ASSOCIAÇÃO VITORIENSE DE EDUCAÇÃO, CIÊNCIA E CULTURA - AVEC
CENTRO UNIVERSITÁRIO FACOL - UNIFACOL
COORDENAÇÃO DO CURSO DE DIREITO – BACHARELADO.

ÍTALO MATHEUS BEZERRA DA SILVA

CYBERCRIMES E AS LEGISLAÇÕES PENAIS BRASILEIRAS

VITÓRIA DE SANTO ANTÃO – PE
2024.1

ÍTALO MATHEUS BEZERRA DA SILVA

CYBERCRIMES E AS LEGISLAÇÕES PENAIS BRASILEIRAS

Trabalho de Conclusão de Curso apresentado ao Curso de Direito do Centro Universitário FACOL - UNIFACOL, como requisito parcial para a obtenção do título de Bacharel em Direito.
Área de Concentração: Direito Penal

Orientador: Prof. Fernando Correia

VITÓRIA DE SANTO ANTÃO – PE
2024.1

ATA DE DEFESA

Nome do(a) Acadêmico(a): **ÍTALO MATHEUS BEZERRA DA SILVA**

Título do Trabalho de Conclusão de Curso: **CYBERCRIMES E AS LEGISLAÇÕES PENAIS BRASILEIRAS.**

Trabalho de Conclusão de Curso apresentada ao Curso de Direito do Centro Universitário FACOL - UNIFACOL, como requisito parcial para a obtenção do título de Bacharel em Direito.
Área de Concentração: Direito Penal
Orientador (a): Prof. Fernando Correia

A Banca Examinadora composta pelos Professores abaixo, sob a Presidência do primeiro, submeteu o candidato à análise da Monografia em nível de Graduação e a julgou nos seguintes termos:

Professor:

Julgamento – Nota: Assinatura: _____

Professor:

Julgamento – Nota: Assinatura: _____

Professor:

Julgamento – Nota: Assinatura: _____

Nota Final: Situação do Acadêmico:

MENÇÃO GERAL:

_____

_____
Prof. Me. Severino Ramos da Silva
Coordenador de TCC do Curso de Direito

_____
Prof. Me. Maria Paula Latache Ribeiro de Vasconcelos / Prof. Me. Felipe da Costa Lima de Moura
Coordenação do Curso de Direito

Vitória de Santo Antão – PE, ___ de _____ de 2024.

RESUMO

A progressão dos meios eletrônicos e o advento da era tecnológica e da informação têm ampliado a vulnerabilidade dos usuários. Isso ocorre devido às facilidades proporcionadas pela internet, que frequentemente oferecem oportunidades aos criminosos para cometerem os denominados crimes digitais ou cybercrimes. Por essa razão o objetivo geral da pesquisa, abordará nos diversos capítulos, os aspectos históricos e conceituais desses crimes, assim como os objetivos especificos com algumas noções gerais dos mesmos. Serão explorados os principais tipos de crimes digitais e, por fim, será apresentada uma breve análise da atual legislação brasileira, com uma problematica ao evidenciar a fragilidade do sistema jurídico diante dos crimes virtuais. Para ressaltar a hipótese, foi desenvolvido a relevância nesta pesquisa de como é o procedimento usados nos crimes. Portanto os capítulos incluirão uma análise de trabalhos relacionados ao tema de autores e estudiosos renomados no meio acadêmico. A pesquisa tem como justificativa por meio da análise de estudo, que há uma carência de legislação para abordar um conflito que está em constante crescimento em nossa sociedade contemporânea, uma vez que estamos cada vez mais dependentes do ambiente virtual. A metodologia do trabalho foi embasada no método de pesquisa bibliográfica, pois foi abordado o estudo a diversos artigos, livros e trabalhos acadêmicos referentes ao meio. É esperado que quem se habilite a ler o trabalho irá se deparar com o nosso ordenamento punitivista, contudo, com muitas brechas, e leis anacrônicas, precisando urgentemente de novas atualizações. Foi exposto a posição do ordenamento jurídico vigente no Brasil da legislação em relação ao assunto, pois a lei existente. Pôde-se perceber a necessidade da atuação urgente dos legisladores na elaboração de normas mais especificas e ríspidas em suas punições.

Palavras-chave: Cibercrime. Ciberespaço. Lei. Internet. Análise.

ABSTRACT

The progression of electronic media and the advent of the technological and information age have increased the vulnerability of users. This is due to the facilities provided by the internet, which often offer criminals opportunities to commit so-called digital crimes or cybercrimes. For this reason, the general objective of the research will cover the historical and conceptual aspects of these crimes, as well as some general notions. The main types of digital crime will be explored and, finally, a brief analysis of current Brazilian legislation will be presented, with a problem in highlighting the fragility of the legal system in the face of virtual crimes. In order to highlight the hypothesis, the relevance of this research was developed in terms of the procedure used in these crimes. Therefore, the chapters will include an analysis of works related to the topic by renowned authors and scholars in the academic world. The research is justified by the fact that there is a lack of legislation to address a conflict that is constantly growing in our contemporary society, since we are increasingly dependent on the virtual environment.The methodology was based on the bib- liographical research method, since several articles, books and academic works related to the environment were studied. Internet allows the transmission of a large amount of information between different parts of the planet in a short period of time, thus facilitating communication and relationships between people. Therefore, it is necessary for people to have computational security that guarantees the confidentiality, integrity and reliable availability of systems. This is an exploratory and bibliographical research that aimed to understand what a cybercrime is and report the need for effective laws on virtual crimes and how our criminal regulations are very inefficient regarding the sanctions that cybercriminals should receive. It is expected that whoever reads this paper will come across our punitive system, but with many loopholes and anachronistic laws with an urgent need of updates. The position of the current legal system in Brazil and the inefficiency of the law in relation to the subject were exposed, since the existing law is vague. It was possible to realize the need for urgent action by legislators in the develop- ment of more specific and harsh rules in their punishments.

Keywords: Cybercrime. Cyberspace. Law. Internet. Analysis.

SUMÁRIO

1 INTRODUÇÃO

Diversos são os crimes que podem ser cometidos no âmbito virtual, dentre os quais: pedofilia, difamação, calúnia e injúria (crimes contra honra), *bullying*, instigação ao suicídio, além do mais, crimes que surgiram a partir do advento da internet, e precisam de um certo conhecimento específico para serem praticados como *phishing,* furtos de dados etc. Os crimes virtuais podem ser classificados em várias formas. Para o autor, os crimes próprios transpassam-se nas ações, como por exemplo, acesso não autorizado, obtenção e transferência ilegal de dados, dano informático, disseminação de vírus e de engenharia social. O estudo foi realizado em 3 capítulos, sendo o primeiro capítulo, uma abordagem a internet como meio para pratica de crimes. No entanto, apesar de todos os benefícios trazidos pela internet, também surgiram essas novas formas de crime, conhecidas como crimes cibernéticos, que se proliferaram de maneira avassaladora nesse ambiente, tornando os usuários alvos vulneráveis. Além do conhecimento amplo em informática que a maioria dos criminosos possuem, eles também se beneficiam das distâncias existentes entre eles e suas vítimas, tornando-as alvos fáceis de seus delitos.

Diante desses acontecimentos, o segundo capítulo apresenta as leis criadas para lidar com o enfrentamento e as dificuldades com os crimes virtuais, onde neste trabalho será abordada a eficácia das medidas legais existentes. O objetivo geral deste trabalho é contribuir para uma maior compreensão desse cenário e promover discussões acerca da importância de uma legislação atualizada e eficaz no enfrentamento dos crimes cibernéticos. Portanto a pesquisa nos traz em seus objetivos específicos: As práticas de crimes virtuais; Invasões de sistemas de empresas e indivíduos; Bem como falsidade ideológica e estelionatos. Com uma hipótese diante da complexidade e a velocidade de evolução dos crimes cibernéticos, exigem um constante aprimoramento das leis e das medidas de segurança digital. Já o terceiro capítulo, apresentará o importante papel de, não somente reprimir, mas também acautelar ao criminalizar determinadas condutas que interfiram ou ameacem os princípios básicos do ciberespaço, que são a confidencialidade, integridade e disponibilidade. Os novos criminosos, cuja classificação é extensa e abrangente no decorrer deste trabalho, agem certo de que ficarão impunes, pois não estão presenciando o abatimento da vítima pós-crime, e a sociedade se sente insegura por

não haver uma imediata prisão do infrator do delito.

Contudo, há diversos empecilhos para configurar essa barreira, como dificuldades técnicas na hora da apreensão do equipamento usado para o cometimento do ilícito, necessidade de autorização para quebra de sigilo do acusado, falta de legislação, além das questões relacionadas com territorialidade, jurisdição e competência, todas necessárias ao devido processo legal.

O entrelaçamento entre o real e o virtual vem tornando-se pleno. As condutas praticadas em sociedade cibernética tipificam-se penalmente como se as mesmas tivessem sido praticadas no plano real. Nesses casos, a aplicação penal se expressa a partir de um nexo de causalidade, por analogia hermenêutica, uma vez que o ordenamento jurídico brasileiro existente para regular os crimes cometidos nos ambientes virtuais é vago.

A problemática da pesquisa do cibercrime advém de suas características, são elas que dificultam a sua prevenção, investigação, repressão e punição. Os crimes cibernéticos podem ser considerados recente, pois trata-se de uma questão que foi iniciada juntamente com a aparição da internet. Por esse motivo, apresentar a caracterização e as devidas singularidades existentes é de extrema importância.

Compreender a natureza desses crimes e as especificidades que os envolvem é fundamental para a criação de estratégias eficazes de prevenção e combate.

Nesse sentido como justificativa foi necessário analisar a efetividade das leis existentes e identificar possíveis lacunas que precisam ser preenchidas para melhor proteger os usuários da internet. Outra característica é sua atemporalidade, uma vez que são permitidas as transferências de informações por todo globo, à velocidade de segundos. Durante a pandemia causada pelo novo coronavírus, os golpes financeiros, no período entre 20 de março a 18 de maio de 2020, a busca sobre informações pessoais e bancárias dos brasileiros cresceu 108%, conforme pesquisa feita na Refinaria de Dados.

Logo, a sociedade se vê impotente e desamparada, por isso o presente estudo, busca detalhar o cibercrime, bem como analisar a necessidade de haver uma lei específica e eficaz para tipificar e punir de maneira satisfatória os criminosos que se utilizam da internet como forma de cometer delitos.

A metodologia deste trabalho traz um estudo de pesquisas bibliográficas, pois foi abordado o estudo a diversos artigos, livros e trabalhos acadêmicos referentes ao meio. Para isso, a pesquisa será baseada em estudos de autores, como por exemplo:

Corrêa, Nucci, Zafaroni, entre outros pensadores que elaboraram pesquisas referentes ao tema.

