VII ENCONTRO VIRTUAL DO CONPEDI

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO II

LUIZ FERNANDO BELLINETTI

SÉRGIO HENRIQUES ZANDONA FREITAS

PABLO MARTINS BERNARDI COELHO

D597

Direito penal, processo penal e constituição II [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Luiz Fernando Bellinetti; Pablo Martins Bernardi Coelho; Sérgio Henriques Zandona Freitas – Florianópolis: CONPEDI, 2024.

Inclui bibliografia
ISBN: 978-65-5648-994-0
Modo de acesso: www.conpedi.org.br em publicações
Tema: A pesquisa jurídica na perspectiva da transdisciplinaridade

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito penal. 3. Processo penal. VII Encontro Virtual do CONPEDI (1: 2024 : Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

VII ENCONTRO VIRTUAL DO CONPEDI

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO II

Apresentação

É com muita satisfação que apresentamos o Grupo de Trabalho e Pesquisa (GT) de Artigos denominado “DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO II” do VII ENCONTRO VIRTUAL DO CONPEDI (VII EVC), com a temática “A pesquisa jurídica na perspectiva da transdisciplinaridade”, promovido pelo Conselho Nacional de Pesquisa e Pós-graduação em Direito (CONPEDI), Sociedade Científica do Direito no Brasil, com patrocínio da Faculdade de Direito de Franca e da Universidade UNIGRANRIO - Afya, e apoio do Portucalense Institute For Legal Research - IJP e da Faculdad de Derecho da Universidad de la República Uruguay, em evento realizado entre os dias 24 e 28 de junho de 2024, de forma telepresencial, com a utilização da Plataforma Conferência Web RNP.

Assim, o Grupo de Trabalho recebeu 17 artigos que abordam diferentes aspectos relacionados ao Direito material e processual penal, devendo ser ressaltado que todos os trabalhos direta ou indiretamente trataram da qualidade da prestação da justiça, bem como os avanços e desafios do Direito na contemporaneidade brasileira e mundial. A apresentação dos trabalhos foi dividida em três blocos, não havendo especificidades temáticas em cada um deles.

Destaca-se os títulos dos textos apresentados: Políticas públicas de moradia destinadas às mulheres vítimas de violência doméstica; A aplicação do princípio da insignificância no âmbito da justiça estadual em face dos crimes contra a ordem tributária; Uma análise sobre o processo de modernização do direito penal: do colapso do modelo penal de matriz liberal à investigação sobre o processamento do direito penal moderno; A identificação do perfil genético de condenados: considerações à luz da perspectiva da proteção de dados; O uso de algemas no ordenamento jurídico brasileiro: uma revisão legislativa e jurisprudencial sobre o tema; O reconhecimento do estado de coisas inconstitucional no sistema prisional e as decisões estruturais do poder judiciário brasileiro; Desafios e perspectivas nas decisões do TJRS sobre violência patrimonial contra a mulher: uma reflexão à luz da Lei Maria da Penha; Revista íntima aos visitantes do estabelecimento prisional e a (i)licitude da prova; Violência doméstica e justiça restaurativa: limites e possibilidades de sua aplicabilidade; Crime e espetacularização: o sensacionalismo da cobertura midiática e a responsabilização jurídica dos meios de comunicação no Brasil; Crimes digitais: engenharia social uma arma nas mãos dos cibercriminosos; O direito à saúde nos municípios e a descriminalização da utilização do canabidiol para fins medicinais; Os cadastros públicos de criminosos condenados para a

prevenção da pedofilia; Julgamento com a perspectiva de gênero e fixação de indenização mínima no processo penal: Tema 983 do STJ nos tribunais do Rio de Janeiro, Goiás e Amazonas; Um enfoque multidimensional sobre o tráfico de drogas e as organizações criminosas no Brasil: uma análise das implicações sociais, econômicas e jurídicas das drogas na contemporaneidade; Poderes instrutórios do juiz no processo penal brasileiro: análise a partir da perspectiva de Luigi Ferrajoli na obra "direito e razão"; Lei 14.811 de 2024: aspectos gerais e, finalmente, a tipificação dos crimes de bullying e o cyberbullying.

Em linhas gerais, os textos reunidos traduzem discursos interdisciplinares maduros e profícuos, reflexo de pesquisas e pesquisadores de todas as regiões do país.

Na oportunidade, os Organizadores prestam sua homenagem e agradecimento a todos que contribuíram para esta louvável iniciativa do Conselho Nacional de Pesquisa e Pós-Graduação em Direito (CONPEDI), das instituições parceiras e, em especial, a todos os autores que participaram da presente coletânea de publicação, com destaque pelo comprometimento e seriedade demonstrados nas pesquisas realizadas e na elaboração dos textos de excelência.

Convida-se a uma leitura prazerosa dos artigos apresentados de forma dinâmica e comprometida com a formação de pensamento crítico, a possibilitar a construção de um Direito voltado à concretização de preceitos insculpidos no Estado Democrático Constitucional de Direito.

29 de junho de 2024.

Professor Dr. Luiz Fernando Bellinetti

luizbel@uol.com.br

Professor Dr. Pablo Martins Bernardi Coelho

pablo.coelho@uemg.br

Professor Dr. Sérgio Henriques Zandona Freitas

sergiohzf@fumec.br

CRIMES DIGITAIS: ENGENHARIA SOCIAL UMA ARMA NAS MÃOS DOS CIBERCRIMINOSOS

DIGITAL CRIMES: SOCIAL ENGINEERING A WEAPON IN THE HANDS OF CYBERCRIMINALS

Simone Gomes Leal [1]
Caio Sperandeo De Macedo

Resumo

Com todas as novidades em matéria de tecnologia, em especial as inovações dos meios de comunicação através da internet, que vêm impactando a sociedade em sua totalidade, fazendo surgir novos fatos jurídicos, e, consequentemente, novas perspectivas para a aplicação normativas, o objetivo do presente estudo é esclarecer as características dos mecanismos utilizados pelos hackers e cyberstalkers, na prática de crimes virtuais, utilizando-se da Engenharia Social, para enganar as vítimas. A evolução tecnológica na Sociedade da Informação está proporcionando diversos benefícios para a sociedade, diminuindo a distância entre as pessoas de forma global e mantendo-as hiperconectadas, facilitando a comunicação e promovendo o convívio em uma verdadeira aldeia virtual inserida no ciberespaço. Porém, na mesma medida em que as novas tecnologias oferecem recursos para o desenvolvimento social, também proporcionam oportunidades para a criminalidade informática, como a chamada engenharia social, que facilita a prática de crimes ao explorar a vulnerabilidade das pessoas. Dessa forma, visando o combate eficaz com base no ordenamento jurídico brasileiro e na Convenção de Budapeste. O estudo científico utilizou o método dedutivo, analisando a doutrina e a legislação pertinentes ao tema.

