24 de dezembro de 2019 trouxe alterações pontuais, que visavam uma maior atualização das disposições legais. Dentre estas, destaca-se a redação dada ao parágrafo segundo do artigo 141 do Código Penal, segundo o qual “se o crime é cometido ou divulgado em quaisquer modalidades das redes sociais da rede mundial de computadores, aplica-se em triplo a pena” (BRASIL, 2019).

A redação, posta nas disposições gerais referentes ao Capítulo dos crimes contra a honra, aponta no sentido de que a punição devida nos casos em que ocorra a exposição das informações imputadas à vítima tendo como meio de propagação a Internet e suas redes deve ser majorada. Assim, observa-se a atualização da proteção dos bens jurídicos já existentes, tornando proporcional a responsabilização frente ao maior grau de reprovabilidade da conduta e extensão dos efeitos, considerando que, pela propagação facilitada, as informações atingem um maior número de indivíduos.

4.1.2 Lei n.º 13.968 de 2019 — Alteração no crime de incitação ao suicídio

Responsável por modificar o crime de incitação ao suicídio, a Lei n.º 13.968, de 26 de dezembro de 2019 incluiu as condutas de induzimento, instigação ou auxílio ao suicídio ou à automutilação no artigo 122 do Código Penal. Ainda, quando da disposição dos seus parágrafos, atentou para as situações em que tais condutas sejam realizadas tendo como meio o ambiente virtual. Nesse sentido, dispõe:

> Art. 122. Induzir ou instigar alguém a suicidar-se ou a praticar automutilação ou prestar-lhe auxílio material para que o faça:
>
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos.
>
> [...]
>
> § 4º A pena é aumentada até o dobro se a conduta é realizada por meio da rede de computadores, de rede social ou transmitida em tempo real.

> § 5º Aumenta-se a pena em metade se o agente é líder ou coordenador de grupo ou de rede virtual.

Assim, ainda que não haja a criação de um tipo penal novo, tendo em vista a adaptação de uma previsão já existente, tornando-a mais ampla, os impactos resultantes da possibilidade de punição acentuada quando da realização dos delitos através da rede de computadores apontam no sentido da compreensão legal das consequências mais gravosas inerentes ao compartilhamento pela Internet.

4.1.3 Lei n.º 14.132 de 2021 — Lei de Stalking

Originada a partir do Projeto de Lei n.º 1.369 de 2019, de autoria da senadora Leila Barros (PSB-DF), a Lei n.º 14.132, de 31 de março de 2021 alterou o Código Penal ao tipificar o delito de perseguição, incluindo-o no texto do artigo 147-A, que dispõe:

> Art. 147-A. Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade. (BRASIL, 2021).

Esta previsão foi a responsável por popularizar a referida legislação conforme a nomenclatura "*Lei de Stalking*", sendo esta última uma palavra pertencente à língua inglesa, que se refere à atitude de importunar repetidamente outra pessoa, aproximando-se e perseguindo-a, geralmente de modo sorrateiro. Nesse sentido, aponta Marlene Matos *et al.* (2011, p. 20) que o *stalking* é "um padrão de comportamentos de assédio persistente, que representa formas diversas de comunicação, contacto, vigilância e monitorização de uma pessoa-alvo por parte de outra — o/a *stalker*".

Ressalta-se que, em momento anterior, a previsão legal inerente a esta conduta possibilitava o seu enquadramento somente como contravenção penal, conforme disposição do artigo 65 da Lei de Contravenções Penais — Decreto-Lei n.º 3.688, de 3 de outubro de 1941 — recebendo a denominação de "Perturbação da tranquilidade alheia". No entanto, com a sanção da Lei de *Stalking*, resta revogada a referida disposição legal, sendo esta conduta atualmente enquadrada no crime de perseguição.

Assim, ao dispor em seu caput sobre a possibilidade de que a perseguição ocorra "por qualquer meio", a legislação em comento apresenta-se como importante

inovação jurídica, ao passo que compreende o *cyberstalking*, conceituado como sendo a perseguição que possui como meio de execução a internet. A esse respeito:

> O *cyberstalking*, por sua vez, tornou-se relevante no cenário mundial com a popularização da tecnologia e por sua adoção generalizada nos mais diversos segmentos da vida dos cidadãos, seja em casa, no lazer, no trabalho ou demais núcleos de pertencimento (DE CASTRO; SYDOW, 2017, p. 13).