Contudo, há de se salientar que, o corpo de autores tende a ampliar na medida em que a leitura vier a ser desenvolvida. Partindo dos conceitos apresentados pelos autores do Direito Penal, o trabalho analisará como nosso ordenamento consegue se sair frente as ações ilícitas dos cibercriminosos. O estudo terá caráter essencialmente qualitativo, com ênfase na observação e estudo documental, simultaneamente que será necessário o cruzamento dos levantamentos com toda a pesquisa bibliográfica já feita.

Na análise doutrinária e legislativa, empregar-se-á essencialmente o método hipotético-dedutivo, utilizando o procedimento bibliográfico, realizado por meio de material teórico e jurídico, além de sites e livros que versam sobre o tema. Nessa perspectiva, é indispensável primeiro analisar os dados a partir de alguns artigos, livros e revistas científicas, quais as leis penais que atualmente vigoram no nosso ordenamento penal, e quais deveriam ser melhoradas ou até criadas, além do mais, verificar como os outros países lidam com a mesma situação.

A popularização da internet, em que pese a enorme facilidade que proporciona à coletividade, traz consigo também questões preocupantes acerca da utilização indevida, motivo pelo qual os procedimentos investigativos perante a nossa normativa penal vigorante ao tratar dos crimes virtuais necessitem se adequar para satisfazer a proteção estatal dos cidadãos. Mas como isso pode ser feito de forma eficaz e eficiente, de modo que resguarde os direitos e mantenha a segurança dos cidadãos.

2 A INTERNET COMO MEIO PARA A PRÁTICA DE CRIMES

2.1 Internet: conceito e histórico

A lei vem antes da sociedade humana e se estende à sabedoria das civilizações antigas. À medida que o homem começa a adquirir conhecimento e compreensão, torna-se cada vez mais importante ter regras que estabeleçam a sincronia no grupo. Desta forma, deve-se dizer que o Direito vem do homem e visa regular o convívio social.

Conforme preleciona Paulo Nader:

> O Direito não corresponde às necessidades individuais, mas a uma carência de coletividade. A sua existência exige uma equação social. Só se tem direito relativamente a alguém. O homem que vive fora da sociedade vive fora do império das leis. O homem só, não possui nem direitos nem deveres. (Nader, 2014).

Portanto, para que haja uma organização estrutural é essencial haver regulação pública. Pois, a prevenção serve exatamente para monitorar as situações futuras. Pois, os métodos servem para controlar determinados comportamentos, que em sua maioria são contrários aos princípios morais e dos bons costumes. O doutrinador, sobre o assunto explana:

> A participação do Estado na vida do Direito não se restringe ao controle da elaboração das regras jurídicas. Além de zelar pela manutenção da ordem social por seus dispositivos de prevenção, com o seu aparelho coercitivo aplica o Direito a casos concretos. (Daun, 2000, p. 34)

Na mesma linha de pensamento há o doutrinador Hans Kelsen (1964), detentor da Teoria Pura do Direito: “Em determinadas circunstâncias, um determinado sujeito deve observar tal ou qual conduta; se não a observa, outro sujeito, órgão do Estado, deve aplicar ao infrator uma sanção.” Então, assim, tivemos o surgimento do Direito, por meio do qual derivou o Direito Digital. Uma forma de gerenciar a comunidade a viver em harmonia. A advogada especialista, Patrícia Peck, no assunto Digital, discorre:

> Ter uma janela aberta para o mundo exige muito mais que apenas a seleção do público-alvo. Exige a criação de uma logística jurídica que reflita a diversidade cultural dos consumidores/clientes virtuais. No aspecto de atendimento ao consumidor, por exemplo, parte das empresas inseridas na rede recorrem à terceirização, contratando *contaccenters* especializados para atender a demanda de usuários de diferentes culturas e países. No aspecto jurídico, é preciso que os profissionais de Direito também estejam preparados para criar logística, sabendo que a todo o momento terão de lidar com diferentes normas, culturas e legislações. (Pinheiro, 2009, p. 22)

Desse modo, torna-se uma exaustiva tarefa para o Direito acompanhar, resguardar e compreender as demasiadas demandas de uma sociedade civil moderna que vive em constante progressão, necessitando de formas que auxiliem na manutenção da ordem social. Em meio a esta requisição, surge o Direito Digital, visando interpelar lacunas provenientes da modernidade e da evolução tecnológica.

Nesse diapasão, atribui:

> A tecnologia digital é uma realidade, e justamente por isso estamos diante da criação de lacunas objetivas, as quais o direito tem dever de estudar, entender e, se necessário, preencher. Com a crescente popularização da grande rede, evidenciamos a criação de novos conceitos sobre tradicionais valores, tais como a liberdade, a privacidade e o surgimento de “crimes” digitais. (Corrêa, 2011, p. 205)

Nesse contexto, tratando-se da internet, há também violações ao direito alheio. Os chamados Crimes Cibernéticos, ou crimes virtuais, digitais é uma forma genérica que retrata um ou diversos atos ilícitos que podem ser cometidos no âmbito virtual, atendo-se da tecnologia para sua realização. Corrêa contribui:

> Poderíamos dizer que os “crimes” digitais seriam todos aqueles relacionados as informações arquivadas ou em trânsito por computadores, sendo esses dados acessados ilicitamente, usados para ameaçar ou fraudar; para tal prática é indispensável a utilização de um meio eletrônico. Toda sociedade dependente da informação acaba sendo vítima de simples ameaças e até do terrorismo e do vandalismo eletrônicos. (Corrêa, 2011, p. 205)

Para Ferreira (2009), esta forma de crime, “consiste na utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele a ordem econômica, à honra, ao patrimônio, etc.”. Por isso,

esse crime se torna uma grande dificuldade para ciência jurídica, em virtude da identificação que necessita de um conhecimento detalhado para apurar, além de estarmos amparados por uma carente legislação, o que torna ainda mais complexo.

2.1.1 Evolução da internet

Antes do surgimento da internet propriamente dita, já existiam diversos meios de comunicação, como rádios, telefone e televisão. Especificamente, já existiam computadores ligados entre si e moderados por um computador central, por meio do qual era possível trocar informações. Desse modo, a ideia da internet era construir um tipo de comunicação entre computadores que não fosse centralizada. Ou seja, a informação seria trocada agora em redes, com máquinas autônomas e interdependentes. Essa teoria teve consequências práticas com o projeto chamado *Advanced Research Projects Agency*, ou simplesmente *ARPANET*. Curiosamente, ele era parte de uma pesquisa militar dos Estados Unidos.

Conforme Bernardo Lins (2010), há quatro principais períodos que marcam a trajetória da internet mundialmente. Primeiramente, na década de 1980, ela era utilizada entre grandes computadores ligados por cabo ou redes telefônicas. Nesse contexto, a internet dava seus primeiros passos e tinha usos específicos de troca de informações. Após esse momento, a internet chega ao grande público. Assim, surgem as “conexões discadas” da década de 1990, que foram as primeiras formas de acesso à rede pelas pessoas em geral. Na época, o conteúdo da internet se restringia majoritariamente a textos e *hiperlinks*.

Em seguida, a terceira fase da internet marca o avanço nas conexões de banda larga a partir do final da década de 1990. Desse modo, os conteúdos vinculados na rede se desenvolveram com imagens, músicas, gifs e jogos. Além disso, surgem as plataformas de bate-papo, as interações personalizadas com avatares e as redes sociais. (Filho, 2009)

Por fim, o período atual é marcado pela pluralidade de meios de comunicação, principalmente com o uso dos smartphones. Além disso, o tablet, os relógios e até mesmo a televisão tornaram-se porta de acesso à internet. Agora, o mundo das redes não é algo acessado pelas pessoas apenas em um momento específico: ele é integrado em suas vidas. (Lins, 2010).

Atualmente, o desenvolvimento das redes sociais, as formas de armazenamento em nuvem e as discussões sobre segurança e ética marcam a internet. Afinal, campanhas eleitorais e discussões importantes ocorrem nas redes na contemporaneidade. Portanto, é importante que os debates sobre a internet ocorram sempre tendo em vista a ética envolvida nas relações sociais. Ao mesmo tempo que o “mundo virtual” reproduz muitos aspectos do “mundo real”, a internet também traz mudanças sobre os rumos das histórias humanas. Assim, os velhos e os novos tempos sempre convivem de algum modo, e é necessário discutir com responsabilidade sobre eles.

2.2 Métodos, técnicas, recursos e ferramentas utilizadas pelos criminosos

Segundo Jesus (2016, p.28) “o crime cibernético no Brasil está menos técnico e muito mais criativo”.

A criatividade tornou-se a chave para cometer delitos na internet, e considerando que nada atrai mais a vítima do que o poder da persuasão, a criatividade é mais benéfica para os criminosos do que o próprio conhecimento técnico da rede, por isso é justo dizer que o planejamento para realizar uma atividade criminosa através de um computador começa apenas com as habilidades do cérebro humano.

2.2.1 Estrutura de métodos

São técnicas usadas por criminosos virtuais para atacar computadores e dados dos usuários bem como as suas defesas em várias camadas como: Bullying virtual - Conforme Albino e Terêncio, o *cyberbullying* consiste na truculência de forma intencional e repetitiva de atitudes agressivas dentro do ciberespaço das redes sociais, podendo ser caracterizado como difamação, calúnia e injúria. O contato entre vítima e agressor não ocorre presencialmente, mas online. (Albino, 2015).

Pode ocorrer via e-mail, em fóruns ou websites, mas ganha cada vez mais notoriedade nas redes sociais, onde a instantaneidade das mensagens facilita as ofensas e ameaças dos criminosos; Extorsão – Devisate (2021) conceitua que, ao usar programas maliciosos, criminosos podem roubar fotos e vídeos pessoais e, assim, chantagear os usuários para não divulgar as imagens na Web. Em muitos

casos, para preservar sua intimidade e evitar a divulgação de fotos íntimas ou sexuais, os usuários acabam pagando o preço exigido pelos bandidos. Essa prática é conhecida como *Sextorsing;* Venda de imagens.

Conforme disposto por Lauren (2018), os criminosos vendem fotos para criar perfis falsos em redes sociais que, por sua vez, são usados para cometer outros tipos de delitos, como praticar crimes de ódio ou disseminar mais vírus e malwares. Além da extorsão, fotos e vídeos pessoais roubados podem ser vendidos para outros fins ilegais; Phishing e engenharia social.

Ferreira (2016) entende que, é um truque psicológico projetado para convencer alguém a fazer algo que não deveria, e o phishing é a forma mais conhecida de engenharia social.

Dessa forma, os cibercriminosos se passam por entidades legítimas, amigos, familiares, organizações públicas e empresas conhecidas, e tentam induzir as vítimas a compartilharem informações pessoais, o que também é chamado de *phishing*; Ataques de força bruta Fernando (2018) dispõe que, é comum que credenciais fáceis de serem lembradas sejam escolhidas por muitos usuários.

