UNIVERSIDADE FEDERAL DA PARAÍBA – UFPB
CENTRO DE CIÊNCIAS JURÍDICAS
DEPARTAMENTO DE CIÊNCIAS JURÍDICAS
TRABALHO DE CONCLUSÃO DE CURSO

ANÁLISE CRÍTICA DO PAPEL DA VÍTIMA NOS CRIMES CIBERNÉTICOS E DOS DESAFIOS DO CONTROLE PENAL

LUCAS QUEIROGA NÓBREGA DE SOUSA

SANTA RITA
2023

LUCAS QUEIROGA NÓBREGA DE SOUSA

ANÁLISE CRÍTICA DO PAPEL DA VÍTIMA NOS CRIMES CIBERNÉTICOS E DOS DESAFIOS DO CONTROLE PENAL

Trabalho de Conclusão de Curso apresentado ao Curso de Direito do Departamento de Ciências Jurídicas da Universidade Federal da Paraíba, como exigência parcial da obtenção do título de Bacharel em Ciências Jurídicas.

Orientadora: Profa. Dra. Ana Clara Montenegro Fonseca

SANTA RITA

2023

Catalogação na publicação
Seção de Catalogação e Classificação

S725a Sousa, Lucas Queiroga Nóbrega de.
Análise crítica do papel da vítima nos crimes cibernéticos e dos desafios do controle penal / Lucas Queiroga Nóbrega de Sousa. - Santa Rita, 2023.
76 f.

Orientação: Ana Clara Montenegro Fonseca.
Monografia (Graduação) - UFPB/CCJ/DCJ.

1. Crimes cibernéticos. 2. Vitimodogmática. 3. Vulnerabilidade da vítima. 4. Segurança cibernética. 5. Política criminal. I. Fonseca, Ana Clara Montenegro. II. Titulo.

UFPB/DCJ/CCJ-SANTARITA CDU 34

Elaborado por ANA BEATRIZ DE OLIVEIRA ABRANTES SILVA - CRB-15/596

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS JURÍDICAS
DIREÇÃO DO CENTRO
COORDENAÇÃO DE MONOGRAFIAS
DEPARTAMENTO DE CIÊNCIAS JURÍDICAS
DISCIPLINA: TRABALHO DE CONCLUSÃO DE CURSO

CCJ Centro de Ciências Jurídicas

DISCIPLINA: TRABALHO DE CONCLUSÃO DE CURSO – TCC

ATA DA BANCA EXAMINADORA DA DEFESA PÚBLICA DO TRABALHO DE CONCLUSÃO DE CURSO

Ao vigésimo sétimo dia do mês de Agosto do ano de dois mil e vinte três, realizou-se a sessão de Defesa Pública do Trabalho de Conclusão do Curso de Direito intitulado "Análise crítica do papel da vítima nos crimes cibernéticos e dos desafios do controle penal", sob orientação do(a) professor(a) Ana Clara Montenegro Fonseca que, após apresentação oral, foi arguido pelos integrantes da Banca Examinadora que se reuniram, reservadamente, e decidiram emitir parecer favorável à Aprovação, de acordo com o art. 33, da Resolução CCGD/02/2013, do(a) aluno(a) Lucas Queiroga Nóbrega de Sousa com base na média final de 9,9 (nove vírgula nove). Após aprovada por todos os presentes, esta ata segue assinada pelos membros da Banca Examinadora.

Ana Clara Montenegro Fonseca

Ítalo Ramon Silva Oliveira

Werna Karenina Marques Souza

AGRADECIMENTOS

Agradeço a Deus, antes de tudo, por sempre iluminar os meus caminhos, revelando sempre o real sentido da vida e sendo o meu alicerce diante de todas as adversidades. Assim como agradeço a Nossa Senhora, por sua presença sublime em minha caminhada e por todas as graças que me foram proporcionadas através de sua intercessão.