Ainda, expõe a Senadora Leila Barros (2021, *online*):

> O avanço das tecnologias e o uso em massa das redes sociais trouxeram novas formas de crimes. [...] O aperfeiçoamento do Código Penal era necessário para dar mais segurança às vítimas de um crime que muitas vezes começa on-line e migra para a perseguição física. [...] Com a nova legislação poderemos agora mensurar com precisão os casos que existem no Brasil e que os criminosos não fiquem impunes como estava ocorrendo.

Justifica-se, portanto, a relevância desta previsão legal, ao passo que prevê a realização da perseguição por diversos meios, incluindo a internet, exigindo, de todo modo, que a conduta seja reiterada para que ocorra a consumação. Por fim, atenta-se para o fato de que as penas previstas não excluem as sanções correspondentes à violência resultante da conduta, conforme previsão do art. 147-A, §2º, característica essa capaz de promover uma maior proteção às vítimas.

4.1.4 Lei n.º 14.155 de 2021 — Alterações nos delitos de violação de dispositivo informático, furto e estelionato, cometidos de forma eletrônica ou pela Internet

Sancionada em 27 de maio de 2021, a Lei n.º 14.155, de 2021, trouxe alterações ao texto do Código Penal, tornando mais graves os crimes de violação de dispositivo informático, furto e estelionato, cometidos de forma eletrônica ou por meio da internet, além de acrescentar ao Código de Processo Penal a definição da competência nas modalidades de estelionato. (BRASIL, 2021).

Dentre as modificações, pode-se destacar o aumento da pena para o crime de invasão de aparelhos de informática para obtenção, modificação e destruição de dados, quando da invasão resultar prejuízo econômico. Na redação original, o artigo 154-A do Código Penal possuía como pena detenção de 3 (três) meses a 1 (um) ano, e multa, tendo a Lei 14.155/2021 dado redação que prevê pena de reclusão, de 1 (um) a 4 (quatro) anos, e multa.

Portanto, percebe-se que este delito perdeu a sua classificação como de menor potencial ofensivo, natureza esta que, na redação anterior, somente seria perdida nos casos qualificados segundo o §3º (se como resultado fosse obtido conteúdo de comunicações privadas ou controle remoto não autorizado do dispositivo). Ademais, quanto à previsão do *caput*, a legislação atual sofreu alterações que promoveram uma ampliação da incidência do tipo penal, pois:

> Nota-se, primeiramente, que o tipo penal não exige mais que o dispositivo informático seja de propriedade alheia, bastando que esteja sendo utilizado por outra pessoa. Dessa forma, ainda que o agente seja o proprietário do aparelho, pode cometer o crime se esse aparelho estiver sendo utilizado por alguém. E, por coerência, a lei agora faz referência à falta de autorização expressa ou tácita do usuário do dispositivo, não mais do titular.
>
> Além disso, o tipo não pressupõe mais que haja violação indevida de mecanismo de segurança. Antes, a violação era um meio necessário para que o invasor respondesse criminalmente pela invasão com a finalidade de obter, adulterar ou destruir dados ou informações ou de instalar vulnerabilidades no aparelho. (CUNHA, 2021, *online*).

Diante do exposto, torna-se possível compreender a importância desta legislação, ao passo que trouxe penas mais severas aos crimes cometidos através do meio virtual, além das demais previsões que reformam a legislação, de modo a adequá-la à realidade cada vez mais ligada à tecnologia. Por meio destas alterações, o texto legal adequa-se para lidar melhor com as práticas delituosas que surgem de modo proporcional à difusão tecnológica social, com vistas a minimizar a prática dos crimes cibernéticos, através de uma punição mais gravosa aos sujeitos ativos.

4.1.5 Emenda Constitucional 115 — Inclusão da proteção de dados pessoais no rol de direitos e garantias fundamentais

Seguindo a tendência de inclusão de matérias relacionadas à intersecção entre direito e tecnologia, no dia 10 de fevereiro de 2022 foi promulgada a Emenda Constitucional de n.º 115, responsável por alterar a Constituição Federal de modo a incluir a proteção de dados pessoais entre os direitos e garantias fundamentais. Ademais, fixou competência privativa da União para legislar sobre a proteção e o tratamento de dados pessoais.