Isso, porém, facilita os ataques de força bruta, onde os criminosos tentam diferentes combinações de senhas para tentar acessar contas. Outra técnica de força bruta é a pulverização de senha. Nesse caso, os criminosos usam software automatizado para testar uma lista de senhas usadas com mais frequência em uma conta; por dedução.

Conceitua Higor (2013), os hackers possuem ferramentas automatizadas para realizar ataques de força bruta e descobrir senhas, às vezes eles nem precisam delas, dependendo da força da credencial escolhida pelos usuários. E, com pesquisas mostrando que a senha mais comum em 2021 foi *123456*, seguida por *123456789*, a dedução dos criminosos pode ter sucesso, em muitos casos.

2.2.2 A utilização das técnicas

São os recursos utilizados para alcançar o objetivo de quem adquire habilidades para alterar todo e qualquer dispositivo eletrônico, programa entre outros como: Ataques DdoS - A sigla vem do inglês *“Distributed Denial of Service*” que, em português, significa “Ne- gativa de Serviço Distribuída”. Um primo próximo do DDoS é o DoS, no qual apenas um criminoso, com um único computador, ataca

várias máquinas. Dessa forma, “derruba” redes, servidores ou computadores comuns que contenham baixas especificações técnicas. No DDoS, um computador pode comandar diversos outros (até milhões) e assim coordenar um ataque em massa. O aparelho principal, chamado de mestre, “escraviza” outras máquinas que, obrigatoriamente, acessam o que o proprietário solicita; Manipulação de url , é usado por alguns hackers, conforme doutrina Wellington (2015), para fazer o servidor transmitir páginas às quais ele não teria autorização de acesso.

Na prática, o usuário só tem acesso a links que são fornecidos pela página do site. Se o usuário altera manualmente a URL, ele pode testar diversas combinações para chegar a um endereço que esconde uma área restrita; Ataque DMA (Direct Memory Access) Wellington (2015) afirma que o ataque de Acesso Direto à Memória é uma função que permite ao hardware da máquina ter um acesso direto à memória RAM sem passar pelo processador, acelerando, assim, a taxa de transferência e processamento do computador.

Esse recurso, no entanto, pode ser usado por hackers para acessar os dados da memória RAM por meio de um periférico, mesmo sem um software específico; *Eavesdropping* - Kenia (2020) afirma que no ataque o hacker utiliza diferentes sistemas de e-mail, mensagens instantâneas e telefonia, além de serviços de internet, para violar a confidencialidade da vítima, roubando seus dados para usá-los de forma indevida posteriormente. A palavra significa *bisbilhotar*, e é basicamente o que o criminoso faz, sem modificar as informações, apenas interceptando e armazenando.

2.2.3 Recursos adquiridos pelos criminosos

Conceitua Almeida (2020) que, além de sites de publicidade, com o advento da internet surgiram diversas redes sociais, bem como aplicativos que disponibilizam a troca de mensagens instantâneas. Visto que, essas redes sociais podem ser facilmente utilizadas por criminosos para atrair suas vítimas, uma vez que não há como garantir uma navegação segura. Por muitas vezes, na internet, a única segurança será a precaução do próprio internauta.

Do boleto falso - De acordo com a Febraban (2022), cerca de 6 bilhões de boletos falsos são emitidos anualmente no Brasil. Esse vem sendo o tipo mais comum de fraude no Brasil. Normalmente, os criminosos elaboram um boleto falso

contendo todos os dados da vítima, onde fingem ser uma empresa de cobrança real. Eles enviam o boleto via *WhatsApp* solicitando pagamento;

Via SMS - Jonatas (2022) entende que o SMS é um dos golpes favoritos dos criminosos. Nas mensagens, eles pedem que a vítima atualize cadastros de bancos, enviando links que direcionam para páginas falsas. O objetivo final desse golpe é conseguir os dados pessoais para acessar os canais oficiais;

Do perfil falso - Conforme Lariane (2020), nesse golpe, os criminosos usam contas com perfis falsos nas redes sociais. Ele se divide em duas formas: Golpistas se passando por contas de lojas, onde vendem os produtos que não são entregues. Nesse caso, a vítima fica no prejuízo e não recebe as compras; quando se passam por pessoas e simulam relacionamentos virtuais, conhecido como *Catfish*. Eles encontram um alvo e começam a ganhar confiança da vítima. Após estreitarem relações, começam a relatar problemas e dificuldades financeiras, pedindo dinheiro para cobrir despesas. Na maioria das vezes, as mulheres são as grandes vítimas desse tipo de golpe.

2.2.4 As ferramentas utilizadas no crime

Os cibercriminosos não precisam estar munidos de armas de fogo ou estar presente pessoalmente no local do crime, pois, para conseguir praticar os cibercrimes basta: invadir um computador com códigos maliciosos para ter acesso a senhas, furtar ou roubar documentos e informações, destruir ou alterar dados.

Além disso, o Conselho Nacional de Justiça (2018) lembra sobre a possível também praticar pedofilia, lavagem de dinheiro, fraudes financeiras, todas através de um link na *aba* de mensagens do celular ou computador.

A prática mais comum é por intermédio de *malwares* que invadem *e-mails, softwares* e páginas da internet por meio de técnicas de *pshishing,* que influenciam no clique de *links* infectados por vírus.

2.3 Surgimento do Cibercrime

Rossini (2013) descreve “delito informático” como “uma conduta ilícita e típica, constitutiva de crime ou contravenção penal, dolosa ou culposa, comissiva ou

omissiva, podendo ser praticada por pessoa jurídica ou física, com uso da informática em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança da informática que tem por elementos a integridade, a disponibilidade, e a confidencialidade.

Nesse diapasão, pode-se depreender que os intitulados “infrações informáticas” não se trata de crimes e contravenções penais restritos apenas ao âmbito proveniente da internet, como também a um computador “*offline*”, servindo como mecanismo para a consumação do crime da mesma forma.

Segundo Pedro (2000), a revolução da tecnologia proporcionou uma disseminação numa velocidade inimaginável, bastando apenas um click, e com isso, veio também um aprimoramento do acúmulo de conhecimento, de armazenamento de dados e muitos outros benefícios. Em razão do avanço tecnológico ocorrido nas últimas décadas, o conceito de crime deixou de ser viabilizado somente na esfera social, passando a “mostrar as caras” no âmbito virtual também. Ocorre que, o fato de haver uma liberdade flexível na era da informação, propiciada pelo advento da internet aliado a gama de informações, acaba por tornar um grande potencial de poder, pois, se a internet consegue atingir um número ilimitado de pessoas com informações, é lógico que pode ser feito também para o uso errôneo, favorecendo cibercriminosos. (Burke, 2020)

Esse problema acabou por chamar atenção das nações, no final da década de 1990. Um pequeno grupo de nações agrupadas no G8, países mundialmente desenvolvidos, fizeram uma reunião em Lyon, visando analisar a problemática acerca da ampliação dos crimes mediante os meios digitais. E dessa reunião saiu a denominação “cibercrime”, uma forma genérica de intitular crimes virtuais.

Todavia, cumpre salientar a dificuldade de determinar os bens jurídicos que devem ser resguardados pelo Direito Penal no tocante aos cibercrimes. Pois, percebe-se que a conduta geradora de danos é a mesma que aquela considerada para crimes no âmbito comum, denotando o dever de observarmos uma outra faceta quanto ao cibercrime, tendo em vista seu caráter diferenciado quanto às outras espécies de infrações já tipificadas pelo nosso ordenamento jurídico. (Polido, 2018)

2.4 Espécies de crimes virtuais

2.4.1 Crimes próprios

Segundo preleciona Oliveira (2009), crime cibernético próprio é aquele que:

> [...] só pode ser cometido no ciberespaço, ou seja, necessariamente, deve ser realizado no ambiente do ciberespaço, para que a conduta seja concretizada, tendo um tipo penal distinto do tradicional. Ademais, tanto a ação quanto o resultado da conduta ilícita consumam-se no ciberespaço.

Para alguns doutrinadores, como Marco Túlio Viana, crimes virtuais próprios "são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados)''. (Viana, 2003, p. 54)

Corroborando com esse conceito, valiosas são as lições de Damásio Evangelista de Jesus:

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computa- dor e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da má- quina e periféricos) é o objeto jurídico tutelado. (Damásio, 2015, p.28)

Logo, os crimes virtuais próprios são aqueles em que o sujeito ativo utiliza o sistema informático do sujeito passivo, no qual o computador como sistema tecnológico é usado como objeto e meio para execução do crime. Nessa categoria de crimes está, não só a invasão de dados não autorizados, mas toda a interferência em dados informatizados como, por exemplo, invasão de dados armazenados em computador seja no intuito de modificar, alterar, inserir dados falsos, ou seja, que atinjam diretamente o software ou hardware do computador e só podem ser concretizados pelo computador ou contra ele e seus periféricos.

2.4.2 Crimes impróprios

Os crimes virtuais denominados impróprios são aqueles realizados com a utilização do computador, ou seja, por meio da máquina que é utilizada como instrumento para realização de condutas ilícitas que atinge todo o bem jurídico já tutelado, crimes, portanto que já tipificados que são realizados agora com a utilização

do computador e da rede, utilizando o sistema de informática seus componentes como mais um meio para realização do crime, e se difere quanto a não essencialidade do computador para concretização do ato ilícito que pode se dar de outras formas e não necessariamente pela informática para chegar ao fim desejado como no caso de crimes como a pedofilia. (Almeida, 2015).

Sobre o tema, discorre Castro (2022, p. 21):

> Os tais “crimes de informática” qualificados como impróprios admitem a prática por diversos meios, inclusive os meios informáticos.

Nestes crimes impróprios, o agente se vale do computador como meio para produzir resultados naturalístico, que ofenda o mundo físico, ameaçando ou lesando outros bens, pode ser cometido no meio digital através de um e-mail, bate-papo ou qualquer outro meio, os exemplos mais comuns são a calúnia, difamação e injúria, tipificados no Código Penal.

3 O AMBIENTE VIRTUAL E OS DESAFIOS IMPOSTOS AO DIREITO PENAL

3.1 As diferentes dimensões do espaço virtual

Conforme o Comitê Gestor da Internet no Brasil, milhões de cidadãos já usam a internet no país, e para pequenos criadores e novos mafiosos que diversificaram seus criadores, o cibercrime é um negócio lucrativo.

A Febraban, Federação Brasileira de Bancos, é um indicador do índice de sucesso dos crimes cibernéticos e afirma que a fraude no banco eletrônico causará 95% das perdas aos bancos brasileiros (Febraban, 2021).

Lima (2005) define a intrusão no sistema da Internet e posterior modificação dos dados como fraude virtual, com o fim de obter vantagens em bens ou em espécie, como simulação de planos eleitorais aprovados, fiscalização de demonstrações financeiras, transações bancárias, todos falsos e assim por diante.