Agradeço aos meus familiares, por toda fonte de incentivo inesgotável, especialmente aos meus pais e à minha irmã, Genésio, Eddy e Taysa, que são verdadeiros pilares em minha vida, cujo todo amor e generosidade refletem a luz da Sagrada Família de Nazaré em minha vida.

Agradeço aos meus professores e a cada um dos colaboradores do Departamento de Ciências Jurídicas da Universidade Federal da Paraíba. Agradeço, em especial, à minha orientadora, Profa. Dra. Ana Clara Montenegro Fonseca, por todo auxílio prestado ao longo desta etapa desafiadora, sempre amparando com preciosas contribuições durante suas orientações.

Agradeço à Giullia, pelos essenciais incentivos para que eu adentrasse na referida instituição de ensino e por todo encorajamento durante a minha trajetória acadêmica.

Agradeço aos meus amigos, que foram apoios essenciais ao longo de toda a minha graduação. Bem como, agradeço a todos que de forma direta ou indireta contribuíram para que eu alcançasse a conclusão deste importante ciclo.

RESUMO

Diante de uma crescente dependência da sociedade aos sistemas digitais, os crimes cibernéticos têm adquirido maior frequência e complexidade na era contemporânea. O presente trabalho teve como objetivo analisar as principais categorias que influenciam a participação e a vulnerabilidade da vítima na concretização dos crimes cibernéticos, estabelecendo uma conexão com os desafios enfrentados na aplicação do controle penal diante dessa realidade. Para tanto, a pesquisa explorou os efeitos gerados pelo desenvolvimento tecnológico sobre a autonomia dos usuários, partindo, em ato contínuo, para uma análise voltada ao viés vitimodogmático de Bernd Schunemann. Posteriormente, examinou-se a incógnita do risco no mundo virtual, fazendo referências a teorias funcionalistas moderadas, como a de Claus Roxin. Incluindo, em seguida, análises filosóficas e teóricas de Zygmunt Bauman, Pierre Lévy e Andy Clark acerca da complexidade dessa temática na contemporaneidade. Buscou-se ainda analisar o relevante papel da vítima no crime através de um viés doutrinário e, *a posteriori*, o estudo dedicou-se a discutir os impactos gerados pela vulnerabilidade da vítima em dissonância com a evolução normativa dos crimes cibernéticos, destacando os persistentes desafios no âmbito do controle penal e na identificação dos perpetradores. Investigando, seguidamente, a respeito de possíveis estratégias de prevenção e combate aos referidos crimes. A metodologia adotada baseou-se na abordagem lógico-dedutiva, mediante análises bibliográficas e documentais. Ademais, foram examinadas as medidas de mitigação dos riscos na busca do fortalecimento da segurança cibernética e da redução da ocorrência dos crimes cibernéticos, contribuindo para a discussão das atuais estratégias de política criminal no controle desta crescente criminalidade informática.

Palavras-chave: crimes cibernéticos; vulnerabilidade da vítima; vitimodogmática; autorresponsabilidade; autocolocação e heterocolacação em risco; política criminal; segurança cibernética.

ABSTRACT

In the face of a growing societal dependence on digital systems, cybercrimes have increased in frequency and complexity in the contemporary era. This study aimed to analyze the main categories influencing the participation and vulnerability of victims in the commission of cybercrimes, establishing a connection with the challenges faced in the application of criminal control in this reality. The research explored the effects of technological development on user autonomy, followed by an analysis focusing on the victimological bias of Bernd Schunemann. Subsequently, the enigma of risk in the virtual world was examined, referring to moderate functionalist theories such as Claus Roxin's. This was followed by philosophical and theoretical analyses by Zygmunt Bauman, Pierre Lévy, and Andy Clark regarding the complexity of this theme in contemporary times. The study also sought to analyze the significant role of the victim in the crime from a doctrinal perspective, and subsequently, the research focused on discussing the impacts generated by the vulnerability of the victim in dissonance with the normative evolution of cybercrimes, highlighting persistent challenges in the realm of criminal control and perpetrator identification. The investigation then delved into possible strategies for preventing and combating these crimes. The methodology adopted was based on a logical-deductive approach, involving bibliographical and documentary analyses. Additionally, risk mitigation measures were examined to strengthen cybersecurity and reduce the occurrence of cybercrimes, contributing to the discussion of current criminal policy strategies in controlling this growing form of criminality.