Esta temática, no tempo da promulgação do texto da Carta Magna, não apresentava igual relevância e implicações tais como podem ser observadas

atualmente. Por essa razão, com a revolução tecnológica e a inserção de dispositivos eletrônicos na rotina mundial, o tema tornou-se assunto recorrente nos tribunais, pelas problemáticas que, relacionando-se com a informatização de dados e com a própria segurança do cidadão e usuário da rede, acabaram por levar à judicialização de demandas que exigiam do texto legal uma especificidade no tratamento dos registros eletrônicos, chamados de dados.

Nesse sentido, anteriormente à Emenda n.º 115, visando proporcionar segurança jurídica e uniformidade de entendimento, o Supremo Tribunal Federal já possuía pronunciamentos (ADI 6387, 6388, 6389 e 6390) que identificavam a proteção de dados pessoais como um direito fundamental implícito no texto constitucional, fundamentando tal afirmação nos incisos X e XII, do artigo 5º da Constituição.

Dessa forma, restando comprovada a importância e repercussão do tema, tem-se justificada a inclusão da proteção dos dados na Constituição Federal, de modo explícito, consolidando o posicionamento do STF e oferecendo arcabouço legal para o aprofundamento da tutela dos registros eletrônicos.

4.2 Das disposições esparsas

Além das previsões contidas nas leis alvo de reflexão anterior, podem ser encontradas disposições em leis específicas, cujas condutas perpetradas no ambiente comum também possuem formas de execução através de ambiente virtual.

Como exemplo disso, cita-se o parágrafo 2º do artigo 20 da Lei n.º 7.716, de 5 de janeiro de 1989, responsável por majorar a pena aplicada nos casos de prática, indução ou incitação da discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional, “se qualquer dos crimes previstos no caput é cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza”, com pena de reclusão de dois a cinco anos e multa. (BRASIL, 1989, *online*).

Ainda, torna-se válido mencionar o artigo 241-A da Lei n.º 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), responsável por tipificar a pornografia infantil, incluindo os meios informáticos, conforme a redação a seguir:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
>
> § 1 o Nas mesmas penas incorre quem:
>
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
>
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
>
> § 2 o As condutas tipificadas nos incisos I e II do § 1 o deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo. (BRASIL, 1990, *online*).

Como último exemplo, pode ser encontrada a disposição do que se considera *cyberbullying*, presente no parágrafo único do artigo 2º da Lei n.º 13.185, de 6 de novembro de 2015, cuja redação apresenta que:

> Há intimidação sistemática na rede mundial de computadores (*cyberbullying*), quando se usarem os instrumentos que lhe são próprios para depreciar, incitar a violência, adulterar fotos e dados pessoais com o intuito de criar meios de constrangimento psicossocial. (BRASIL, 2015, *online*)

Diante do exposto, torna-se possível compreender a existência de disposições legais encontradas em legislações específicas, cujo objetivo aponta no sentido de promover a adequação das formas de consumação de condutas ao ambiente virtual. Classificam-se, portanto, como crimes virtuais impróprios, entendidos como delitos “já tipificados, que são realizados agora com a utilização do computador e da rede, utilizando o sistema de informática e seus componentes como mais um meio para a realização do crime” (ALMEIDA *et al*., 2015, p. 225).

4.3 Da (in)suficiência legislativa e da (des)necessidade de criação de legislação específica

Diante do exposto, torna-se possível reconhecer que a revolução tecnológica e social promovidas pela Internet trouxeram desafios ao Direito, uma vez que as novas situações e condutas que afetam bens jurídicos foram percebidas e exigiram da legislação uma adaptação rápida. Ainda assim, o Brasil está bem atrasado em termos de legislação penal informática (JESUS; MILAGRES, 2016, p. 70), ao passo que as regulamentações encontram-se distribuídas por dispositivos legais gerais e específicos, tornando dificultoso o acesso às regras.