A partir de análogos russos e ingleses dos criminosos brasileiros estabeleceram um vivido mercado negro para serviços e bens, o mundo do crime online ascendeu. Dessa forma reduz as barreiras de origem e melhora a curva de aprendizado para os cibercriminosos locais, que usam seu conhecimento para atacar bancos locais e serviços de pagamento online.

O *malware* usado em quase todo o país é gerado para ataques locais. O motivo para ter essas instalações virtuais de crime e ter tanto sucesso, de certa forma, é que as vítimas são geralmente as menos informadas, menos discernidas de conhecimento e as necessidades de segurança mais específicas no uso de técnicas simples e básicas para combater os crimes cibernéticos.

Além do fato de haver uma influência social fraca. Diferentemente do típico submundo de língua inglesa ou russa (onde o sigilo e o anonimato são cruciais), no Brasil, os crimes cibernéticos existem abertamente e amplamente sem medo de que as autoridades policiais se aproveitem por suas dificuldades e falta de dissuasão legal, muitas vezes, sem preocupar em esconder a localização exata e de sua verdadeira identificação. (Inellas, 2004).

Enquanto os criminosos locais trapacearam nas transações financeiras, o cibercrime organizado no Leste Europeu poderia facilmente chamar a atenção para o real brasileiro. Ou forme uma aliança com *hackers* brasileiros por intermédio das redes sociais e fóruns na internet, use o *Google Translator* para planejar ataques a

instituições bancárias e governos, invadir e armazenar banco de dados de instituições de crédito de cidadãos brasileiros para uso premeditado ou vendê-los para o fraudador de rede profunda. (Roxin, 2006).

A prática de crimes cibernéticos no Brasil é visivelmente atordoante, visto que, em fraudes na internet, temos o maior número de fraudes bancárias online e *malware* financeiro contra qualquer país do mundo, não somente no sistema bancário brasileiro, mas também envolvendo roubo de moedas virtuais criminosas.

Com o eventual aumento de crimes cibernéticos e a ineficácia das leis e do direito penal relacionados a esses casos, o submundo do crime cibernético continua a ascender. Isso se dá mediante a algumas prerrogativas, entre eles, o baixo investimento no embate a esses crimes; falta de segurança digital adequada e falta de uma cultura voltada para a conscientização da comunidade de usuários; que geralmente não é compreendida e conscientizada pelos setores públicos e privados. (Nucci, 2013).

Na sociedade atual, Era da informação, e na nova realidade econômica que marca o processo cultural e progressivo do mundo, um ambiente virtual resguardado é amplamente pertinente. O tráfego digital na Internet aumentou consideravelmente, variados usuários utilizam a internet para consumir determinado tipo de produto ou serviços. Todavia, o ecossistema digital é extremamente vulnerável ataques criminosos digitais, ameaçando a segurança do usuário.

Portanto, é de suma importância que um país tenha um sistema jurídico condizente com as mudanças atreladas ao avanço tecnológico, e tenha capacidade de amparar, de fato, os usuários frente as infrações cometidas no âmbito virtual. Na mesma linha, conceitua Nucci:

> Estamos passando por uma fase de mudança em que as conexões sociais e os dispositivos de comunicação móvel estão interagindo cada vez mais, mas estamos nos tornando cada vez mais vulneráveis a ataques no campo da privacidade. (Nucci, 2013, p.38)

Para a ciência jurídica, o crime é de um objeto de estudo de extrema importância no seu objetivo de gerar conhecimento para sua aplicação em prol do bem-estar social. A segurança da pessoa (no sentido amplo, de direitos humanos resguardados) é fundamental para amparar a paz e a ordem que favorece a evolução da humanidade.

Em suma, deve-se fazer uma separação do mundo real com o virtual, mais especificamente quanto as condutas, isto é, como as condutas típicas, sejam ações ou omissões, que tenham consequências jurídicas-penais sob a égide da teoria clássica dos crimes. São percebidos por nossos sentidos de forma imediata e natural, muito pelo contrário, os atos ilegais perpetra- dos no ambiente virtual são aqueles que exclusivamente os nossos sentidos podem compreender por intermédio da utilização eletrônica cuja plataforma é comunicação especialmente a internet.

Nesse sentido, Zaccaria (2009, p. 58) atribui:

> A internet é uma rede de computadores, integrada por outras redes menores, comunicando entre si, os computadores se comunicam através de um endereço lógico, chamado IP., onde há uma gama de informações sendo repassadas, surgindo aí um pequeno problema, existe uma quantidade enorme de informações pessoais disponíveis na rede, ficando a disposição de milhares de pessoas, quando não disponíveis informações pessoais pelo próprio usuário, são procuradas por outros usuários que buscam na rede o cometimento de crimes, os denominados crimes virtuais.

No espaço dos crimes, há os crimes cibernéticos cuja manifestação é realizada no ambiente virtual. Geralmente o nome desse tipo de crime vem acompanhado do prefixo “cibernético” e “virtual”. Como enfatiza Rodrigues (2010), majoritariamente, a doutrina define o crime de informática pelo bem tutelado, determinando uma definição incompleta. Dessa forma, para ele o crime digital é “todo procedimento que atenta contra dados, que faz na forma em que estejam armazenados, compilados, transmitidos ou em transmissão”.

Por isso, o crime cibernético é uma realidade indesejável em boa parte dos países do mundo onde a tecnologia predomina, em maior ou menor grau. Crime informático, acaba por ser qualquer conduta ilegal, não ética, ou não autorizada que envolva o processamento automático de dados e/ou transmissão de dados.

Paralelo às benesses com o advento da internet, vieram também, atreladas a condutas ilícitas, visando se abster da legislação em virtude da dificuldade de identificar os autores dos crimes, os crimes no âmbito virtual. Tais condutas são conhecidas de diversas formas, como: crimes virtuais, crimes cibernéticos, digitais, informáticos, telemáticos, de alta tecnologia, crimes por computador, crimes de internet, fraude virtual, entre outras.

Nesse meio, tempos a figura do criminoso informático, cujo possui inteligência, conhecimento de sistemas de informações e usos de meios informatizados, mas que se volta a atingir bens tutelados alheios, fazendo-se valer de um novo universo de possibilidades de atuação criminosa.

O Direito Penal, em suma, tem grande importância acerca do assunto, tendo em vista que sua existência adentrou em evidência a partir de tensões e conflitos sociais que, por ora, acabarão destruindo sua vigência, dando margem a novos entendimentos, e, consequentemente, a novos tipos penais. (Zaffaroni, 2004).

A linha de raciocínio dos doutrinadores citados demonstra como o Direito Penal age, consolidando a ideia de que quando o Direito Penal interrompe seus efeitos e anseios perante a sociedade, acaba por ficar delimitado a um simples exercício do poder por parte do Estado, perdendo a sua efetividade.

Desse modo, precisa ser evidenciado as questões acerca das tarefas que o Direito Penal terá de confrontar frente ao desenvolvimento social que se apresentam e rege a nova sociedade. Nesse diapasão, a Ciência do Direito Penal coloca no banco dos réus as convicções clássicas e deverá proceder à revisão destas, passando a cultivar de forma mais acentuada as premissas supranacionais.

É necessário ter em mente que alguns crimes somente tiveram sua aparição acentuada graças a evolução da sociedade, além da revolução tecnológica, e que só pode ser confrontado a partir de uma atuação conjunta, de modo que, regulações distintas e de diferentes intensidades acarretam num verdadeiro “oásis de criminalidade”. Acerca dessa temática, Roxin (2006, p.30) discorre:

> A Ciência Penal terá de proporcionar as bases científicas para um direito penal supranacional em curto prazo, isto é, propiciar o fortalecimento de um Direito Internacional (...) A ciência penal do futuro terá que desenvolver-se sobre fundamentos internacionais em maior medida do que há feito até agora.

O ciberespaço é um lugar, que só temos acesso pelo computador, mesmo assim precisa estar ligado à realidade pelo uso que temos feito dele atualmente, transformando-o em um espaço interligado entre o mundo imaginário e o real.

Para Terceiro:

> Os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo, por isso, ficaram usualmente definidos como sendo crimes no âmbito virtual, ou seja, os delitos praticados por intermédio da internet são denominados de crimes virtuais, devido à ausência de seus autores e seus adeptos. (Terceiro, 2022, p.07).

O que se observa, é que o crime virtual é qualquer conduta antijurídica e culpável, realizada a partir de um meio eletrônico conectado à internet.

Segundo Rossini:

> O conceito de “delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade, e a confidencialidade. (Terceiro, 2022, p.07).

É possível analisar que a criminalidade é um fenômeno que tem origem de forma muito similar em todos os países do globo, especialmente, com a acessibilidade proporcionada por intermédio dos meios tecnológicos, sobretudo a Internet, que fomenta para que uma espalhe seus efeitos em qualquer país; assim, há o costume de denominar os delitos perpetrados em ambiente virtual de criminalidade transacional. Portanto, o futuro do direito penal, não obstante as diferentes leis penais existentes em cada país, exige, no mínimo, uma maior colaboração entre os Estados do globo, para que haja uma eficácia maior de uma suposta investigação e sanção penal aos infratores. (Rossini, 2004).

Entretanto, há de se falar que existem alguns mecanismos agindo para a obtenção de êxito quando se trata na segurança jurídica acerca de crimes virtuais, tais como: o controle de acesso subdividido em autorização e autenticação; dispositivos de defesa composto por um sistema ou um corpo de sistemas, que reforça o cumprimento de políticas de controle de acesso; o chamado Virtual Private Network (VPN), que permite uma troca de informações altamente decodificada por intermédio de redes públicas; monitoramento de arquivos de registros gerado pelos

serviços de rede; sistemas compostos de *hardware* e *software* capazes de capturar informações; além da criptografia e assinatura digital. (Domingues, 2005).

Todavia, a falta de incentivos eficazes ao desenvolvimento de programas mais modernos, bem como a desvalorização de profissionais da área tecnológica, são desafios diários que precisam ser superados para que a internet seja, de fato, uma rede de progresso em prol da coletividade. Ademais, reconhecer que o Direito tradicional não se atualizou em medida igual as novas tecnologias, também demonstra que a legislação aplicável em toda a persecução penal no caso de crime virtuais precisa de aprimoramento, pois, caso contrário, o processo estará fadado ao fracasso, em virtude da ausência de provas de materialidade delitiva e autoria, ou pelo instituto da prescrição, por exemplo.

3.2 Dificuldades de investigação e repressão dos crimes

Com essa acessibilidade que a tecnologia proporcionou, além do uso exacerbado de aparelhos eletrônicos, o avanço tecnológico ocorre cada dia mais, os crimes virtuais acontecem na mesma proporção, pois os criminosos vão se especializando, porém, as autoridades responsáveis por tratar das investigações e punir os crimes, não acompanharam esses avanços.