Key-words: cybercrimes; victim's vulnerability; victimodogmatics; self-responsibility; self-placement and hetero-placement at risk; criminal policy; cybersecurity.

SUMÁRIO

INTRODUÇÃO **9**

1. A CONDUTA DA VÍTIMA EM UMA SOCIEDADE VIRTUAL **13**

1.1 Breve histórico acerca da ascensão do paradigma virtual 13

1.2 O Impacto do mundo virtual na autonomia da vítima 17

1.3 Perspectiva vitimodogmática na abordagem de crimes cibernéticos com enfoque na vítima 21

2. A INCÓGNITA DO CONHECIMENTO DO RISCO NO MUNDO VIRTUAL 28

2.1 Reflexões acerca do risco virtual sob à ótica de teorias de Claus Roxin 28

2.2 Conscientização da vítima no ambiente virtual: Perspectiva filosófica contemporânea 35

2.3 A Relevância da conduta da vítima e o seu impacto perante à dogmática penal informática 41

3. A INEFICÁCIA DO CONTROLE PENAL DOS CRIMES CIBERNÉTICOS 48

3.1 Breve exposição do arcabouço normativo dos crimes cibernéticos 49

3.2 Desafios acerca do controle penal e da identificação dos crimes cibernéticos 55

3.3 Medidas de prevenção e combate aos crimes cibernéticos 61

CONSIDERAÇÕES FINAIS 68

REFERÊNCIAS 72

INTRODUÇÃO

Na contemporaneidade, a sociedade experimenta uma profunda transformação ocasionada pelo advento da era digital e da virtualização de inúmeros aspectos de nossas vidas. Este cenário, marcado pela ubiquidade da tecnologia, delineia um contexto em que as interações humanas, a circulação de informações e as transações comerciais são cada vez mais mediadas por plataformas e dispositivos eletrônicos.

Com essa evolução tecnológica, surge um universo interconectado e complexo, proporcionando mais peculiaridades e mecanismos que se tornam disponíveis com certa facilidade para qualquer explorador desse ramo. De modo que o mundo virtual, hodiernamente, acaba entrelaçando-se de maneira considerável com uma parte significativa da vida cotidiana dos indivíduos. Entretanto, por conseguinte, tal situação também abre margens para uma constante expansão de novas formas de criminalidade no âmbito virtual, que cresce exponencialmente ao mesmo passo da ascensão tecnológica.

Diante desse cenário, essas inovadoras formas de criminalidade são cometidas ao ambiente virtual e representam cada vez mais um desafio complexo para o sistema jurídico, exigindo uma análise crítica da identificação e controle penal dessas condutas. Tendo em vista que, embora haja o direito penal informático como uma área que compreende e adapta as leis tradicionais às especificidades digitais, resta aparente que a problemática em questão ainda carece de uma maior efetividade no enfrentamento às suas peculiaridades no âmbito jurídico penal.

Ademais, considerando que uma boa parte das vítimas envolvidas em crimes cibernéticos inadvertidamente colocam-se em situações de vulnerabilidade no ambiente virtual, tal situação exige um estudo que realce a importância de compreendermos essa natureza complexa e interconectada do mundo virtual com o real.

O presente estudo visa abordar um amplo espectro de temas relacionados a abordagens multidisciplinares aplicadas no âmbito do controle penal, com uma atenção particular voltada ao significativo papel desempenhado pelas vítimas nos cenários dos crimes cibernéticos. Serão exploradas as categorias fundamentais da conduta da vítima no direito penal informático e a caracterização dos crimes virtuais, assim como as técnicas e ferramentas utilizadas pelos perpetradores. Além disso, será analisada a complexidade das investigações de crimes cibernéticos,

considerando desafios como anonimato da autoria e a falta de coordenação entre jurisdições.