Por este motivo, encontra-se na doutrina a discussão acerca da necessidade da criação de uma legislação específica, cujo objetivo seria reunir em um código separado a maior parte dos artigos referentes aos delitos virtuais, facilitando a sua utilização e alcance pelos operadores do Direito, autoridades competentes e membros da sociedade. De toda forma, a corrente contrária defende não haver a necessidade de que seja criada uma legislação, tendo em vista que, segundo seus defensores, a maioria dos crimes informáticos já são previstos no Código Penal brasileiro.

Corrobora com tal pensamento Alexandre Jean Daoun (2011, p. 2, *apud* JESUS; MILAGRES, 2016, p. 63), ao afirmar que:

> Daí a crítica a essa compulsividade de legislar, de criar lei penal para isso, para aquilo, porque o Direito Penal é o instrumento mais drástico que se tem. [...] Então, para não se perder a credibilidade, é direito penal mínimo. E no ambiente virtual, 95% das relações que se tem já são disciplinadas na legislação penal. Não há por que criar e falar tanto em legislação penal específica.

Neste cenário, a partir da observação da promulgação da Lei n.º 12.737, de 30 de novembro de 2012, Lei n.º 13.964, de 24 de dezembro de 2019, Lei n.º 13.968, de 26 de dezembro de 2019, Lei n.º 14.132, de 2021 (Lei de Stalking) e da Lei n.º 14.155, de 27 de maio de 2021, a tendência que pode ser observada é de que o legislador criminal brasileiro encaminha-se no sentido de promover alterações pontuais no Código Penal e no Código de Processo Penal, ao invés de apostar na criação uma lei específica voltada para a regulamentação dos crimes cibernéticos.

De todo modo, ainda que seja reconhecida a evolução na previsão de delitos cometidos tendo como meio o ambiente virtual, deve-se analisar a sua eficácia, característica essa definida por Afonso da Silva (2007, p. 66) como:

> (...) Eficácia é a capacidade de atingir objetivos previamente fixados como metas. Tratando-se de normas jurídicas, a eficácia consiste na capacidade de atingir os objetivos nela traduzidos, que vêm a ser, em última análise, realizar os ditames jurídicos objetivados pelo legislador.
>
> (...) Uma norma pode ter eficácia jurídica sem ser socialmente eficaz, isto é, pode gerar efeitos jurídicos, como, por exemplo, o de revogar normas anteriores, e não ser efetivamente cumprida no plano social.

Nesse cenário, apresenta-se como fonte de informação o repositório da Central Nacional de Denúncias de Crimes Cibernéticos, resultado de uma parceria entre a Organização Não Governamental Safernet Brasil com órgãos como o Ministério Público Federal (MPF), Senado Federal e Polícia Federal. A partir da

leitura dos gráficos e análise das informações, percebe-se que o Brasil ocupa o 5º (quinto) lugar no ranking de países que mais hospedam endereços eletrônicos distintos denunciados no ano de 2021[1].

Ainda, encontram-se em destaque as denúncias relacionadas a pornografia infantil, registrando aumento de 3,65% em relação ao ano de 2020, e ao neonazismo, com a recepção de 14.476 denúncias anônimas no ano de 2021, o que aponta para um crescimento de 60,7% em comparação ao registrado no ano anterior. Por essa razão, citando os dados obtidos pela parceria em comento, justificou-se a aprovação do Projeto de Lei n.º 2.496/2019, pela Comissão de Direitos Humanos e Minorias da Câmara dos Deputados, com vistas a ampliar o rol de crimes de ódio praticados ou planejados através do meio digital, cuja competência para investigação é da Polícia Federal[2].

Portanto, ao analisar as previsões legais brasileiras expostas durante a realização do estudo, tornou-se possível identificar alterações pontuais que encaminham-se no sentido de promover a adaptação de tipos penais existentes, conforme sua execução através da internet. De todo modo, surge a percepção da necessidade de constante atualização da legislação, a fim de que o arcabouço legal brasileiro possua os instrumentos necessários para o combate efetivo de tais delitos, ao passo que, na falta de previsão específica, o caminho que recebe preferência é o de adequação do caso em concreto às disposições legais com maior proximidade.