Evidencia-se uma grande dificuldade em investigar e punir esses crimes, todavia, dentre ao fato de muitos delituosos agirem de modo a deixarem o mínimo de suspeitas possíveis, utilizando o mundo tecnológico a seu favor que permite agirem de forma anônima e silenciosamente. Desse modo, aumenta o grau de impasse para identificá-los, tendo em vista que esses infratores fazem uso de dispositivos tecnológicos em locais públicos disponibilizando facilmente o acesso, tendo esses agentes artifícios para agir de forma anônima.

O anonimato está interligado ao lado oculto da internet que poucas pessoas conseguem ter acesso, chamado de *Deep Web.* A *Deep Web* é um local onde as pessoas trocam arquivos, informações, de forma totalmente anônima, não podendo ser identificada por mecanismos de busca comuns. Podendo ser acessada através de navegadores como o *TOR* (The Orion Rout), que elimina as “pegadas” de acesso. Muito embora pareça seguro, alguns sites ao serem acessados na rede pode exigir login por intermédio de um navegador comum, facilitando a identificação.

Não obstante, há de se falar também, no despreparo dos profissionais

competentes dessa problemática, que demonstram uma ineficiência altíssima em investigações. Assim como, a carência de incentivo das políticas públicas em fomentar melhores condições de profissionalização e ferramentas para acentuar a investigação. Constata-se que, tratando-se da prova criminal, por intermédio da perícia, o exame pericial é elaborado com um aparelho similar ao que deveria estar apto, que, ainda por cima, precisa de uma autorização de outra autoridade para o uso.

Assim menciona:

> Como no flagrante, onde se consegue o IP (internet protocolo) do computador, porém é necessária a autorização judicial para a obtenção das informações disposta pelo IP, que são localização máquina e os acessos feitos na mesma, contudo os provedores não armazenam tais informações por um longo período. O que compromete a eficácia do trabalho do agente combatente". (Estefam, 2012, p. 98).

Podemos observar a correlação aos aplicativos sociais de comunicação (*WhatsApp, Facebook, Instagram, Telegram*, entre outros), em que o suporte de proteção de usuários é ineficiente. A proteção é feita através de mecanismos de alertas, uma tecnologia de fácil violação, além de ser pouco eficaz.

Esse tipo de proteção acaba por deixar os usuários vulneráveis a supostos ataques virtuais, se fazendo necessário uma melhor associação entre usuários e desenvolvedores/criadores do sistema, acessibilidade para pessoas que não sabem como utilizar o aplicativo, assim como, deixar aparente cartilhas com informações condizentes de como se proteger de crimes como furtos, fraudes, *hackers,* e etc. (Domingues, 2005).

Outrora, uma dificuldade extremamente diária é acerca da legislação aplicável aos casos de crimes cibernéticos, que em muitas vezes são inexistentes, ou quando existem, pecam pela falta de técnica, dando margem a interpretações dúbias, o que dificulta a aplicabilidade. (Frota, 2017).

Um exemplo é a Lei nº 11.829, de 25 de novembro de 2008, que alterou o Estatuto da Criança e do Adolescente, sendo um dos primeiros passos importantes dado pelo Legislativo quando se trata de combater os crimes virtuais; uma vez que a referida lei definiu algumas condutas específicas relacionadas a prática de crimes de pornografia infantil no ambiente virtual, suprindo a lacuna legislativa que deixava

criminalmente isentos aqueles que tinham armazenados em seus computadores vídeos e fotos atrelados a essa prática vil. (Domingues, 2005).

Desse modo, um dos grandes “vilões” não diz respeito à criação de tipos penais exclusivos aos crimes cibernéticos, mas sim em relação à área “administrativo” da rede, sobretudo em relação à guarda dos logs pelos provedores de acesso. Como supracitado no presente trabalho, em síntese, ao se obter o endereço de IP utilizado na prática da conduta criminosa, teria a localização do agente criminoso e sua consequente identificação. Entretanto, há variadas formas de se burlar esse tipo de evidência, tais como a utilização dos servidores *proxies*, das redes de *Wi-Fi* abertas*,* bem como o acesso facilitado por intermédio das denominadas *Lan House.*

> Dentre essas redes abertas, consistem locais gratuitos na internet, criadas em função da crescente onda de utilização de *smarthphones* e outros dispositivos de informática portáteis. Porém, por terem características de serem de acesso gratuito e de plena acessibilidade ao público em geral, estas redes permitem o uso de pessoas não identificadas, apresentando-se *aos cibercriminosos* como um leque de oportunidades para a prática de atividades com fins maliciosos, porque, em razão de ser possível ser acessada por qualquer cidadão, estorva a localização de seus usuários, propiciando uma chance maior de êxito por parte dos criminosos, favorecendo a impunidade. (Oliveira, 2012).

Portanto, o ideal para um combate mais assertivo frente aos crimes virtuais é um fomento maior no investimento tecnológico que auxilie as investigações criminais; capacitar os profissionais com cursos meramente especializados, bem como o treinamento aos agentes de polícia; a inserção de mais delegacias especializadas, especialmente nos interiores do estado, onde o crime é bem mais recorrente, devido a pouca instrução educacional das pessoas; normativas majoradas, visando leis mais convergentes com as ações da atualidade, tendo em vista que os crimes se adequam ao avanço tecnológico também. (Hauser, 2010).

A tecnologia da informática é privativa de grande complexidade e dinamismo sem igual, o que faz com que os órgãos investigativos e judiciários não estejam adequadamente preparados para lidar com esta nova criminalidade e a cada uma de suas repentinas mudanças. (Hauser, 2010).

Frequentemente, é possível encontrar agentes públicos ineficientes que, por sua vez, exista uma falta técnica de conhecimento específico, esbarra também na

falha de prestação da proteção estatal aos cidadãos nos órgãos responsáveis pela persecução penal. Entretanto, não é somente a capacitação técnica dos agentes estatais que encarece o sistema investigatório, equipamentos de última geração para um melhor desempenho das investigações dos crimes cibernéticos, caracterizando flagrante, denomina falha do Estado, em sentido amplo, em propiciar um melhor abastecimento dos seus agentes com as “armas” necessárias ao embate contra os infratores do mundo virtual. (Fragoso, 1963).

Com isso, o ideal é que haja uma melhor preparação dos agentes responsáveis pela persecução penal, bem como o desenvolvimento de uma melhor estrutura organizacional do aparelhamento da polícia investigativa, a fim de que o Estado possa prestar o devido amparo aos cidadãos aos *cibercriminosos*.

4 CIBERCRIMES E SEUS REFLEXOS NO DIREITO BRASILEIRO

4.1 Lei nº 12.737/2012: lei Carolina Dieckmann

Em 2011, a atriz Carolina Dieckmann teve diversas fotos íntimas subtraídas do seu laptop particular, e foi coagida para tê-las de volta. Como ela decidiu não ceder à chantagem, suas imagens acabaram sendo publicadas no âmbito virtual, tornando-se inevitável associar esse evento, que envolvia uma conduta lesiva que utilizava um meio informatizado, ao projeto de lei, que passou então a ser conhecido, após sua aprovação, como Lei Carolina Dieckmann. (Oliveira, 2022).

Após esse evento, que gerou grande repercussão na mídia nacional, o legislador deparou numa situação em que não podia mais adiar a aprovação dos projetos de lei que estavam em tramitação e versavam sobre os crimes de informática. Desse modo, foram aprovadas e sancionadas as Leis 12.735 e 12.737, ambas em 30 de novembro de 2012. (Brasil, 2012).

A tipificação dos crimes informáticos está prevista no primeiro artigo do referido diploma legal, mas, valendo-se da hermenêutica jurídica, onde se lê “crimes informáticos”, devem ser interpretados como “crimes cibernéticos”. Já o seu segundo artigo, por sua vez, realizou alterações na seção IV do Código Penal brasileiro, que trata dos crimes contra a inviolabilidade dos segredos, visto que se acrescentou ao código penal os artigos. 154-A e 154-B. Destaca-se que ambos os artigos de Lei buscam se precaver de quaisquer violações os dispositivos informáticos, senão vejamos:

> Art. 154 – A – Invadir dispositivos informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena – detenção, de 3(três) meses a 1 (um) ano, e multa.
> §1° Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> §2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> §3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a

> conduta não constitui crime mais grave.
> §4º Na hipótese do §3º aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
> §5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> Presidente da República, governadores e prefeitos;
> Presidente do Supremo Tribunal Federal;
> Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou da Câmara Municipal; ou Dirigente máximo da administração direita e indireta federal, estadual, municipal ou do Distrital Federal. (Brasil, 2012).

O caput do dispositivo acima transcrito (Art. 154-A do CP) pode ser considerado o maior avanço proporcionado por essa norma. Isso porque, o legislador visou realizar o combate às principais práticas danosas, denominadas por trazerem transtorno para quem se utiliza ou necessita dessas tecnologias. (Cabette, 2014).

Ademais, os artigos inseridos no código penal brasileiro pela Lei 12.337/12 buscam enfrentar a invasão de dispositivos informáticos alheios, conectados ou não à rede de computador. Importante salientar que se entende por dispositivos informáticos: computador de mesa, *notebook, laptop, ultrabook, tablete, Ipad, smartphone* e etc. O tipo penal indica, ainda, a necessidade de o dispositivo informático possuir algum mecanismo de segurança, sob pena de ser considerado desprotegido penalmente. (Nucci, 2013).

Dessa forma, tem-se, então, que para haver a conduta tipificado do referido artigo o sujeito ativo deverá invadir, violar, ou transgredir o dispositivo alheio, sem precisar necessariamente estar conectado à rede de computadores, e com a finalidade de obter, adulterar ou destruir dados ou informações.

Além do mais, na previsão trazida pelo §1º, o qual insere como condutas do tipo normativo produzir, oferecer, distribuir, vender ou difundir, constituem práticas que dependem das condutas típicas previstas no caput do artigo 154-A, ou seja, para cometimento dos ilícitos tipificados nesse parágrafo o sujeito deverá reunir elementos objetivos e subjetivos do tipo. Agora, ao tratar do terceiro artigo da mencionada lei, o qual alterou a redação do art. 266 do CP, incluindo a figura do tipo normativo o serviço informático, telemático ou de informação de utilidade pública, prevendo, ainda, que a interrupção ou perturbação das novas formas de comunicação seja crime. (Oliveira, 2022).

Cabe denotar que, o quarto artigo da Lei “Carolina Dieckmann”, por fim, traz consigo disposições acerca da *vacatio legis,* estipulando que a norma entraria em vigor em 120 dias a partir da sua publicação. (Costa, 2012).