Assim, o escopo desta investigação reside na análise do impacto que o comportamento negligente ou desatento dos usuários pode ter sobre a responsabilidade penal do agente em face dos delitos informáticos relacionados a bens jurídicos disponíveis.

A pertinência desse tema encontra sua justificativa principalmente na proliferação desses delitos informáticos após o exponencial aumento dos meios tecnológicos, como por ora exposto, que resultam em violações frequentes e significativas aos sistemas informáticos, aos dados pessoais e ao patrimônio, ao mesmo tempo em que ressalta a necessidade de os usuários assumirem um papel central e autônomo nesse contexto.

De modo que, ao compreender os principais obstáculos e explorar abordagens multidisciplinares, esta pesquisa pode contribuir para o desenvolvimento de estratégias mais eficientes de prevenção e combate aos crimes cibernéticos, proporcionando uma maior segurança para indivíduos, empresas e instituições. Esta análise jurídica visa, principalmente, examinar os principais aspectos relacionados à identificação e prevenção de crimes cibernéticos, considerando o arcabouço legal existente e os desafios enfrentados pelos sistemas jurídicos.

A metodologia adotada, de natureza lógico-dedutiva, permite uma abordagem rigorosa e estruturada na condução da pesquisa, partindo de questionamentos e suposições específicas para chegar a conclusões gerais, devido à natureza multidisciplinar da temática. O estudo seguirá uma abordagem exploratória, fundamentada em procedimentos bibliográficos e documentais, visando obter um entendimento mais amplo da temática. Seguindo referências variadas, como livros, artigos científicos, teses, relatórios e documentos oficiais para embasar a análise e a discussão. Além disso, a análise dos dados coletados será qualitativa, visando identificar padrões, desafios comuns e possíveis soluções.

Para tal desiderato, o trabalho estrutura-se em três capítulos inter-relacionados, cada qual dedicado a aspectos fundamentais dessa temática emergente, nos quais se dedica, em primeiro plano, a uma investigação aprofundada sobre o impacto da vítima na efetivação dos crimes cibernéticos. Diante da validação dessa premissa central, empreende-se uma busca meticulosa para compreender de que maneira essa influência ocorre, contrapondo essa hipótese à perspectiva tradicional do direito penal

fundamentada em preceitos consolidados pelo direito europeu. Essa contraposição é realizada ao considerar a desafiadora realidade do contexto digital, permeada por todo o panorama de avanço tecnológico.

Sendo assim, debruçando a temática em questão, o capítulo inicial examina um breve aparato do desenvolvimento tecnológico nos últimos tempos que desencadeou na influência do mundo virtual na autonomia da vítima, minuciando ainda uma análise centrada na vítima sob a ótica da vitimodogmática nos crimes cibernéticos. Se propondo a explorar e analisar, de forma aprofundada, o papel e o impacto da conduta da vítima no universo virtual, com enfoque especial nos crimes cibernéticos.

No âmbito da ciência do direito penal, análises vitimodogmáticas realçam a relevância de compreender o impacto que as ações da vítima exercem na prevenção de crimes e na análise apropriada da responsabilidade penal do perpetrador, o que se revela de grande importância para a investigação dos crimes informáticos relacionados a bens jurídicos disponíveis.

Em um segundo momento, ao longo da presente pesquisa, contempla-se acerca de toda a complexidade de compreender o conhecimento do risco no âmbito virtual. Para tal, foram investigadas teorias funcionalistas moderadas, como a de Claus Roxin, proporcionando um substrato teórico para análises filosóficas e teóricas conduzidas por renomados pensadores como Zygmunt Bauman, Pierre Lévy e Andy Clark. Este embasamento filosófico e teórico se tornou crucial para compreender a intrincada conexão entre risco, tecnologia e sociedade na contemporaneidade, acrescentando uma camada de profundidade às análises subsequentes.