Assim, pela falta de direcionamento próprio, algumas penas podem ser desproporcionais aos reflexos que o cometimento das infrações possuem, considerando-se brandas, levando em consideração o alcance das ferramentas digitais. Esta análise, portanto, aponta para o reconhecimento de certo grau de ineficácia das legislações disponíveis, ao passo que os dados estatísticos demonstram a necessidade de um endurecimento legal que vise a diminuição dos delitos cometidos no ambiente cibernético.

Por essas motivações, torna-se válido atentar para a necessidade de um trabalho conjunto entre os órgãos estatais e a população, esta última agindo de modo a obter conhecimento acerca dos riscos inerentes ao meio virtual, visando

---

[1] Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos. **Datasafer**. Disponível em: <https://indicadores.safernet.org.br/>. Acesso em: 23 maio 2022.

[2] Comissão aprova projeto que amplia relação de crimes de ódio na internet investigados pela PF. **Câmara dos Deputados.** Disponível em: < https://www.camara.leg.br/noticias/822518-comissao-aprova-projeto-que-amplia-relacao-de-crimes-de-odio-na-internet-investigados-pela-pf/>. Acesso em: 23 maio 2022.

mitigar sua vulnerabilidade. Por sua vez, o Estado atuaria de modo repressivo, oferecendo um arcabouço legal estruturado, seja pela criação de leis específicas ou adequação das existentes, com penas proporcionais aos cibercrimes e tipos penais específicos, adequados às alternativas digitais, garantindo a punibilidade dos delitos e, consequentemente, promovendo uma maior segurança jurídica.

5 METODOLOGIA

A presente pesquisa fez uso do método dedutivo, tendo em vista que partiu de uma análise geral para uma hipótese particular, chegando-se a uma conclusão por via lógica, a fim de promover uma análise do objeto de estudo. Ainda, possuiu caráter exploratório, ao passo que se volta para a descoberta de novas informações sobre o tema, buscando conhecê-lo com mais profundidade, esclarecendo-o (MUNARETTO, *et al*., 2013, p. 10). Para além disso, caracteriza-se como sendo descritiva, pois levanta informações sobre situações específicas e relacionadas para proporcionar a visualização de uma totalidade (GIL, 2017, p. 28).

Por essa razão, quanto ao meio de investigação, a pesquisa apresenta-se como bibliográfica, conceituada como aquela cujo objetivo principal é o aprofundamento em determinado assunto, de modo a promover uma explicação do objeto de estudo, pela análise de teorias a seu respeito. Nesse sentido:

> A pesquisa bibliográfica é então feita com o intuito de levantar um conhecimento disponível sobre teorias, a fim de analisar, produzir ou explicar um objetivo sendo investigado. A pesquisa bibliográfica visa então analisar as principais teorias de um tema, e pode ser realizada com diferentes finalidades. (CHIARA, KAIMEN, et al., 2008, *online*).

A coleta de dados foi possível a partir de levantamento bibliográfico, utilizando como fontes artigos, dissertações, teses científicas e livros que tratam acerca dos crimes cibernéticos, além das legislações existentes que se relacionam ao tema. Foram utilizadas, portanto, as técnicas histórica e conceitual, visando o estudo dos crimes cibernéticos a partir da compreensão de seu surgimento, atrelado ao advento da internet, da evolução histórica dos equipamentos tecnológicos e da relação entre a sociedade e a tecnologia. Por fim, a exposição das legislações e alterações alvo do estudo organizou-se conforme o critério cronológico.

6 CONCLUSÃO

A rede mundial de computadores estreitou as relações entre seres humanos e tecnologias, de modo que podem ser observados benefícios diversos, a exemplo da facilitação de fenômenos como a globalização e comunicação em grande escada. De todo modo, ao passo que determinados processos tornaram-se de fácil execução, novos desafios foram impostos, especialmente no que diz respeito à segurança dos usuários da Internet.

Em decorrência das fragilidades existentes, tais como a dificuldade de identificação dos usuários e a possibilidade de modificação das informações como a localização do dispositivo utilizado, o meio virtual tornou-se campo para a prática de condutas delituosas. Fundamental, pois, que estas práticas sejam pauta de discussão, tendo em vista a ampla utilização das redes no cenário mundial, sendo expressivo o número de usuários em potencial risco de tornarem-se vítimas.