Palavras-chave: Crimes cibernéticos, Avanço tecnológico, Engenharia social, Sociedade da informação, Convenção de budapeste

Abstract/Resumen/Résumé

With all the new developments in technology, especially the innovations in the means of communication via the internet, which have been impacting society as a whole, giving rise to new legal facts, and, consequently, new perspectives for the application of regulations, the objective of This study aims to clarify the characteristics of the mechanisms used by hackers and cyberstalkers, in the practice of virtual crimes, using Social Engineering, to deceive victims. Technological evolution in the Information Society is providing several benefits to society, reducing the distance between people globally and keeping them hyperconnected, facilitating communication and promoting coexistence in a true virtual village inserted in cyberspace. However, to the same extent that new technologies offer resources for social development, they also provide opportunities for computer crime, such as so-called social

[1] Mestranda em Direito da Sociedade da Informação pelo Centro Universitário das Faculdades Metropolitanas (FMU). Pós-Graduada em Direito Civil Aplicado pela Universidade Católica de Minas Gerais (Puc Minas). Advogada.

engineering, which facilitates the commission of crimes by exploiting people's vulnerability. In this way, aiming at effective combat based on the Brazilian legal system and the Budapest Convention. The scientific study used the deductive method, analyzing the doctrine and legislation relevant to the topic.

Keywords/Palabras-claves/Mots-clés: Cybercrime, Technological advancement, Social engineering, Information society, Budapest convention

1 INTRODUÇÃO

Os crimes digitais, também conhecidos como crimes cibernéticos ou cibercrimes, são todas as formas de atividades proibidas pelo ordenamento jurídico e praticadas de maneira ilícita com o auxílio de dispositivos informáticos, conectados ou não à internet. O advento da Sociedade da Informação, juntamente com o avanço tecnológico, tem facilitado a prática desses crimes, tornando as pessoas cada vez mais vulneráveis e necessitando, portanto, de um amplo amparo legal. Isso lança ao poder judiciário o desafio de aplicar penas justas e ao legislativo a responsabilidade de elaborar leis mais firmes e eficientes.

Neste contexto, o presente artigo propõe-se a analisar a prática dos crimes cibernéticos. Serão apresentados conceitos fundamentais e suas classificações, buscando esclarecer melhor o crime cibernético e examinando os mecanismos que garantem os direitos e regulamentam o uso da internet, além da aplicação das sanções diante do cenário de vulnerabilidade do ambiente virtual, especialmente com a utilização da Engenharia Social, na qual os criminosos empregam artifícios para enganar suas vítimas. Diante desse contexto social, o problema de pesquisa que pode ser formulado é o seguinte questionamento: Como combater a Engenharia Social diante das inovações tecnológicas?

A Engenharia social é utilizada por criminosos para manipular pessoas a fim de obter informações confidenciais. Uma das formas de proteção é que as pessoas devem tomar o máximo de cuidado com senhas e estar atentas a e-mails e mensagens maliciosas. Outra abordagem importante é o enrijecimento das penalidades para quem comete esses crimes. Nesse sentido, nosso ordenamento jurídico já é amplamente amparado pela Constituição Federal em questões envolvendo crimes cibernéticos, principalmente em relação à violação dos direitos fundamentais dos cidadãos. Invocamos o Constitucionalismo Digital, que visa garantir os direitos fundamentais na Sociedade da Informação.

O constitucionalismo digital abrange desde a proteção dos dados dos cidadãos, por meio da Lei Geral de Proteção de Dados (LGPD) - Lei n. º 13.709, de 14 de agosto de 2018, até o Marco Civil da Internet - Lei n. º 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, além de diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios nessa área. Existem também outras leis

infraconstitucionais lançadas visando a proteção das atividades realizadas no ambiente virtual e por meio de dispositivos informáticos, como a Lei n. º 12.737/12, que tipifica os delitos informáticos, e a Lei n.º 14.132/2021, que tipifica o cyberstalking.

No âmbito internacional, o Brasil agora é signatário da Convenção de Budapeste, promulgada por meio do Decreto n. º 11.491, de 12 de abril de 2023, que tem como objetivo estabelecer uma unidade protetiva contra crimes cibernéticos. Essa convenção visa facilitar a cooperação entre os países para identificar cibercriminosos e realizar operações conjuntas. Portanto, a forma mais adequada de combater a engenharia social é por meio dos dispositivos legais e regulatórios já existentes e em desenvolvimento, tanto no âmbito nacional quanto internacional.

Logo, o objetivo do presente artigo é fornecer esclarecimentos sobre o cenário atual dos crimes cibernéticos, especialmente diante da vulnerabilidade encontrada no ambiente virtual, com foco na engenharia social. Destaca-se que, para se prevenir contra tais crimes, além do respaldo legal, é fundamental manter-se informado e cauteloso para evitar cair em golpes perpetrados no ambiente digital. A importância deste estudo reside no aumento exponencial dos crimes praticados no ambiente digital, os quais exploram a vulnerabilidade das pessoas. A pesquisa utilizou o método científico dedutivo, apoiando-se na legislação pertinente e na revisão bibliográfica sobre o tema em estudo.

2 O AVANÇO TECNOLÓGICO E AS VULNERABILIDADES NA SOCIEDADE DA INFORMAÇÃO

A era pós-industrial, que teve início nos anos de 1950, representa uma diferenciação significativa em relação ao período anterior, especialmente no setor de serviços, pois provocou mudanças substanciais na indústria e na produção agrícola, entre outros aspectos. Posteriormente, emerge a era pós-moderna, caracterizada pela globalização, na qual a população está cada vez mais informatizada, promovendo o fluxo acelerado de conhecimento, cultura e criatividade. Sobre esse tema, Jean-François Lyotard discorre detalhadamente.

> O cenário Pós-Moderno é essencialmente cibernético-informático-e informacional [...] No entanto, ocenário pós-moderno, com sua "vocação" informática e informacional, "investte" sobre essa concepção do saber científico. Como muito bem notou Alfred N. Whitehead, o século XX vem sendo o palco de uma descoberta fundamental. Descobriu que as fontes das fontes chama-se informação. (Lyotard, 2021, p. 10-11)

O cenário pós-moderno é marcado por fortes mudanças na sociedade, abrangendo aspectos econômicos, políticos, culturais e sociais, com avanços tecnológicos cada vez mais frequentes. O primeiro computador surgiu em 1945, concebido pela mente e mãos de Alan Turing em colaboração com a equipe do projeto ENIAC (Electronic Numerical Integrator and Computer), sob a liderança de John von Neumann, que já havia trabalhado com Turing. Eles inovaram com uma máquina chamada "Electronic Numerical Integrator and Computer" (Turing, 2019, p. 96).