Para tal, em ato contínuo, trata-se acerca da relevância da conduta da vítima perante a dogmática penal. Tendo como objetivo primordial evidenciar a inadequação da noção dogmática de vítima como sinônimo inquestionável de sujeito passivo, discernindo-a das inúmeras outras denominações, frequentemente confundidas, associadas ao seu domínio semântico, sobretudo no contexto cibernético.

Este estudo almeja, assim, contribuir para uma compreensão mais precisa e contextualizada do papel da vítima nos crimes cibernéticos, no intuito de informar e aprimorar o embasamento teórico necessário para enfrentar os desafios inerentes a este domínio jurídico complexo e em constante transformação.

Por fim, a terceira parte do trabalho trata-se do estudo mais aprofundado e específico acerca da temática, concentrando-se em discutir os impactos provenientes da vulnerabilidade da vítima diante da evolução normativa dos crimes cibernéticos.

Neste contexto, são evidenciados os persistentes desafios enfrentados no âmbito do controle penal, particularmente no que tange à identificação dos perpetradores, contribuindo para uma reanálise das estratégias atuais de política criminal no controle dessa forma de criminalidade informática. Ademais, explora-se a respeito de estratégias viáveis de prevenção e combate a estes delitos, buscando um equilíbrio entre segurança cibernética e proteção dos indivíduos.

Pretende-se, assim, após a leitura desse estudo, que se haja uma compreensão mais profunda e perspicaz das constantes problemáticas que se apresentam à política criminal contemporânea no que concerne à temática em questão, uma vez que o avanço tecnológico impulsiona uma transformação radical no panorama da criminalidade, demandando estratégias eficazes para seu enfrentamento.

O estudo delineado a partir destas considerações, destarte, objetiva analisar os perigos e as obrigações provenientes da inserção da informática no cotidiano dos indivíduos, além de examinar os papéis desempenhados por cada agente nesse contexto tecnológico. Evidenciando assim que os crimes informáticos demandam de uma abordagem mais abrangente do que aquela voltada exclusivamente para o agente da ação, fatores esses que serão discutidos ao longo desta pesquisa.

Dessa maneira, busca-se não apenas compreender o panorama da conduta da vítima na sociedade virtual e suas implicações jurídicas, mas também lançar luz sobre as complexidades intrínsecas aos crimes cibernéticos, provendo subsídios para uma abordagem mais robusta e fundamentada no âmbito do direito penal. Portanto, a presente pesquisa pretende contribuir para a compreensão das interações entre o mundo virtual, a conduta da vítima e os desafios enfrentados na mitigação e enfrentamento dos crimes perpetrados neste ambiente.

1. A CONDUTA DA VÍTIMA EM UMA SOCIEDADE VIRTUAL

Diante de uma evidente disseminação exponencial da tecnologia da informação sem parâmetros, os indivíduos estão se tornando cada vez mais dependentes desse meio para suas atividades diárias. Assim sendo, o processo de modernização introduz na sociedade transformações que, em muitas ocasiões, ultrapassam significativamente a capacidade de adaptação e de controle jurídico até certo ponto.

De modo geral, pode se dizer que o indivíduo na sociedade contemporânea habita um ambiente marcado por incertezas e riscos constantes e inevitáveis, com efeito, tais aspectos devem ser considerados para entender a conduta da vítima[1] perante uma sociedade imersa num mundo virtual[2] em constantes transformações.

Para tanto, tendo em vista que as fronteiras entre o mundo físico e o virtual estão se tornando, cada vez mais tênues, é imperativo compreender mais solidamente o contexto em que aqueles que são afetados por violações da segurança digital estão inseridos e como essa drástica mudança impacta na autonomia dos usuários, o que será melhor delineado alhures.

1.1 Breve histórico acerca da ascensão do paradigma virtual

A priori, como é de conhecimento geral, o avanço da tecnologia e sua convergência no âmbito digital têm sido uma narrativa dominante no cenário contemporâneo, moldando profundamente a maneira como interagimos e concebemos a realidade. Uma das facetas mais impactantes desse desenvolvimento é a criação e evolução de uma espécie de mundo virtual, uma esfera tecnológica complexa que se expandiu exponencialmente desde o surgimento do computador.