Portanto, reconhecendo a crescente utilização da rede mundial de computadores pela comunidade global, o presente estudo buscou estudar os impactos jurídicos oriundos da revolução tecnológica que relacionam-se aos crimes cibernéticos, identificando a legislação existente sobre o tema no ordenamento jurídico brasileiro. Para isto, analisou as principais alterações legislativas relacionadas às novas tecnologias, pontuando as normas definidoras de tipos penais enquadrados nos crimes cibernéticos, investigando o arcabouço legal existente.

Verificou-se, pois, a existência de tipos penais relacionados à temática na Lei n.º 9.983, de 14 de julho de 2000, Lei n.º 12.737, de 30 de novembro de 2012, Lei n.º 13.964, de 24 de dezembro de 2019, Lei n.º 13.968, de 26 de dezembro de 2019, Lei n.º 14.132, de 2021 (Lei de *Stalking*), Lei n.º 14.155, de 27 de maio de 2021, além de previsões gerais e regulamentadoras, a exemplo da Lei n.º 12.965, de 23 de abril de 2014 (Marco Civil da Internet) e da Lei n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).

Ademais, foram encontradas disposições em legislações esparsas e, de modo mais recente, a inclusão da proteção de dados pessoais no rol dos direitos e garantias fundamentais, no texto constitucional, pela Emenda Constitucional n.º 115. Assim, comprovou-se a relevância do tema, tendo em vista que a previsão expressa no texto da Carta Magna oferece bases para o aprofundamento da proteção dos

registros eletrônicos nas normas infraconstitucionais e proporciona maior segurança jurídica.

Nesse sentido, torna-se válido atentar para o contraste existente entre a extensão temporal dos processos legislativos, normalmente duradouros, e a rapidez de atualização informática, que permite a multiplicação das possibilidades criminais no meio virtual, exigindo do direito, portanto, atualização constante. Assim, a tendência da reforma de diplomas legais existentes, observada durante o desenvolvimento do estudo, apresenta benefícios neste sentido, ao passo que a consagração das alterações pontuais nos dispositivos possibilita uma resposta estatal mais rápida, se comparada com o processo de estudo, criação e sanção de leis específicas voltadas ao ambiente computacional.

No Brasil, considerando as modificações legislativas analisadas, pode-se observar uma evolução dos diplomas legais no acompanhamento das transformações tecnológicas. De todo modo, ainda se nota certa carência de leis específicas relacionadas aos crimes cibernéticos, dotadas de precisão técnica e que aliem o conhecimento jurídico ao domínio das ferramentas informacionais, de modo a combater a execução de condutas prejudiciais aos usuários.

Dessa maneira, cabe pontuar que a adequação legal, ainda que essencial, não promove, por si só, a resolução desta problemática tão complexa, existindo uma necessidade de que o órgão estatal garanta o funcionamento de suas instituições que lidam diretamente com os casos delituosos no âmbito virtual, tais como as Polícias Civis e Federal, além do Ministério Público e o Poder Judiciário. Torna-se válida, portanto, a oferta de treinamento específico aos servidores, para lidarem com as causas que exigem conhecimento interdisciplinar, além da operação dos textos legais.

Por fim, mostra-se oportuno que o Estado trabalhe aliado à comunidade, promovendo ensinamentos de etiqueta digital e disseminando informações acerca da segurança no mundo virtual, visando a conscientização dos usuários da rede, a fim de que identifiquem com maior facilidade condutas delituosas e riscos de exposição indevida de dados pessoais, especialmente os sensíveis, agindo de forma preventiva.

REFERÊNCIAS

ABREU, Karen Cristina Kraemer. **História e usos da Internet**. BOCC – Biblioteca Online de Ciências da Comunicação, p. 1-9, 2009. Disponível em: <http://www.bocc.ubi.pt/_esp/autor.php?codautor=1625>. Acesso em: 03 jan. 2022.

ALMEIDA, Jessica de Jesus et al. **Crimes Cibernéticos**. Caderno de Graduação – Ciências Humanas e Sociais – UNIT. Sergipe, v. 2, n. 3, p. 215 – 236, 2015. Disponível em: < https://periodicos.set.edu.br/cadernohumanas/article/view/2013>. Acesso em: 24 maio 2022.