Alan Turing, matemático e criptógrafo inglês, ficou conhecido como o "pai da computação", especialmente pelo desenvolvimento da "Bombe", uma criação de Turing e sua equipe que conseguiu decifrar a criptografia alemã, considerada indecifrável na época (Turing, 2019, p. 74). Para que toda essa tecnologia começasse a funcionar efetivamente, era necessário pensar na internet e, consequentemente, no ciberespaço.

‘

> A origem da internet está intrinsecamente ligada ao e-mail e, como tantas coisas no desenvolvimento da computação, à necessidade das autoridades militares. A Agência de Projetos de Pesquisa Avançada (ARPA), na sigla em inglês do Departamento de Defesa dos Estados Unidos, foi criada em resposta ao lançamento do satélite Sputinik em 1957que financiou muitos projetos transformadores, numa grande variedade de áreas de pesquisa. A pesquisa relacionada a computação, foi realizada principalmente por universidades famosas do país, como Harvard e o MIT [...] com o tempo a rede chamada ARPA NET, ficou menos associada aos projetos da ARPA e se transformou em um meio de comunicação mais geral. (Turing, 2019, p. 146-147).

Hoje, ocorre a interconexão das redes por meio de dispositivos digitais conectados à internet em todo o mundo, em tempo real, permitindo aos usuários compartilhar não apenas conversas casuais, mas também documentos, reuniões de negócios, exposições culturais e notícias em tempo real. Além disso, há a hiperconexão, uma vez que todos estão conectados o tempo todo, de forma global, colocando o ciberespaço como protagonista na Sociedade da Informação.

Segundo Tiago Cappi Janini e Simone Leal,

> O ciberespaço, portanto, permite novos tipos de relações interpessoais, impensáveis tempos atrás. O progresso da internet provoca profundas alterações nos relacionamentos sociais. Surgem diferentes maneiras de conviver, de interagir, de organizar-se em comunidades, implicando desafios ao mundo “real”. As relações econômicas, sociais, políticas, culturais e jurídicas são transformadas e precisam ser repensadas. O sistema jurídico, então, convive com comportamentos humanos não previstos, necessitando regulamentá-los. Institutos jurídicos concretizam-se no ambiente virtual (Janini; Leal, 2023, p. 307).

O ciberespaço se torna o centro para o desenvolvimento das atividades humanas na Sociedade da Informação, facilitando a informação e a comunicação entre as pessoas. Esse cenário é impulsionado pelo avanço tecnológico e pela descoberta da internet, que possibilitam a interação nesse ambiente digital. Sobre o ciberespaço, Pierre Lévy destaca que

> Além da exteriorização, um outro caráter é frequentemente associado virtualização a passagem do interior ao exterior e do exterior ao interior. Esse efeito “Moebus” declina-se em vários registros: o das relações entre privado e público, próprio e comum, subjetivo e objetivo, mapa território, autor e leitor etc. [...] gora uma imagem, essa ideia pode ser ilustrada com o caso já evocado da virtualização de empresa.[...]. O trabalhador clássico tinha sua mesa de trabalho. Em troca o participante da sua empresa virtual compartilha um certo número de recursos imobiliário, mobiliários e programas com outros empregados. (Lévy, 1996. 24).

Portanto, o ciberespaço hoje é um espaço no qual nossas informações são inseridas por meio de recursos informáticos e tecnológicos, utilizando a internet para alcançar muitas pessoas em locais diversos e distantes, em tempo real. Ou seja, conseguimos alcançar pessoas globalmente, formando uma verdadeira "comunidade digital" na qual as pessoas buscam interagir com outras que compartilham objetivos semelhantes. Emerson Malheiro discorre que

> A comunidade virtual é uma coletividade cibernética que constitui elos relacionais por meio de comunicação à distância e se caracteriza pela reunião de pessoas com interesses gerais, que comutam conhecimentos, notícias, mensagens e experiências em um ambiente virtual, com a utilização de tecnologias de informação e comunicação, com a finalidade de desenvolver a capacidade cognitiva e criativa de cada integrante, ou simplesmente promover o entretenimento de seus membros. (Malheiro, 2016, p. 99).

A Sociedade da Informação surge nesse contexto do avanço das telecomunicações e da informática nos anos 70, apresentando potencial para o processamento de informações de uma forma que antes não possível. A partir dos anos 80, ocorreram avanços tecnológicos significativos, desencadeando de fato uma verdadeira revolução na vida das pessoas, que precisam se adaptar às novidades tecnológicas. Sobre essa temática, Manuel Castells discorre que

> Assim, até certo ponto, a disponibilidade de novas tecnologias construídas como um sistema na década de 1970 foi base fundamental para o processo reestruturação socioeconômica dos anos de 1980. E e a utilização dessas tecnologias na década de 1980 condicionou, em grande parte seus usos e trajetórias na década de 1990. (Castells, 2021, p. 115)

A revolução tecnológica da informação, também conhecida como a "Quarta Revolução Industrial", trouxe muitas descobertas para nossa sociedade. O desenvolvimento tecnológico

abrange avanços significativos na economia, medicina, interação digital, biotecnologia, energia renovável, entre outros. James Magno A. Farias aponta

> A quarta Revolução Industrial não diz respeito apenas a sistemas e máquinas inteligentes e conectadas. Seu escopo é muito mais amplo. Onda de novas descobertas ocorrem simultaneamente em áreas que vão desde o sequenciamento genético até a nanotecnologia, das energias renováveis a computação quântica. O que torna a quarta revolução industrial fundamentalmente diferentes das anteriores é a fusão dessas tecnologias e interação entre domínios físicos, digitais e biológicos. (Farias, 2023, p. 53)

Nesse cenário de expansão do desenvolvimento tecnológico, a sociedade se adapta às mudanças constantes, buscando soluções para compreender a nova dinâmica dos acontecimentos jurídicos. A globalização, juntamente com a consequente sociedade da informação, caracteriza-se pela expansão política, econômica e cultural. A internet e as novas tecnologias desempenham um papel fundamental nesse desenvolvimento global, elevando a economia global a outro patamar.

As pessoas passam a fazer amizades, negócios e até relações de trabalho pela internet. Especialmente, as pessoas conhecem outras com o objetivo de estreitar relações, o que pode gerar problemas de alta complexidade. Estamos convivendo em comunidades virtuais, intermediadas por sistemas de computadores e pela rede de internet. Dessa forma, as pessoas se reúnem com base em objetivos comuns (Lévy, 2005, p. 20).