4.2 Lei n° 12.965/2014: marco civil da internet

Visando estabelecer princípios, garantias, direitos e deveres para a utilização da internet no Brasil, foi aprovada a Lei nº 12.965/14, denominada de Marco Civil da Internet, que propunha eximir a ausência de normas no mundo virtual.

A situação pré-Marco Civil era de completa ausência de regulamentação civil da internet no país. Diferentemente do que alguns entusiastas libertários poderiam achar, a ausência de leis nesse âmbito não representa a vitória da liberdade. Ao contrário, gera uma grande insegurança jurídica. Uma das razões é que juízes e tribunais, sem um padrão legal para a tomada de decisões sobre a rede, acabam decidindo de acordo com regras muitas vezes criadas *ad hoc*, ou conforme as suas próprias convicções, resultando em inúmeras decisões judiciais contraditórias. (Lemos, 2014).

Cabe salientar que o Marco Civil, apesar de primordialmente a tutela dos direitos civis da internet, também tem aplicação no Direito Penal e Processual Penal, uma vez que estabelece conceitos fundamentais, bem como disciplina formas de obtenção de provas quanto à materialidade e à identificação da autoria delitiva.

Popularmente conhecida como Constituição da Internet Brasileira, o Marco Civil da Internet trouxe consigo uma maneira mais sistemática de princípios objetivos para definir em lei os direitos provenientes da utilização da internet, tais como garantias, direitos e deveres versando sobre o que se pode ou não fazer no âmbito civil, antes de se criminalizar condutas cometidas no âmbito virtual. A lei do Marco Civil priorizou princípios como: liberdade, privacidade e Direitos Humanos; governabilidade democrática e colaborativa; universalidade; inovação; segurança e funcionalidade; ambiente padronizado e regulatório.

Os princípios ganham destaque expressamente no art. 3º do Marco Civil da Internet:

- Garantia da liberdade de expressão, comunicação e manifestação do pensamento, nos termos da Constituição Federal.

- Proteção da privacidade.

- Proteção dos dados pessoais, na forma da lei.

- Preservação e garantia da neutralidade de rede

- Preservação da estabilidade, segurança e funcionalidade.

- Responsabilização dos agentes de acordo com suas atividades, nos termos da lei.

- Liberdade dos modelos de negócios promovidos na internet desde que não conflitem com os demais princípios estabelecidos nesta lei.

A preocupação com o amparo aos usuários da internet mais uma vez manifestada no diploma legal, garantindo-lhes voz na rede, seja assegurando-lhes acesso seguro e de qualidade ao mundo digital. Com a conceitualização trazida pelo Marco Civil, é possível padronizar ofícios, petições, mandados judiciais, bem como compreender de forma mais cristalina a dinâmica do ambiente virtual, em termos gerais:

No art. 5 estão elencados alguns conceitos:

I. Internet

A rede mundial de computadores ou internet possui definição técnica, sendo: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes. Ou seja, de um modo mais amplo, pode-se dizer que se trata de um conjunto de redes interligadas entre si, com alcance global, onde trafegam dados diversos, de características públicas ou privadas. (Brasil, 2014).

II. Terminal

O terminal é o computador ou qualquer dispositivo que se conecta internet, tais como celular, *notebook, laptop, tablet,* etc.

III. Endereço de protocolo

O endereço de IP é o código atribuído a um terminal (computador, por exemplo) de uma rede para autorizar sua identificação, definido segundo parâmetros internacionais. Para um terminal se conectar à internet, deve contar com um provedor de conexão, o qual realizará a atribuição ou autenticação de um endereço de IP, que estará disponível do usuário durante toda a conexão.

IV. Administrador de sistema autônomo

É a pessoa física ou jurídica cujo administra blocos de endereço de IP específicos e o respectivo sistema autônomo de roteamento, o qual deve ser cadastrado no Registo.br, que é o responsável pelas atividades de registro e manutenção dos nomes de domínio.

V. Conexão à internet

Foi definida como habilitação de um terminal (computador, celular, *tablet*) para envio e recebimento de pacotes de dados pela internet, por intermédio autenticação de um endereço de IP.

VI. Registro de conexão

O conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração, o endereço de IP utilizado pelo terminal para o envio e recebimento de pacotes de dados, além do fuso horário respectivo, formam os registros de conexão.

VII. Aplicações de Internet

Tem-se por aplicações de internet o conjunto de funcionalidades que podem ser disponibilizadas por intermédio de um terminal conectado à internet, como, por

exemplo, sites de bancos, redes sociais, contas de e-mails, entre outros.

4.3 Lei nº 13.709/18: lei de proteção de dados

Em uma recente pesquisa realizada em 2019 pela Serasa Experian (2019), denota que 75% dos brasileiros desconhecem ou conhecem bem pouco acerca da Lei de Proteção de Dados. É uma normativa tida como revolucionária, um marco jurídico-regulatório na legislação brasileira que, após sucessivos adiamentos, passou a vigorar em setembro de 2020. Acerca do tema, Bioni afirma:

> Os dados pessoais de um indivíduo formam um perfil a seu respeito para a tomada de inúmeras decisões. [...]. Na famosa expressão de Eli Pariser, há uma bolha que, como um filtro invisível, direciona desde a própria interação do usuário com outras pessoas em uma rede social até o acesso e a busca por informação na rede. Doutrina-se a pessoa com um conteúdo e uma informação que giram em torno dos interesses inferidos por intermédio dos seus dados, formando-se uma bolha que impossibilita o contato com informações diferentes. (Bioni, 2019, p.40).

Ela traz consigo a denominação do que são dados pessoais conforme exposto no seu art. 5º, inciso I, considerando que um dado pessoal é aquela informação relacionada a pessoa natural identificado ou identificável. No mesmo art. 5º, inciso II, identifica o que é dado pessoal sensível, que está ligado a origem racial ou étnica religiosidade, escolhas políticas, opção sexual ou dado referente à saúde. Entretanto, no seu art. 14, a legislação dispõe que o tratamento de dados pessoais sobre crianças e adolescentes, caberá a realização consoante autorização dos pais ou responsáveis legais. (Brasil, 2021).

4.4 Adesão do Brasil à convenção de Budapeste

A cooperação jurídica internacional é um mecanismo auxiliador dos Estados para am- parar o funcionamento da justiça em seus territórios, “por meio do qual um Estado, para fins de procedimentos no âmbito da jurisdição, solicita a outro Estado medidas administrativas ou judiciais que tenham caráter judicial em pelo menos um desses Estados.” (Brasil, 2021).

Criada em 2001, os Estados membros do Conselho da Europa, juntamente com outros países, que hoje totalizam sessenta e dois signatários, realizaram a Convenção de Budapeste para criar uma política criminal comum de confronto e repressão aos delitos “com objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional”. (Bioni, 2019, p.40).

Sua criação visa frear uma constante e crescente onda de ataques virtuais aos internautas da rede mundial de computadores, bem como uma adequação e uniformização de legislações dos países contra essas condutas criminosas.

Ademais, pelo caráter transnacional do cibercrime, a jurisdição de cada país poderia interferir nas investigações, pois a simples coleta de dados poderia ser encarada como uma violação à soberania territorial do país onde se tem o alvo das investigações. Nesse contexto, a Convenção da Budapeste surge para erradicar conflitos territoriais, delimitar a legislação acerca da matéria, melhoras técnicas de confronto, e repressão aos delitos, além de uma cooperação jurídica internacional entre os países filiados. (Kethineni, 2020).

O documento aborda documentos com diferentes temas, com orientações que denotam uniformizar as medidas adotadas pelos países signatários. Destaca-se no texto do tratado a precaução com as mudanças provocadas pelo advento do mundo digital e a globalização, que acarretam no uso desse mecanismo para cometimento de delitos. (Brasil, 1988).

Do mesmo modo que, a Convenção se deu ao trabalho de banalizar os bens jurídicos tutelados, quais sejam, o da segurança da informação e vida privada dos usuários da rede, confiabilidade, integridade e disponibilidade de sistemas informáticos.

4.5 Posicionamento dos Tribunais Superiores

Com a inovação do assunto, a jurisprudência dos Tribunais Superiores vem cada vez mais se consolidando em julgados para tratar de casos no âmbito digital.

Como exemplo, tem- se o julgado a respeito do conflito de competência praticado por meio de redes sociais.

Conflito de competência. Crime de ameaça praticado por WhatsApp e

> facebook. Âmbito de aplicação da Lei Maria da Penha. Delito formal. Consumação no local onde a vítima conhece das ameaças. Conflito de competência conhecido. Declarada a competência do juízo suscitado. 1. O crime de natureza formal, tal qual o tipo do art. 147 do Código Penal, se consuma no momento em que a vítima toma conhecimento da ameaça. 2. Segundo o art. 70, primeira parte, do Código de Processo Penal, "A competência será, de regra, determinada pelo lugar em que se consumar a infração". 3. No caso, a vítima tomou conhecimento das ameaças, proferidas via WhatsApp e pela rede social Facebook, na Comarca de Naviraí, por meio do seu celular, local de consumação do delito e de onde requereu medidas protetivas. 4. Independentemente do local em que praticadas as condutas de ameaça e da existência de fato anterior ocorrido na Comarca de Curitiba, deve-se compreender a medida protetiva como tutela inibitória que prestigia a sua finalidade de prevenção de riscos para a mulher, frente à possibilidade de violência doméstica e familiar. (Brasil, 2021).

O relator ministro Ribeiro Dantas, ao julgar o conflito de competência do caso exposto, utilizou-se do artigo do Código de Processo Penal e estabeleceu que em regra a competência será determinada pelo lugar em que se consumar a infração.

No âmbito das fraudes praticadas pela internet, é importante mencionar conflito de competência nº 145.576, julgado pelo Superior Tribunal de Justiça:

> Conflito negativo de competência. Penal e processual penal. Furto mediante fraude. Transferência bancária via internet sem o consentimento da vítima. Consumação no local da agência onde o correntista possui a conta fraudada. Competência do juízo suscitado. 1. A Terceira Seção desta Corte Superior firmou o entendimento no sentido de que a subtração de valores de conta corrente, mediante transferência fraudulenta, utilizada para ludibriar o sistema informatizado de proteção de valores, mantidos sob guarda bancária, sem consentimento da vítima, configura crime de furto mediante fraude, previsto no art. 155, § 4º, inciso II, do Código Penal - CP. 2. O delito em questão consuma-se no local da agência bancária onde o correntista fraudado possui a conta, nos termos do art. 70 do Código de Processo Penal – CPP. (Brasil, 2021).

Em relação ao furto mediante fraude, praticado por transferência bancária pela internet, o Superior Tribunal de Justiça decidiu que o delito se consumou no local da agência bancária, onde o correntista fraudado possuía a conta. O STJ tem interpretado normas infraconstitucionais em relação aos ilícitos praticados pela rede (Brasil, 2018).