ASSUNÇÃO, Ana Paula Souza. **Crimes virtuais**, 2018. Disponível em: <http://repositorio.aee.edu.br/jspui/handle/aee/538>. Acesso em: 15 jan. 2022.

BEZERRA, Clayton da Silva; AGNOLETTO, Giovani Celso. **Combate ao crime cibernético, doutrina e prática**. A visão do delegado de polícia. 1. ed. Rio de Janeiro: Mallet Editora, 2020.

BRASIL. **Lei nº 7.716, de 5 de janeiro de 1989**. Define os crimes resultantes de preconceito de raça ou de cor. Brasília, DF: Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l7716.htm>. Acesso em: 20 jan. 2022.

_____. **Lei nº 8.069 de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente. Brasília, DF: Presidência da República. Disponível em: <http://www.planalto.gov.br/Ccivil_03/leis/L8069.htm>. Acesso em: 20 jan. 2022.

_____. **Lei 9.609 de 19 de fevereiro de 1998**. Brasília, DF: Presidência da República. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l9609.htm> Acesso em: 19 jan. 2022.

_____. **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: Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 15 jan. 2022.

_____. **Lei nº 13.185, de 6 de novembro de 2015**. Institui o Programa de Combate à Intimidação Sistemática (Bullying). Brasília, DF: Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13185.htm>. Acesso em: 16 jan. 2022.

_____. **Lei nº 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Brasília, DF: Presidência da República. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm>. Acesso em: 11 jul. 2022.

_____. **Lei nº 13.968, de 26 de dezembro de 2019**. Brasília, DF: Presidência da República. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13968.htm>. Acesso em: 11 jul. 2022.

_____. **Lei nº 14.132, de 31 de março de 2021**. Brasília, DF: Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14132.htm>. Acesso em: 24 maio 2022.

_____. **Lei nº 14.155, de 27 de maio de 2021**. Brasília, DF: Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm>. Acesso em: 22 maio 2022.

CASTRO, B. B. **Direito Digital na Era da Internet Das Coisas — O Direito à Privacidade e o Sancionamento da Lei Geral de Proteção de Dados Pessoais**. 2019. Disponível em: <https://ambitojuridico.com.br/cadernos/direito-civil/direito-digital-na-era-da-internet-das-coisas-o-direito-a-privacidade-e-o-sancionamento-da-lei-geral-de-protecao-de-dados-pessoais/>. Acesso em: 21 maio 2022.

CHARA, Ivone Di; KAIMEN, Maria Júlia; CARELLI, Ana Esmeralda. **Normas de documentação aplicadas à área da saúde**. Rio de Janeiro: Ed. E-papers, 2008.

Comissão aprova projeto que amplia relação de crimes de ódio na internet investigados pela PF. **Câmara dos Deputados**. Disponível em: < https://www.camara.leg.br/noticias/822518-comissao-aprova-projeto-que-amplia-relacao-de-crimes-de-odio-na-internet-investigados-pela-pf/>. Acesso em: 23 maio 2022.

CUNHA, Rogério Sanches. **Lei 14.155/21 e os crimes de fraude digital**: primeiras impressões e reflexos no CP e no CPP. Meu site jurídico. 2021. Disponível em: <https://meusitejuridico.editorajuspodivm.com.br/2021/05/28/lei-14-15521-e-os-crimes-de-fraude-digital-primeiras-impressoes-e-reflexos-no-cp-e-no-cpp/>. Acesso em: 23 maio 2022.

DE CASTRO, Ana Lara Camargo; SYDOW, Spencer Toth. **Stalking e cyberstalking: obsessão, internet, amedrontamento**. [Coleção Cybercrimes]. Belo Horizonte: Editora D'Plácido, 2017. Disponível em: <https://cdnv2.moovin.com.br/livrariadplacido/imagens/files/manuais/247_stalking-e-cyberstalking-obsessao-internet-amedrontamento.pdf>. Acesso em: 24 maio 2022.

DONEDA, Danilo. **Da privacidade a proteção de dados pessoais**. 2. Ed., São Paulo: Revista dos Tribunais, 2019.