No entanto, o avanço tecnológico também proporciona facilidades para aqueles que buscam cometer crimes. Esses recursos tecnológicos fornecem equipamentos para as organizações criminosas e oferecem recursos para pessoas mal-intencionadas ludibriarem e enganarem com o objetivo de obter vantagens em detrimento de terceiros. Ou seja, os recursos tecnológicos estão enriquecendo os métodos de operação, especialmente no que diz respeito às ferramentas para o cometimento de crimes, na atual sociedade da informação. Para Manuel Castells:

> simultaneamente, as atividades criminosas e organizações ao estilo da máfia, de todo o mundo, também se tornaram globais e informacionais, propiciando os meios para o encorajamento de hiperatividade mental desejo proibido, juntamente com toda e qualquer forma de negócio ilícito procurados por nossa sociedade de armas sofisticadas a carne humana. (Castells, 2021, p. 62).

Dessa forma, à medida que ocorreram mudanças significativas na sociedade devido ao avanço tecnológico, surgiram recursos que equipam organizações criminosas e fornecem ferramentas para alimentar a criatividade daqueles que cometem crimes. Isso coloca as pessoas em

um cenário de vulnerabilidade, exigindo que o legislador acompanhe essa dinamicidade tecnológica por meio da formulação de leis especiais. Essas leis devem tipificar os novos tipos penais que surgem no atual contexto social, sempre em consonância com os princípios constitucionais.

3 CONSTITUCIONALISMO DIGITAL E SOCIEDADE DA INFORMAÇÃO

A Constituição Federal é a base do ordenamento jurídico brasileiro; toda e qualquer norma deve estar em conformidade com a Constituição. Com o advento da Sociedade da Informação, surgem na sociedade novos desafios e complexidades que precisam ser enfrentados pelo legislador. Enquanto novas normas infralegais não forem lançadas no ordenamento jurídico ou apresentarem lacunas, cabe à Constituição Federal preencher as falhas presentes nos textos infralegais. Isso é feito por meio do Constitucionalismo Digital, que se responsabiliza por preencher essas lacunas utilizando os preceitos fundamentais constitucionais, visando aplicar os direitos fundamentais do cidadão.

Gilmar Ferreira Mendes e Victor Oliveira Fernandes realizam estudos voltados para esclarecer o Constitucionalismo Digital.

> A expressão "Constitucionalismo Digital" foi utilizada nos estudos iniciais sobre o tema para se referir a um movimento constitucional de defesa da limitação do poder privado de atores da internet, em oposição à ideia de limitação do poder político estatal. Em trabalhos mais recente, porém, a terminologia passou a ser utilizada como um guarda-chuva que abrange as mais diversas inciativas jurídicas e políticas, estatais e não-estatais, voltadas à afirmação de direitos fundamentais na internet[...] (Mendes; Fernandes, 2020, p. 4)

As garantias constitucionais são fundamentais para todo cidadão e para o ordenamento jurídico. Mesmo que surjam leis especiais ou novas regulamentações, estas devem se submeter à Constituição e ter seu conteúdo amparado e resguardado por ela. Nesse contexto, Newton Lucca, Adalberto Simão Filho e Cintia Rosa Pereira de Lima pontuam sobre o tema.

> O Avanço da informática fez que a sociedade reclamasse um sistema mais efetivo de proteção de sua intimidade, em função da fragilidade dos instrumentos de garantias existentes. A partir da promulgação da Constituição da república de 1988, houve o reconhecimento de um direito geral à intimidade e à vida privada explicitado por disposições que atualizam o sistema de proteção dos direitos fundamentais, sobretudo do direito à intimidade (....) (Lucca; Simão Filho; Lima, 2015, p. 310).

O Constitucionalismo Brasileiro vem enfrentando desafios significativos diante dos avanços tecnológicos, buscando adaptar-se aos novos aspectos normativos da contemporaneidade, com a preocupação primordial de proteger os direitos fundamentais. Nesse sentido, utiliza-se o Constitucionalismo Digital como base para garantir os direitos fundamentais do cidadão. Anízio Pires Galvão Filho e colaboradores propõem que o Constitucionalismo Digital na atualidade representa um "modelo de Constitucionalismo moderno".

> [..] A adaptação do modelo de constitucionalismo moderno aos problemas oriundos do universo digital ainda se mostra como meio mais eficiente para a promoção e a proteção dos direitos na sociedade contemporânea. Assim, o chamado constitucionalismo digital representa uma forma de chamar a atenção para violações a direito que reclamam melhores respostas, bem como, um importante passo para quem sabe, em um futuro não muito distante, significativa reconfiguração do modelo constitucionalismo moderno. (Galvão Filho; Motta; Paiva, 2023, p. 4)

Dessa forma, o constitucionalismo digital tem a missão de adequar os novos direitos fundamentais ao texto constitucional. Na formação do constitucionalismo moderno, são afirmados os direitos de liberdade do cidadão (liberdades individuais), tendo o Estado a função de limitar o exercício do poder (Galvao Filho; Motta; Paulo, 2023).

Assim, o Constitucionalismo Digital visa proteger os direitos fundamentais do cidadão no atual cenário das inovações tecnológicas. Está inserido no contexto da sociedade tecnológica e informacional. O conceito inicialmente denominado constitucionalismo informacional por Fitzgerald e "constitucionalismo constitutivo" por Berman acabou sendo chamado de "constitucionalismo digital", denominação que também foi adotada por estudiosos subsequentes (Celeste, 2021, p. 71).

Diante disso, o constitucionalismo digital é uma forma de adaptar o ordenamento jurídico para amparar condutas e novos fatos jurídicos que surgem nesse novo cenário social, proporcionado pelas novas Tecnologias da Informação e Comunicação (TICs). Para isso, o legislador inovou com a Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº. 13.709, de 14 de agosto de 2018, que trata de um dos direitos fundamentais relacionados aos dados pessoais e sensíveis das pessoas.

Sobre essa temática, Victor Hugo Pereira Gonçalves aduz que

> A proteção de dados pessoais é um direito fundamental, contra majoritário, do indivíduo, em face do excesso de informação obtidos pelo estado e por empresas, que pela LGPD, agora são controladores, ou operadores, públicos ou privados. E, ao mesmo tempo, é um

> direito de autodeterminação do ser humano e está interligado, a dignidade humana no seu aspecto virtualizado. (Gonçalves, 2022, p. 92).

Já o Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014, tem como finalidade estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Portanto, a Constituição Federal, no contexto da teoria do constitucionalismo digital e do convívio no ciberespaço, tem estrutura para amparar amplamente os novos direitos fundamentais inerentes ao cidadão que interage nesse novo ambiente virtual.

Dessa forma, as leis especiais lançadas no ordenamento jurídico visando amparar os crimes digitais, como é o caso da Lei nº 12.737/12, também são abrangidas pelo Constitucionalismo Digital, uma vez que a proteção não se limita a uma lei ou fatos específicos. Isso inclui os crimes digitais, a Lei Geral de Proteção de Dados, o Marco Civil da Internet, entre outros institutos jurídicos lançados no ordenamento jurídico visando a proteção dos novos direitos.