O tribunal, por exemplo, decidiu manter preso preventivamente um homem

que usou a internet para obter fotos e vídeos com conteúdo erótico e depois extorquiu mulheres para não divulgar as imagens. Por meio das mídias sociais, um rapaz de 19 anos compelia jovens (algumas menores de idade) a enviar fotos e vídeos íntimos e depois exigia que elas lhe entregassem dinheiro e outros bens para não divulgar o material na internet.

Ele também estendia as ameaças às famílias das vítimas. Para o ministro Rogerio Schietti Cruz (2018), relator do caso, ficou nítido que o acusado se aproveitou da vulnerabilidade das vítimas no ambiente virtual para exigir os valores, que eram cada vez mais altos a cada ato de extorsão.

Ao negar pedido de Habeas Corpus, Schietti (2018) destacou que os crimes sexuais virtuais são impulsionados pela oportunidade do anonimato e, independentemente dos aspectos que permeiam a vida pessoal e socioeconômica do criminoso, estariam “diretamente relacionados ao comportamento sexista, comumente do gênero masculino”. O processo está em segredo de Justiça.

Nas hipóteses de ameaças feitas por redes sociais como o Facebook e aplicativos como o WhatsApp, o STJ tem decidido que o juízo competente para julgamento de pedido de medidas protetivas será aquele de onde a vítima tomou conhecimento das intimidações, por ser este o local de consumação do crime previsto no artigo 147 do Código Penal.

Com base nesse entendimento, a 3ª Seção do STJ, fixou a competência da comarca de Naviraí (MS) para a análise de pedido de concessão de medidas protetivas em favor de mulher que teria recebido pelo WhatsApp e Facebook mensagens de texto com ameaças de pessoa residente em Curitiba (CC 156.284).

O relator, ministro Ribeiro Dantas, destacou que o artigo 70 do Código de Processo Penal estabelece que a competência será, em regra, determinada pelo lugar em que se consumar a infração. (Brasil, 2018).

O STJ tem adotado a tese de que é ilícita a prova obtida diretamente dos dados armazenados no celular do acusado. A jurisprudência do tribunal entende que são inválidas mensagens de texto, SMS e conversas por meio de aplicativos como o WhatsApp obtidas diretamente pela polícia no momento da prisão em flagrante, sem prévia autorização judicial.

4.6 Desafios apresentados:

A lei nº 12.737, de 30 de novembro de 2012, intitulada Carolina Dieckmann, trouxe alterações no Código Penal vigente, acrescentando os artigos 154-A e 154-B, assim, originou-se o tipo penal “Invasão de dispositivo informático”, apresentando-se desta forma:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput
> § 2o Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4o Na hipótese do §3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas. (Brasil, 2012).

De acordo com Ângelo (2018), o bem jurídico amparado por estes artigos é a inviolabilidade dos dados informáticos. Busca-se preservar, desta forma, a privacidade e intimidade, constadas no artigo 5º da Constituição Federal de 1988. O sujeito ativo é qualquer indivíduo que não está licenciado ao acesso as informações. Já o sujeito passivo é qualquer pessoa, podendo esta ser física ou jurídica, proprietária dos dados computacionais. Porém, uma das maiores críticas acerca da lei encontra-se no sujeito ativo, pois é atípica a conduta de pessoa que invade aparelho computacional próprio para obter dados de outrem que lá estejam, por exemplo, em uma *Lan House*, o proprietário não irá cometer crime se acessar as informações do locador do computador.

Desta forma, há falha na lei, pois quem cometeu o crime deveria ser punido, não devendo importar quem quer que o praticou. Outra falha, ou melhor, lacuna, apresentada por esta lei, encontra-se nos “mecanismos de segurança”, uma vez que um usuário inexperiente que não faz uso de aparatos de segurança, como antivírus

ou senhas de acesso, não será amparado pelos artigos, sendo o crime atípico. Além destas falhas, temos a pena apresentada, que é detenção de três meses a um ano, portanto, considerada uma conduta de médio potencial ofensivo. Ademais, este tipo de penalidade permite o cumprimento no regime semiaberto ou imediatamente no regime aberto, podendo até mesmo com base no artigo 44, §2º do Código Penal, ser substituída por pena pecuniária. (Brasil, 2012).

Há, também, chance de ser substituída por pena alternativa ou restritiva de direitos. Desta forma, uma conduta que pode causar danos irreparáveis a suas vítimas, tem uma punição branda e pouco impactante. No ano de 2014, foi sancionada a Lei nº 12.965, intitulada “Marco Civil da Internet”. Esta foi produzida com o intuito de preencher as lacunas de nosso sistema jurídico no tocante aos crimes virtuais. Inicialmente, trata dos fundamentos e conceitos, elencando os direitos dos usufruidores. Tipifica princípios, tais como liberdade, neutralidade e privacidade, além de determinar garantias, direitos e deveres no ambiente virtual. Um destaque se dá ao direito e garantia a inviolabilidade da intimidade e da vida privada. (Bioni, 2019, p. 40).

Contudo, sabemos que no momento de punição ao desrespeito de tais princípios as penas são plácidas e não atingem um resultado satisfatório. Além disto, para requisições de informações privadas é necessária ordem judicial, não podendo o provedor da internet fornecer dados como IP, senha e login dos criminosos, deixando o trabalho de investigação moroso. Por mais válida que seja a tipificação de garantias e direitos, tais artigos não abarcam por completo o campo de atividade dos criminosos virtuais, ficando as lacunas à mercê de suprimento advindo de outras legislações, como por exemplo, casos de compras on-line, que são regulamentadas pelo CDC (Código de Defesa do Consumidor).

Desta forma, a falta de uma legislação específica aos crimes cibernéticos no Brasil traz, em muitos casos, a impunidade dos criminosos, uma vez que determinadas condutas não são tipificadas e as que são, tal como a lei nº 12.737/12, traz lacunas e dúbias interpretações. Com o avanço tecnológico e o crescente número de usuários, se torna indispensável a criação de uma lei que defina as condutas criminosas praticadas no meio virtual, com penas destinadas aos seus agentes proporcionais aos resultados danosos que estes produzem.

4.7 Dificuldade na determinação da autoria destes crimes

Ocorre que, nos crimes cibernéticos a imputação objetiva ao autor do crime e sua com- provação é muito difícil frente à ausência física do sujeito ativo, pois em sua maioria utilizam dados inverídicos de endereço de suas máquinas, ocorrendo assim uma camuflagem dos dados, que somente com uma investigação detalhada é possível se chegar aos criminosos.

E frente à importância da identificação do autor do crime, surgiu a necessidade de se criar um perfil denominado para esses grupos que praticam determinados crimes virtuais, dentre essas nomeações temos a figura do hacker. (Bioni, 2019, p. 40).

> Os hackers, sujeitos com conhecimentos especiais de informática, eletrônica e redes de computadores, são, em geral, os responsáveis pela maioria dos delitos cometidos com o uso dos computadores e da internet. (Bioni, 2019, p. 40).

Ou seja, os hackers são pessoas que acessam sistemas computacionais para modificar softwares, hardwares e aplicam seus conhecimentos para desenvolver e adaptar soluções de segurança e apontar possíveis falhas nesses sistemas, bem como para prejudicar terceiro.

4.8 Conflito de competência

Ângelo conceitua competência como,

> “a delimitação, previamente estabelecida em lei, desse poder de julgar”, e continuando neste raciocínio, afirma ser “o espaço, legislativamente delimitado, dentro do qual o órgão estatal, investido do poder de julgar, exerce sua jurisdição.” (Ângelo, 2018, p34).

Faz-se necessário para uma correta interpretação acerca da determinação da competência de julgamento dos crimes cibernéticos, entender primeiramente qual o lugar que se considera para fins jurídicos, como sendo o local onde são cometidos tais crimes, seja por meio da internet/dispositivos ou contra estes, uma vez que os crimes desta seara, são capazes de ultrapassar os limites territoriais internos do nosso país, e ainda torna-se importante verificar qual o tempo de realização desse

tipo de crime. (Ângelo, 2018, p34).

5 CONSIDERAÇÕES FINAIS

O trabalho teve como principal objetivo demonstrar como a cooperação jurídica internacional e, especialmente, a Convenção de Budapeste, o mais importante tratado sobre cibercrime, são mecanismos indispensáveis na pressão dos crimes cibernéticos no Brasil. Em uma sociedade extremamente conectada, a ocorrência de ilícitos no meio digital cresce exponencialmente no dia a dia, conforme o ser humano fica mais dependente da internet e de dispositivos eletrônicos, seja para o uso profissional ou pessoal. É quase impossível imaginar uma sociedade sem as facilidades que a internet proporciona.

Pode-se afirmar que o Brasil, embora seu esforço exorbitante na criação de leis que busquem auxiliar a segurança nacional, como o Marco Civil da Internet, a Lei Geral de Proteção de Dados e as novas leis que preveem as mais recorrentes condutas delitivas no ciberespaço, ainda assim, não dispõe de meios suficientes para coibir de forma eficaz a prática de crimes informáticos, por diversos fatores, como ausência de criminalização de alguns ataques cibernéticos considerados pertinentes, por carência da estrutura tecnológica da polícia judiciária para realizar investigações ou, ainda, pela morosidade da justiça.

Desse modo, mesmo na perspectiva da política de controle, não basta uma legislação que incrimine determinadas condutas ilícitas, enquanto persiste uma série de entraves à persecução penal, como é o caso da adoção de teoria territorial incompatível com a modalidade de crime cibernético e a redação das normas que reproduzem interpretações dúbias, como a do artigo 154-A do Código Penal, por exemplo. Frisa-se, não há de se olvidar que o Direito Penal configura como *última ratio* no ordenamento jurídico e se está longe de querer transpassar um viés exclusivamente punitivista com o presente trabalho.

Todavia, também não se pode desconsiderar que muitas condutas criminosas no meio virtual ainda apresentam ameaças e não possuem tipificações, abrindo espaço para a impunidade dessas ações, e outras que seque são conhecidas ainda, tendo em vista que em se tratando de tecnologia, informática e meio virtual, todos os dias se descobre novidades. Baseado em tudo isso, o investimento em capacitação e estrutura tecnológica também representa grande parte no objetivo.

Existem diversos instrumentos que podem ser usados para diminuir a

incidência dos crimes cibernéticos, como, por exemplo, a criação de um grupo especializado em diversas áreas do conhecimento, para que possam analisar as qualidades e deficiências legislativas, propondo maneiras mais eficazes de assegurar a proteção do sistema e dos usuários; a promoção de cursos, em instituições educativas, enfatizando sobre os riscos existentes na internet e sobre posturas éticas que devem ser seguidas quando se está conectado em uma rede; a instalação de medidas de segurança aos usuários, a criação de agências especializadas na repressão dos crimes, dentre outras medidas.