De tal modo que a história do mundo virtual está intrinsecamente ligada ao advento deste importante artefato citado. Nesse viés, o período pós Segunda Guerra Mundial, figuras visionárias como Alan Turing, Claude Shannon e John von Neumann delinearam os fundamentos teóricos e práticos dos primeiros computadores

[1] Partindo do conceito de vítima definido por ANDRADE: “toda pessoa física ou entidade coletiva diretamente atingida, contra sua vontade, na sua pessoa ou no seu patrimônio pela *deviance*”. ANDRADE, Manuel da Costa. A vítima e o problema criminal. Coimbra: Coimbra Editora, 1980, p. 50

[2] Representação digital de um espaço no qual os usuários podem interagir entre si e com elementos virtuais.

programáveis[3]. Estes dispositivos foram marcos iniciais, desencadeando uma revolução que culminaria na disseminação dos computadores pessoais e, como resultado, na exploração do mundo virtual.

Nessa perspectiva, a década de 1970 foi marcada como uma fase crucial com o advento da revolução digital, na qual inovações como os microprocessadores possibilitaram a criação de computadores pessoais mais acessíveis, tendo gigantes da indústria, a exemplo da Microsoft[4], desempenhado papéis significativos na popularização desses dispositivos.

Analogamente, a década de 1990 testemunhou um marco paradigmático, desta vez, com a democratização do acesso à Internet. A criação da *World Wide Web*[5] pelo físico britânico Tim Berners-Lee, em 1989, foi um catalisador fundamental para a proliferação do mundo virtual. Essa interconexão global de sistemas de informação e comunicação proporcionou o surgimento de novas plataformas e a facilitação da comunicação e compartilhamento de informações em escala global.

No Brasil, em 1992, foi estabelecida a primeira rede que se conectou à internet, interligando as principais universidades do país. Em 1995, surgiu o Comitê Gestor da Internet no Brasil (CGI.br), com o propósito de coordenar e promover esforços para o desenvolvimento de uma internet de alta qualidade, inovação e ampla oferta de serviços. Uma das funções primordiais do CGI.br era a disseminação de informações relacionadas ao uso da internet no território brasileiro, servindo como referência para a formulação de políticas cruciais para a inclusão digital da população[6].

Nessa conjuntura, de maneira exponencial, os avanços tecnológicos desenfreados revolucionaram a realidade da internet ao longo dos anos, transformando-a de um espaço simples de comunicação e pesquisa para um

[3] Turing, A. M. On computable numbers, with an application to the Entscheidungsproblem. Proceedings of the London Mathematical Society, 2 s. vol. 42, 1937, p. 230–265.

[4] A Microsoft desempenhou um papel fundamental no advento dos computadores na década de 1970, contribuindo de maneira significativa para o desenvolvimento e popularização da tecnologia. Fundada em 1975 por Bill Gates e Paul Allen, a empresa foi pioneira na produção de software para microcomputadores. A atuação da Microsoft foi marcada por sua visão estratégica de criar sistemas operacionais padronizados para computadores pessoais, o que simplificou a interação dos usuários com as máquinas e impulsionou a aceitação e adoção da computação pessoal.

[5] BERNERS-LEE, T.J.; CAILLIAU, R.; LUOTONEN, A.; NIELSEN, H.F.; SECRET, A. The World-Wide Web. Communications of the ACM, v. 37, n. 8, agosto de. 1994, p. 76-82.

[6] ADACHI, Tomi. Comitê Gestor da Internet no Brasil (CGI. br): uma evolução do sistema de informação nacional moldada socialmente. Tese de Doutorado. Universidade de São Paulo, 2009, p. 37.

ecossistema multifuncional que permeia praticamente todos os aspectos da vida dos indivíduos.