4 CRIMES CIBERNÉTICOS

O crime cibernético, também conhecido como cibercrime ou crimes digitais, refere-se à atividade ilícita praticada por meio da invasão de dispositivos informáticos, estejam eles conectados à internet ou não. A internet facilita algumas práticas de cibercrimes, pois muitos desses crimes são cometidos por meio de redes sociais, e-mails, aplicativos como WhatsApp, entre outros, possibilitando a prática de diversos delitos por meio desses dispositivos.

De acordo com Emerson Wendt e Higor Vinicius Nogueira Jorge, crime cibernético é definido como: "Os delitos praticados por intermédio de dispositivos informáticos (como computadores, notebooks, celulares etc.), conectados ou não à internet" (Wendt; Jorge, 2021, p. 14). O crime cibernético está tipificado no Artigo 154-A da Lei nº 12.737, de 30 de novembro de 2012, conhecida como Lei Carolina Dieckmann.

> O Artigo 154-A Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: (Barroso; Araújo Junior, 2016, p. 596)

A Lei Carolina Dieckmann, que combate os crimes cibernéticos, completou 10 anos em dezembro de 2023. Esta lei carrega uma grande responsabilidade, pois é considerada o marco

inicial para a proteção dos dados pessoais no contexto do combate aos crimes cibernéticos. Até o presente momento, vem sendo avaliada pelos juristas da área como bem-sucedida. Sobre esse tema, Emerson Wendt traz pontos relevantes.

> A Lei 12.737/2012, surgiu no Direito Brasileiro em um período de discussões sobre a regulamentação civil da internet, aprovada em 2014 através da Lei 12. 965/2014 "o denominado, "Marco Civil da Internet" (MCI). [...] Antes da edição do MCI, destacaram que deveríamos cobrar do poder público uma atenção prioritária em relação a defesa da vida privada, e da intimidade diante de qualquer tipo de intromissão, pública ou particular. O contexto e recorte metodológico, dos autores foi a regulação e proteção penal. Essa foi, aliás, em face dos intensos debates sobre o PL 84/99 ("Projeto de Lei Azeredo") que criminalizava condutas praticadas na / através da internet e foi chamada de "AI 5 Digital". (Wendt, 2015, p. 52)

Dessa forma, os crimes cibernéticos são tipificados e suas penas serão aplicadas de acordo com os novos parâmetros legais estipulados na referida lei.

> Artigo. 154-A Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Art. 154-B os crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos[1].

Portanto, para que haja a tipificação de um crime cibernético, o sujeito deve ter praticado as condutas elencadas nos artigos supramencionados, tais como a invasão de sistema eletrônico, digital e similares, visando prejudicar terceiros por meio da destruição ou adulteração, estando o sistema conectado à rede de computadores ou não. Destaca-se ainda que o crime cibernético possui duas modalidades: próprio (puro) e impróprio (impuro), as quais serão exemplificadas nos tópicos seguintes.

[1] Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos."

O art. 1º da Lei nº 12.737/2012, dispõe sobre a tipificação de delitos informáticos. Essa questão da tipificação da conduta é complexa, uma vez que, para que configure um crime cibernético, é necessário que haja a invasão do dispositivo informático. Logo, se o criminoso obteve previamente a autorização do proprietário do aparelho e mesmo assim consegue adulterar algum documento ou acessar dados confidenciais, a conduta será considerada atípica. Nesse caso, ele poderá responder na esfera cível, caso cause algum dano material ou moral à vítima.

Os autores Emerson Wendt e Higor Vinícius Nogueira Jorge aduzem:

> As Ações jurídicas atípicas" são aquelas condutas. Práticas por intermédio de dispositivos informáticos, que causas algum transtorno e/ ou prejuízo para a vítima, porém não existe uma previsão penal, ou seja: o indivíduo que invade o computador de um conhecido sem o objetivo de obter adulterar, ou destruir dados ou informações não será indiciado, nem preso, pois esses fatos não são criminosos, por não se adequarem ao art. 154-A do Código Penal (nova redação dada pela lei n.º 14. 155/2021). Por outro lado, o causador do transtorno pode ser responsabilizado na esfera civil, como por exemplo ser condenado a pagar indenização em virtude de danos morais / materiais produzidos. (Wendt; Jorge, 2021, p. 15)

Porém, se o hacker obtém informações da vítima por meio de artifícios fraudulentos para acessar seu computador, celular, etc., e comete algum crime, estará configurando a fraude prevista no Artigo 171 do Código Penal. Recentemente, essa prática foi acrescentada como estelionato qualificado ou "fraude eletrônica". Emerson Wendt e Higor Vinícius Nogueira Jorge apontam essa consideração.

> Temos a previsão de vários tipos de fraudes eletrônicas no direito penal brasileiro. O estelionato é a principal delas e está previsto no art. 171 do Código Pena, incluído a tipificação recente do "estelionato eletrônico ". Mas também temos várias outras possibilidades relacionadas as fraudes, como por exemplo, fraude processual, fraude empresarial, fraude em seguros, fraude no sistema financeiro, fraude tributária e fraudes no sistema eleitoral. (Wendt; Jorge, 2021, p. 58)

As fraudes eletrônicas, portanto, são praticadas por meio de informações fornecidas pelas próprias vítimas, muitas vezes induzidas pelas artimanhas da engenharia social.

4.1 CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

Os crimes cibernéticos têm a internet como uma forte aliada para suas inovações delitivas, sendo facilitadas diversas modalidades criminosas. Para compreender cada uma delas, é necessário

entender que o crime cibernético é classificado em crimes cibernéticos puros/próprios e impuros/impróprios. Alessandro Gonsalves Barreto e Beatriz Silveira Brasil fazem uma classificação dos crimes cibernéticos como puros ou próprios, e impuros ou impróprios. Segundo eles, os crimes cibernéticos impuros ou impróprios são aqueles que...

> São aqueles onde o dispositivo tecnológico é utilizado como meio para a prática do delito, propiciando a sua execução a sua execução ou o seu resultado. Aqui apenas o veículo em que o crime é praticado é que envolve tecnologia, sendo perfeitamente adequadas diversas figuras típicas previstas no Código Penal Brasileiro ou em leis penais especiais. (Barreto; Brasil, 2016, p. 18)

Portanto, ao falarmos de crimes cibernéticos, não podemos deixar de observar que um crime "comum" tipificado no Código Penal, quando praticado através da internet ou de dispositivos informáticos, também pode ser considerado um crime cibernético.