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

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 6. Ed. São Paulo: Atlas, 2008. Disponível em: <https://ayanrafael.files.wordpress.com/2011/08/gil-a-c-mc3a9todos-e-tc3a9cnicas-de-pesquisa-social.pdf>. Acesso em: 20 jan. 2022.

Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos. **Datasafer**. Disponível em: <https://indicadores.safernet.org.br/>. Acesso em: 23 maio 2022.

JARDIM, Renato César. O direito como fator de transformação social. **Revista Amagis Jurídica**, n. 6, p. 153-164, 2019. Disponível em:

<https://revista.amagis.com.br/index.php/amagis-juridica/article/view/168>. Acesso em: 25 maio 2022.

Lei que criminaliza stalking é sancionada. Senado Federal. Senado Notícias, 05 de abril de 2021. Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/04/05/lei-que-criminaliza-stalking-e-sancionada>. Acesso em: 24 maio 2022.

MATOS, Marlene et al. **Inquérito de Vitimação por Stalking. Relatório de Investigação**. Grupo de Investigação sobre Stalking em Portugal. 2011, 78 p. Disponível em: <http://repositorium.sdum.uminho.pt/handle/1822/31235>. Acesso em: 24 maio 2022.

MUNARETTO, Lorimar Francisco; CORRÊA, Hamilton Luiz; DA CUNHA, Júlio Araújo Carneiro. Um estudo sobre as características do método Delphi e de grupo focal, como técnicas na obtenção de dados em pesquisas exploratórias. **Revista de Administração da Universidade Federal de Santa Maria**, v. 6, n. 1, p. 9-24, 2013. Disponível em: <http://www.redalyc.org/articulo.oa?id=273428927002>. Acesso em: 20 jan. 2022.

OLIVEIRA, Beatriz Martins de; WALDMAN, Ricardo Libel. Conceitos de informação e sociedade da informação e sua importância. **Meritum, Revista de Direito da Universidade FUMEC**, 2020. Disponível em: <https://doi.org/10.46560/meritum.v15i4.7965>. Acesso em: 18 jan. 2022.

PINHEIRO, Patrícia Peck. **Direito digital**. 5. ed. rev. atual. e ampl., São Paulo: Saraiva, 2013.

PINHEIRO, Patrícia Peck. Regulamentação da Web. **Cadernos Adenauer XV**, Rio de Janeiro, n. 4, p. 33-44, out/2014. Disponível em: <http://www.kas.de/wf/doc/16471-1442-5-30.pdf>. Acesso em: 21 dez. 2021.

REALE, Miguel. **Filosofia do direito**. 19. Ed. Rio de Janeiro: Jorge Zahar, 1996.

REIS, A. N. R.; VIANA, G. D. **Crimes Virtuais: legislações insuficientes ou ineficiência das autoridades competentes?**. Revista Ibero-Americana de Humanidades, Ciências e Educação. v. 7 n. 10, 2021. Disponível em: <https://doi.org/10.51891/rease.v7i10.2684>. Acesso em: 08 jul. 2022.

SILVA, José Afonso. **Aplicabilidade das Normas Constitucionais**. Ed. Malheiros. 8. Ed. 2012.

SILVA, José Carlos Teixeira da. Tecnologia: novas abordagens, conceitos, dimensões e gestão. **Production**, v. 13, p. 50-63, 2003. Disponível em: <https://doi.org/10.1590/S0103-65132003000100005>. Acesso em: 21 dez. 2021.

SILVA, Marco Antônio Duarte. **Considerações sobre a interpretação e aplicação da lei penal**. 2013. Disponível em: < https://www.jurisway.org.br/v2/dhall.asp?id_dh=12203>. Acesso em: 25 maio 2022.

SIQUEIRA, Marcela Scheuer et al. **Crimes virtuais e a legislação brasileira. (Re)Pensando o Direito** – Rev. do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo. v. 7, n. 13, 2017. Disponível em: <http://local.cnecsan.edu.br/revista/index.php/direito/article/view/468>. Acesso em: 01 fev. 2022.

SOUZA, Gilson Sidney Amâncio de. Breves considerações sobre a lei nº 11.106, de 28.03.2005, que alterou o Código Penal. **IBCCRIM**. 2005. Disponível em: <https://www.ibccrim.org.br/noticias/exibir/3900/>. Acesso em: 25 maio 2022.