O Brasil tem capacidade e poderio financeiro para reprimir a marginalidade cibernética. Nos últimos anos, um grande avanço no arcabouço legislativo interno de preocupação com a segurança virtual, que tem aptidão de incorporar a Convenção de Budapeste em seu ordena- mento, o que promoverá apenas benefícios aos pais. Por outro lado, a criação, em âmbito nacional e internacional, de divisões policiais especializadas na investigação de cibercrimes permitiria a concentração de esforços e o compartilhamento de *know-how* tecnológico específico, os quais convergiriam ao favorecimento do combate e prevenção de crimes cibernéticos.

A realização de uma investigação preliminar no espaço *cibernético*, por intermédio de unidades policiais de investigação especializadas em crimes informáticos, asseguraria a manutenção da integridade de vestígios e provas simultaneamente em que possibilitaria a adequação dos organismos policiais à velocidade dos crimes digitais.

Deve-se levar em consideração, todavia, que a busca incansável por indícios de autoria e materialidade delitiva pode ensejar o transgressor e a violação de direitos e garantias fundamentais como privacidade e o devido processo legal.

Com isso, só haveria o sobrepujamento da via célere em detrimento de valores consolidados na Constituição Federal como inerentes ao sujeito que é alvo de qualquer investigação.

REFERÊNCIAS

ÂNGELO, Ana Elisa; SANCHES, Ademir Gasques. **Insuficiência das leis em relação aos crimes cibernéticos no Brasil.** 2018 p.34 - ed 2. Disponível em: https://jus.com.br/artigos/66527/insuficiencia- das-leis-em-relacao-aos-crimes-ciberneticos, 2018. Acesso em: 15 dez.2023.

BENSON, V; MCALANEY, J; FRUMKIN, L. A. Emerging Threats for the Human Element and Countermeasures in Current Cyber Security Landscape. In **Psychological and Behav- ioral Examinations in Cyber Security** (pp. 266-271). IGI Global, 2018.

BIONI, Bruno Ricardo. **Proteção de dados pessoais e os limites do consentimento**. Editora Forense – ed. 05, p.40, publicado em 2019.

BRANCO, D. C. **Esses são 5 principais métodos usados pelos criminosos para roubar se- nhas,** 2022. Canaltech. Disponível em: https://canaltech.com.br/seguranca/esses-sao-5-princi- pais-metodos-usados-pelos-criminosos-para-roubar-senhas-207181/. Acesso em: 10 fev. 2024.

BRASIL. **Decreto-lei nº 3.688**, de 3 de outubro de 1941. Lei das Contravenções Penais. Disponível em: https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-3688-3-outu- bro-1941-413573-publicacaooriginal-1-pe.html#:~:text=Dolo%20e%20culpa-,Art.,de%20outra%2C%20qualquer%20efeito%20jur%C3%ADdico. Acesso em: 17 fev. 2024.

_____. **Decreto-Lei nº 3.689**, de 3 de outubro de 1941. Código de Processo Penal.

_____. **Constituição da República Federativa do Brasil de 1988**. Brasília: Palácio do Planalto, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constitui- cao.htm. Acesso em: 18/01/2024.

_____. Ministério da Ciência e Tecnologia. Secretaria de Política de Informática e Automação. **Evolução da internet no Brasil e no mundo**. 2000.

CANAL CIÊNCIAS CRIMINAIS. **Cybercrime x cyberbullying**. 2017. Https://canalcienci- ascriminais.jusbrasil.com.br/artigos/547931721/cybercrime-x-cyberbulying. Acesso em: 14 dez. 2023.

CARDOSO, Lucas de Holanda M. **O direito na era digital**: O Cibercrime no Ordenamento Jurídico Brasileiro. 2017. Disponível em: 1611400792P734.pdf (femanet.com.br) Acesso em: 20 jan. 2024.

CASTRO, Aldemario Araujo. **A internet e os tipos penais que reclamam ação criminosa em público**. 2022, p. 31. Disponível em: http://egov.ufsc.br/portal/sites/default/files/anexos/13308-13309- 1- PB.pdf. Acesso em: 20 jan.2024.

_____. **Internet e os Tipos Penais que Reclamam Ação Criminosa em Público.** Disponível em: Webly.com.br/fórum/lofiversion/index.php/t11293.html>. Acesso em 20 jan. 2024.

COLHADO, J. G. **Conceito de Crime no Direito Penal brasileiro**. 2016. Disponível em: https://jus.com.br/artigos/47517/conceito-de-crime-no-direito-penal-brasileiro. Acesso em: 20 jan.2024.

CORRÊA, Gustavo Testa. **Aspectos jurídicos da Internet**. 5ª Ed. p. 205 - São Paulo: Saraiva, 2011.

CUNHA, Rogério Sanches. **Manual de Direito Penal**: Parte Geral. 4ª Edição. Salvador: Jus- PODIVM, 2016.

DAOUN, Alexandre Jean.; BLUM, Renato Opice. Cybercrimes. In: LUCCA, N.; SIMÃO FI- LHO, A. (coord.). **Direito e internet**: aspectos jurídicos relevantes. Bauru: Edipro, 2000. P,34.

DIAS, V. M. A problemática da investigação do cibercrime. DATAVENIA. **Revista Jurídica Digital**. Ano 1. N.º 01. julho-dezembro 2012. Disponível em: https://www.datavenia.pt/fi- cheiros/edicao01/datavenia01_p063-088.pdf. Acesso em: 25 jan. 2024.

DUFFER, C. **Aprendendo Pentest com Python.** Ed: Novatec. São Paulo, 2016.

ESTADÃO. **Crimes Virtuais afetam 42 milhões de brasileiros**. 2017. Disponível em: https://economia.estadao.com.br/noticias/releases-ae,crimes-virtuais-afetam-42-milhoes-de- brasileiros,70001644185. Acesso em: 28 jan.2024.

ESTEFAM, André; GONÇALVES, Victor Eduardo Rios. Direito Penal Esquematizado: Parte Geral. Coord. Pedro Lenza. São Paulo: Saraiva, 2012, p.98.

FRAGOSO, Heleno Claudio. **Lições de direito penal**: Parte Especial. Rio de Janeiro: Forense, 1983.

GARCIA, P. S. et al. **A influência da injustiça organizacional na motivação para a prática de crimes cibernéticos**. ISTEM J. Inf.Syst. Technol. Manag. 15; 2018.
Disponível em: https://www.sci-elo.br/j/jistm/a/3Qj7Xvdg9Sd3T6RFNHvSbWB/?lang=pt. Acesso em: 21 jan. 2024.

GERCKE, M. **Understanding cybercrime**: Phenomena, challenges and legal response. ITU Telecommunication Development Sector, 380. 2014.

GOMES, Flávio Luiz. **Crimes informáticos**. Disponível em: <www.direitocriminal.com.br>. Acesso em: 30 mar. 2024.

HAUSER, Ester Eliana. **Política Criminal**. Ijuí, 2010.

INELLAS, Gabriel César Zaccaria de. **Crimes na Internet.** 2ª ed., atualizada e ampliada. São Paulo: Editora Juarez de Oliveira, 2009, p. 58.

JESUS, Damásio de; MILAGRES, José Antonio. **Manual de crimes informáticos** p. 28, São Paulo: Saraiva, 2016;

KETHINENI, Sesha; CAO, Ying. The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. **Sage Journals**, v. 30, n. 3, set. 2020. DOI: https://doi.org/10.1177/1057567719827051. Disponível em: https://journals.sage-pub.com/doi/abs/10.1177/1057567719827051. Acesso em: 30 mar. 2024.

KINAST, P. **10 golpes mais comuns na internet**. Oficina da net. 2022. Disponível em: https://www.oficinadanet.com.br/internet/39464-golpes-mais-comuns-internet. Acesso em: 30 mar. 2024.

LEMOS, Ronaldo; LEITE, George Salomão (Coords.). **Marco Civil da Internet**. São Paulo: Atlas, 2014.

LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional**. Campi- nas, SP: Ed. Millennium, 2005.

LINS, B. F. E. **A evolução da internet**: uma perspectiva histórica. Associação dos Consulto- res Legislativos e de Orçamento e Fiscalização Financeira da Câmara dos Deputados, 2013-04.

MORAES, Alexandre de. **Direitos Humanos Fundamentais**: Teoria geral, comentários aos arts. 1º a 5º da Constituição da República Federativa do Brasil, doutrina e jurisprudência. 8ª Ed. São Paulo: Saraiva, 2007.

NUCCI, Guilherme de Souza. **Manual de direito penal**. 9.ed. São Paulo: Revista dos Tribunais, 2013, p 38-60;

OLIVEIRA, Anderson Soares Furtado. **Crime por Meios Eletrônicos**. Brasília: Universidade Gama Filho, 2009.

PINHEIRO, Patrícia Peck. **Direito Digital**. 3ª Ed. São Paulo: Saraiva, 2009. p. 22.

RAMOS, J. E. M. **História da Internet**. Sua pesquisa. com. 2020. Disponível em: https://www.suapesquisa.com/internet/. Acesso em: 20 mar. 2024.

REINALDO FILHO, Demócrito. **O projeto de lei sobre crimes tecnológicos (Pl nº 84/99)**. 2004. Disponível em: https://jus.com.br/artigos/5447/o-projeto-de-lei-sobre-crimes-tecnologi- cos-pl-n-84-99/2. Acesso em: 20 mar. 2024.

REVISTA COBERTURA. **Crimes Cibernéticos no Brasil**. Disponível em: http://www.re- vistacobertura.com.br/2018/02/19/brasil-e-segundo-pais-com-maior-numero-de-vitimas-de- crimes-ciberneticos/. Acesso em: 20 mar. 2024.

RODRIGUES, Silva. **Crimes de Informática**. São Paulo. BH Editora, 2008.

ROXIN, Claus. **A proteção de bens jurídicos como função do direito penal**. Porto Alegre: Livraria do Advogado, 2006, p. 30.

SILVA, Rita de Cássia Lopes da. **Direito penal e sistema informático**. São Paulo: Revista dos Tribunais, 2003.

SOUZA, T. **História da Internet**: quem criou e quando surgiu. Toda matéria. 2022. Disponível em: Https://www.todamateria.com.br/historia-da-internet/. Acesso em: 20 mar. 2024.

TERCEIRO, Cecilio da Fonseca Vieira Ramalho. **O problema na tipificação penal dos cri- mes virtuais**. 2022, p.07 Disponível em: <http://jus.uol.com.br/revista/texto/3186/o-problema-na-tipifi- cacao-penal-dos-crimes-virtuais>. Acesso em: 15 mar. 2024.

VIANA, A. P. **Crimes virtuais e a necessidade de uma legislação específica**. 2017, p. 54. http://www.egov.ufsc.br/portal/conteudo/crimes-virtuais-e-necessidade-de-uma-le- gisla%c3%a7%c3%a3o-especifica. Acesso em: 20 mar. 2024.