4.1.1 CRIMES CIBENÉTICOS PUROS

Alessandro Gonsalves Barreto e Beatriz Silveira Brasil fazem uma classificação dos crimes cibernéticos em puros ou próprios, impuros ou impróprios. Segundo eles, os crimes cibernéticos puros ou próprios,

> São aqueles que os sistemas informáticos, bancos de dados, arquivos ou terminais (computadores, smartfhones, tablets, por exemplo), são atacados por criminosos com a intenção da prática criminosa, normalmente após identificar vulnerabilidades, seja por meio de programas maliciosos, ou ainda por engenharia social. (Golpista engana a vítima, fazendo com que forneça informações pessoais e/ ou estratégicas). Aqui o dispositivo informatizado e/ou seu conteúdo é o alvo dos criminosos. (Barreto; Brasil, 2016, p. 17)

Um exemplo de crime cibernético puro são as fraudes, em que o cibercriminoso se utiliza do dispositivo informático para instalar programas maliciosos, com o objetivo de extrair informações para poder lesar a vítima.

> Para Norton Symantec, esse tipo de crime informático apresenta como principais características: geralmente acontece apenas uma vez, (por exemplo, quando a vítima baixa o Cavalo de Tróia que instala um programa de registro de digitação no computador); frequentemente é facilitado por softwares de atividades ilegais; e muitos casos, aproveita-se de falhas ou vulnerabilidades de segurança. (Barreto; Brasil, 2016, p. 17)

Portanto, quando falarmos em crimes cibernéticos puros ou próprios, podemos associar as fraudes cibernéticas, em que o criminoso se utiliza de recursos informáticos para implantar artifícios maliciosos no computador da vítima.

4.1.2 CRIMES CIBENÉTICOS IMPUROS

Os crimes cibernéticos impuros ou impróprios são aqueles em que o hacker utiliza dispositivos informáticos como meio para atingir seus objetivos. Um exemplo é o crime de Cyberstalking, no qual os cyberstalkers (perseguidores virtuais) se utilizam de dispositivos informáticos, como celulares, para cometer o crime através do envio de mensagens de WhatsApp, em redes sociais via mensagem direta, entre outros. No entanto, o crime não se configura apenas com a invasão de dispositivos; o Cyberstalking envolve a perseguição reiterada à vítima com o objetivo de afetar seu psicológico, causando medo, angústia, etc.

"Via de regra, a vítima do crime de stalking se sente ameaçada psicologicamente ou fisicamente pelo criminoso. O uso das redes sociais possibilitou o uso da tecnologia para praticar a perseguição, resultando no denominado Cyberstalking" (Lopes, 2023, p. 38). Assim, o crime possui sua tipificação específica, e a utilização dos dispositivos informáticos serve como meio facilitador para o cometimento do crime.

Quanto a Barbara Fernandes dos Santos,

> O Stalking consubstancia um tipo de criminalidade que pode ser potencializada e acentuada pelo uso da internet, sendo uma forma de perseguição que prejudica a paz do visando e que pode culminar em diversos crimes de maior ou menor gravidade. Nos casos de perseguição, um dos meios usados pelo stalker pode ser justamente a internet, o denominado Cyberstalking. (Santos, 2017, p. 137).

Dessa forma, o Cyberstalking enquadra-se como um crime cibernético impróprio ou impuro, no qual o dispositivo informático não é o alvo do crime, mas sim o meio utilizado para sua realização. Um exemplo semelhante é o furto previsto no Artigo 155, § 4º, B do Código Penal, que trata do furto cometido mediante fraude ou por meio de dispositivo eletrônico.[2]

[2] Artigo 155 do Decreto Lei nº 2.848 de 07 de dezembro de 1940, **§ 4º**-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo. (Incluído pela Lei nº 14.155, de 2021)

5 ENGENHARIA SOCIAL UMA ARMA PARA OS HACKERS

Já percebemos a influência das novas Tecnologias da Informação e Comunicação (TICs) para o desenvolvimento da atual Sociedade da Informação. Reconhecemos os inúmeros benefícios que essas novas tecnologias proporcionaram em diferentes setores da vida das pessoas. No entanto, através dos recursos tecnológicos, também se abre um caminho para a prática criminosa, pois pessoas mal-intencionadas encontram nos avanços das TICs e na vulnerabilidade das pessoas a oportunidade de cometer crimes.

Nesse contexto, está inserida a Engenharia Social, que é uma técnica utilizada por criminosos virtuais para enganar e ludibriar suas vítimas, aproveitando-se dos avanços das novas tecnologias da informação e comunicação. Portanto, pode-se entender a engenharia social como diversas formas de manipulação para obter informações das vítimas. "É a utilização de um conjunto de técnicas destinadas a ludibriar a vítima de forma que ela acredite nas informações prestadas e seja convencida a fornecer dados pessoais, realizar alguma tarefa ou executar um aplicativo" (Wendt; Jorge, 2021, p. 16).

Não é possível especificar ou determinar todas as técnicas utilizadas para a prática de crimes por meio das artimanhas da Engenharia Social, nem afirmar que ela é um fenômeno exclusivo da sociedade atual, uma vez que são utilizadas todas as técnicas que um indivíduo encontrar em determinada situação e com determinada pessoa, explorando suas vulnerabilidades. No entanto, os avanços tecnológicos facilitam a utilização da engenharia social.

> A Engenharia Social é uma arte que existe desde tempos imemoriais, mas encontrou um novo terreno fértil na era digital. Ela se baseia na exploração das fraquezas humanas, como confiança, curiosidade e desejo de ajudar, para obter acesso a informações privilegiadas ou induzir as pessoas a tomar ações específicas. (Maximiliano, 2023, p. 2)

Podemos usar como exemplo a situação em que os criminosos entram em contato fazendo-se passar pelo gerente de uma instituição financeira, com o objetivo de obter informações pessoais da vítima. Eles podem pedir, por exemplo, que a vítima instale um aplicativo no celular sob o pretexto de precisarem trocar a senha, mas na verdade conseguem acessar seus dados e praticar o golpe. Atualmente, é muito comum essa prática envolvendo golpes de PIX.

Emerson Wendt e Higor Vinícius Nogueira Jorge abordam esse tipo de estratégia criminosa.

> Cabe destacar, que geralmente os criminosos simulam fazer parte de determinada instituição confiável, como bancos, sites de grandes lojas, órgãos do governo ou outros órgãos públicos, para que a vítima confie nos falsos dados apresentados, o que, na verdade, será a isca para que sejam fornecidas as referidas informações. (Wendt; Jorge, 2021, p. 16)

Enquanto certas ameaças cibernéticas se concentram na vulnerabilidade de uma rede ou servidor, a engenharia social concentra-se na vulnerabilidade da vítima. Como podemos nos proteger da engenharia social? Na verdade, dado que os criminosos buscam vulnerabilidades tanto em redes sociais como diretamente falando com a vítima através de e-mail ou até mesmo pelo telefone celular, é difícil afirmar que existe uma solução eficaz. No entanto, as pessoas devem se informar o máximo possível e evitar fornecer dados pessoais que possam ser usados pelos criminosos. Segundo Wendt e Jorge (2021, p. 16-17), "O que é bem complicado é que não existe uma fórmula definitiva para se defender dos ataques dos hackers que se utilizam da engenharia social para acessar nossos dados. Eles exploram as fragilidades e vulnerabilidades humanas".

Dessa forma, para nos protegermos de possíveis golpes, é essencial ficar atento a situações que despertem dúvidas sobre determinadas transações, como transações bancárias baseadas em informações duvidosas. Nunca compartilhe informações pessoais a menos que tenha absoluta certeza de que está lidando com a pessoa ou instituição correta, pois a engenharia social se baseia na enganação e manipulação de indivíduos visando obter acesso ou divulgar informações e dados.

6 CONVENÇÃO DE BUDAPESTE

O Decreto n.º 11.491, de 12 de abril de 2023, foi publicado no Diário Oficial da União para promulgar a Convenção sobre Crimes Cibernéticos, assinada em 23 de novembro de 2021. A Convenção de Budapeste é um importante instrumento no combate ao cibercrime, uma vez que os crimes podem ocorrer em situações em que o criminoso está em um país e a vítima em outro, ou vice-versa.

O objetivo da Convenção de Budapeste é formar uma unidade de cooperação no combate aos crimes cibernéticos, promovendo coerência interna e linearidade na cooperação entre os países signatários. O Conselho da União Europeia, juntamente com os estados signatários, define os principais objetivos da Convenção sobre Crimes Cibernéticos, destacando a importância de tratar

os crimes cibernéticos de forma universal para que todos os países que aderiram ao tratado possam cooperar mutuamente em casos de crimes praticados entre diferentes países.

Emerson Wendt aborda estes temas.

> i) A uniformização dos tipos penais referentes aos crimes de informática pelos estados signatários;
> ii) Definição dos conceitos e preceitos fundamentais, elencado às principais terminologias e uniformizando os principais conceitos para melhor interpretação e debate;
> iii) Tentativa de implementação de um sistema de cooperação internacional para a persecução desses crimes (Wendt, 2019, p. 20-21).

Existe uma preocupação global com a proteção contra os crimes cibernéticos praticados por hackers. A Convenção existe desde a década de 1980 nos Estados Unidos, mas somente em 2001 ocorreu a Convenção sobre o Cibercrime em Budapeste, logo após os eventos de 11 de setembro nos Estados Unidos (Wendt *et al.*, 2019, p. 20).

A Convenção de Budapeste facilitará a colaboração internacional do Brasil em casos que ocorram no espaço virtual, uma vez que não é possível estabelecer fronteiras claras no ciberespaço. Como visto neste estudo, não conseguimos delimitar o espaço virtual. O Conselho Federal da Europa busca alcançar uma ampla proteção contra crimes digitais. "Até o momento, a Convenção sobre Crimes Digitais é o único documento que aborda esse tema e o Brasil passou a ser signatário em 2021" (Wendt, 2015, p. 20), o que facilitará muito as questões envolvendo cibercrimes com vítimas em outros países.

A Convenção de Budapeste tem como objetivo ampliar a proteção às vítimas de crimes cibernéticos por meio da política criminal, unindo todos os países signatários em uma unidade protetora contra esses crimes. A criminalização de condutas, normas para investigação, produção de provas eletrônicas e meios de cooperação internacional são questões abordadas no acordo. Ele trata do acesso indevido e não autorizado a sistemas de computador, fraudes, material de abuso sexual infantil, violações de direitos autorais e violações de segurança de redes.

Alessandro Gonsalves Barreto e Beatriz Silveira Brasil apresentam uma classificação dos crimes amparados pela Convenção de Budapeste.

> Título 1 - Infrações contra a confidencialidade, integridade e disponibilidade de sistemas informáticos acesso ilegítimo, interceptação ilegítima interferência em dados, interferências em sistemas, uso abusivo de dispositivos.

> Título -2 Infrações relacionadas com computadores, falsidade informática, burla informática.
> Título -3 Infrações relacionadas com o acordo infrações relacionadas com pornografia infantil.
> Título 4 – Infrações relacionadas com a violação do direito do autor e direitos conexos. (Barreto; Brasil, 2016, p. 21).

Feitas essas observações sobre a Convenção de Budapeste, que é um importante instrumento para lidar com os crimes cometidos no âmbito virtual, é crucial entender como funcionará a questão da competência dos crimes cometidos por meio desses dispositivos informáticos, especialmente quando a vítima estiver em outro país. O Artigo 70 do Código de Processo Penal (CPP) estabelece que será adotada a teoria do Resultado.

> A Competência será em regra, determinada em que se consumar a infração, ou no caso de tentativa, pelo lugar em que for praticado o último ato da execução.
> §1º se, iniciada a execução no território nacional, a infração se consumar fora dele, a competência será determinada pelo lugar em que tiver sido praticado, no Brasil o último ato da execução.
> §2º quando último ato da execução for praticado fora do território nacional, embora paranacional, será competente o juiz do lugar em que o crime, embora parcialmente, tenha produzido ou deveria produzir seu resultado.
> §3º quando incerto o limite territorial, entre duas ou mais jurisdições ou quando incerta a jurisdição por ter sido a infração consumada ou tentada nas divisas de duas ou mais jurisdições, a competência firma-se apela prevenção. (Nucci, 2014, p. 206).

O Cibercrime, por sua vez, se caracteriza por ser plurilocal, ou seja, a execução inicia-se em um local e a consumação ocorre em outro, além de a vítima e o autor geralmente estarem em locais distintos. Se a conduta acontecer em um país e o resultado em outro, aplica-se o Art. 6º do Código Penal Brasileiro, que trata dos crimes a distância inspirados pela teoria da ubiquidade (Barreto; Brasil, 2017, p. 25).

> Recentemente o STJ, esclareceu que o local que foi subtraída a coisa no caso das transferências bancárias pela internet, é uma construção jurídica, não sendo equivalente ao local físico. (...) No caso de crimes como fraudes praticados por associação crackers pela internet, deve prevalecer o local onde se encontram estabelecidos os agentes, por ser neste local que são planejadas e executadas as ações delituosas (Barreto; Brasil, 2017, p. 22).

Desta forma, percebemos a importância de trazermos ao presente estudo a Convenção de Budapeste, uma vez que há uma imprescindibilidade de amparo legal às vítimas de crimes virtuais diante das vulnerabilidades encontradas, resultantes dos recursos disponibilizados pelas novas

tecnologias. Isso faz com que os hackers tenham cada vez mais facilidades para enganar suas vítimas, utilizando-se dos recursos tecnológicos e, consequentemente, da engenharia social, podendo cometer crimes inclusive contra pessoas que estejam em outros países.

7 CONCLUSÃO

Como vimos, os crimes digitais têm ganhado fortes aliados, sendo o avanço tecnológico o principal deles, uma vez que está intrinsecamente ligado à internet, proporcionando aos criminosos diversas possibilidades para a prática de delitos no ambiente virtual. Uma das estratégias mais eficazes é a engenharia social, na qual os criminosos, com sua expertise, conseguem enganar as vítimas e cometer uma variedade de crimes, aproveitando-se da vulnerabilidade das pessoas que, inocentemente, acabam caindo nas artimanhas dos criminosos e fornecendo informações fundamentais para a prática delitiva.

O avanço tecnológico também gerou a necessidade de implementação de novos dispositivos legais, levando o legislador a inovar com leis especiais. Diante das novas práticas criminosas, as tipificações anteriormente elencadas no Código Penal não abrangiam esses novos eventos jurídicos. Assim, foram lançadas no ordenamento jurídico a Lei Carolina Dieckmann, que tipifica os crimes cibernéticos, e outras normas infraconstitucionais que visam criar tipificações para os crimes virtuais, como a lei que aborda o Cyberstalking.

Além disso, dois institutos fundamentais, a Lei Geral de Proteção de Dados (LGPD) e o Marco Civil da Internet, têm o objetivo de proteger os cidadãos diante do avanço das tecnologias e do uso da internet no Brasil. Ademais, a Constituição Federal Brasileira, por meio do constitucionalismo digital, ampara amplamente os direitos fundamentais que surgem nesse novo cenário social e tem a função de resguardar os princípios fundamentais no âmbito virtual.

Para proporcionar um amparo ainda maior ao cidadão brasileiro diante desse cenário de vulnerabilidades no âmbito virtual, o Brasil tornou-se signatário da Convenção de Budapeste, cujo principal objetivo é o combate aos crimes cibernéticos em escala global, promovendo a cooperação entre todos os países signatários e formando uma unidade nesse enfrentamento ao cibercrime.

Portanto, o legislador tem demonstrado interesse em proteger o cidadão brasileiro diante das vulnerabilidades decorrentes do desenvolvimento tecnológico. Embora o direito positivado esteja um passo atrás em relação à criatividade delitiva na atual Sociedade da Informação, o

ordenamento jurídico brasileiro vem adaptando as condutas às tipificações já existentes e lançando novos dispositivos legais de proteção.

REFERÊNCIAS

BARROSO, Darlan, ARAÚJO JUNIOR, Marco Antônio, **Vade Mecum, Legislação Selecionada para OAB e Concursos**. 8º ed- São Paulo: Revistas Dos Tribunais, 2016.

BARRETO, Alessandro Gonsalves; BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética à luz do Marco Civil da Internet**. Rio de Janeiro: Braspor, 2016.

BRASIL. **Decreto nº 11.491, de 12 de abril de 2023**. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm#:~:text=DECRETO%20N%C2%BA%2011.491%2C%20DE%2012,23%20de%20novembro%20de%202001. Acesso em: 09 jan. 2024.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 10 mar. 2024.

BRASIL. **Decreto-Lei nº 2.848, de 07 de dezembro de 1940**. Disponível em: https://www.jusbrasil.com.br/topicos/10619836/artigo-155-do-decreto-lei-n-2848-de-07-de-dezembro-de-1940. Acesso em: 02 mar. 2024.

CASTELLS, Manuel. **A Sociedade em Rede**. 23 ed. Rio de Janeiro: Paz e Terra, 2021.

CELESTE, Eduardo. Constitucionalismo Digital: Mapeamento a Resposta Constitucional Aos Desafios da Tecnologia Digital. **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 15, n. 45, p. 63-91, jul./dez. 2021 Disponível em: https://edisciplinas.usp.br/pluginfile.php/7638692/mod_resource/content/1/Constitucionalismo%20digital%20-%20Edoardo%20Celeste.pdf. Acesso em: 01 mar. 2024.

FARIAS, James Magno A. **Direito Tecnologia e Justiça Digital**. São Paulo: LTr, 2023.

GONÇALVES, Victor Hugo Pereira. **Proteção de dados Pessoais, Direitos do Titular**. Rio de Janeiro: Forense, 2023

GALVÃO FILHO, Anízio Pires; MOTTA, Francisco José Borges; PAULO, Lucas Moreschi. **O Constitucionalismo Digital e a Crise das Democracias Liberais**. São Paulo: Editora dialética, 2023.

JANINI, Tiago Cappi; LEAL, Simone Gomes. **Big Brother Fiscal**: A Fiscalização Tributária no Ambiente Digital diante dos Direitos Fundamentais do Contribuinte. Fortaleza, CONPEDI, 2023. Disponível em http://site.conpedi.org.br/publicacoes/pxt3v6m5/1mc21155/D5H1IoMJUxr530oo.pdf. Acesso em:

LÉVY, Pierre. **Ciberespaço**: um Hipertexto com Pierre Levy. Porto Alegre, RS: Artes Ofícios, 2000.

LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cintia Rosa Pereira. **Direito & Internet III, Marco Civil na Internet**. São Paulo: Quartie Latin do Brasil, 2015.

LYOTARD, Jean François. **A Condição Pós-Moderna**. 20 ed. Rio de Janeiro: José Olímpio, 2021.

MALHEIRO, Emerson. **Direito da Sociedade da Informação**. São Paulo: Max Limonard, 2016

MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo digital Jurisdição Constitucional: uma agenda de pesquisa para o caso brasileiro. **Revista Brasileira de Direito**, Passo Fundo, v. 16, n. 1, 2020. Disponível em: https://seer.atitus.edu.br/index.php/revistadedireito/article/view/4103. Acesso em: 22 fev. 2024.

NOGUEIRA, Sandro. **D`Crimes de Informática**. 2. ed. São Paulo: BH Editora e Distribuidora, 2019.

NUCCI, Guilherme de Souza. **Código de Processo Penal Comentado**. 13. ed. Rio de janeiro: Forense, 2014.

SANTOS, Stalking dos. **Parâmetros de Tipificação e o Bem Jurídico da Integridade Psíquica**. Oimbra: Almedina. Net, 217.

TURING, Dermond, A História da Computação do Ábaco à Inteligência Artificial. São Paulo: M. Books do Brasil Editora Ltda., 2019.

WENDT, Emerson; JORGE, Vinicius Nogueira. **Crimes Cibernéticos, Ameaças e Procedimentos de Investigação**. 3 ed. Rio de Janeiro: 2021.

WENDT, Emerson (Org.). **Direito & TI – Cibercrimes**. Porto Alegre: Livraria do Advogado, 2019.