De tal modo que, a partir da ascensão da banda larga e da disseminação da conectividade móvel, foi-se criada uma nova realidade de infraestrutura que permitiu a explosão de conteúdos envolvendo multimídias, como streamings de vídeos e de músicas. Neste contexto, entraram em cena as redes sociais, como Facebook, Twitter e Instagram, alterando fundamentalmente a maneira como nos conectamos, compartilhamos informações e construímos relações. A disseminação de notícias e opiniões encontrou um novo lar nesses espaços digitais, moldando a opinião pública de maneiras antes inimagináveis.

Ademais, um importante fator que alavancou ainda mais os usos dos meios tecnológicos nos últimos tempos foi a pandemia causada pelo COVID-19, que em meio a um grande recolhimento das pessoas dentro de casa, trouxe consigo uma aceleração sem precedentes no uso da internet[7], evidenciando sua importância como ferramenta vital para a comunicação, trabalho, educação, saúde e até mesmo o bem-estar social durante períodos de distanciamento social e isolamento.

Essa interconexão digital permitiu que a sociedade se adaptasse e continuasse a funcionar, minimizando, em certa medida, os impactos socioeconômicos da crise sanitária, muito embora também tenha acentuado ainda mais a tamanha desigualdade[8] ao acesso tecnológico, em virtude desta ascensão.

À vista disso, diante de uma complexa aprimoração da capacidade de processamento dos computadores, possibilitou-se a criação de ambientes digitais tridimensionais, interfaces de usuário mais intuitivas e a manipulação de grandes conjuntos de dados, permitindo a simulação e a representação gradativamente mais

---

[7] Pesquisa sobre o uso das Tecnologias de Informação e Comunicação nos domicílios brasileiros (TIC Domicílios), realizada em 2020, trouxe dados de que, com a pandemia de covid-19 - declarada pela Organização Mundial da Saúde em março de 2020 -, intensificou-se o uso de tecnologias digitais no Brasil, passando de 71% dos domicílios com acesso à internet em 2019 para 83% no ano passado, o que corresponde a 61,8 milhões de domicílios com algum tipo de conexão à rede.
"Estudo mostra que pandemia intensificou uso das tecnologias digitais" em: https://agenciabrasil.ebc.com.br/geral/noticia/2021-11/estudo-mostra-que-pandemia-intensificou-uso-das-tecnologias-digitais. Acesso em: 05 set. 2023.

[8] Apesar de a pandemia de Covid-19 ter acelerado o acesso à internet no Brasil nos últimos dois anos, 7,28 milhões de famílias ainda permaneciam sem conexão à rede em casa em 2021, segundo o Instituto Brasileiro de Geografia e Estatística (IBGE).
"28,2 milhões de brasileiros não têm acesso à internet, diz IBGE" em: https://www.infomoney.com.br/consumo/282-milhoes-de-brasileiros-nao-tem-acesso-a-internet-diz-ibge/#:~:text=Apesar%20de%20a%20pandemia%20de,Geografia%20e%20Estat%C3%ADstica%20(IBGE). Acesso em 05 set. 2023.

realista do mundo físico no espaço virtual. Fazendo, desse modo, com que muitos indivíduos estejam cada vez mais imersos numa pautada realidade paralela e cada vez mais omissos no que diz respeito a se ter um devido conhecimento acerca das evoluções.

Assim, na contemporaneidade, é nítido que o mundo por trás dos ambientes digitais transcende as fronteiras da tela do computador. Impulsionada por desmedidos avanços tecnológicos, a realidade virtual foi consideravelmente aprimorada, acarretando em que estão sendo redefinidas as interações humanas e a maneira como experienciamos essa faceta.

A efeito exemplificativo, o advento e o aprimoramento da Inteligência Artificial, com suas aplicações em aprendizado de máquina e processamento de linguagem natural, está se tornando um pilar essencial no desenvolvimento de mecanismos e de algoritmos mais sofisticados, bem como ao aumento da capacidade computacional e ao acesso a grandes volumes de dados para incontáveis utilidades, proporcionadas de certo modo por tantos avanços da IA[9] nos últimos tempos.

A internet é merecedora de destaque como uma das principais inovações científicas e tecnológicas da história da humanidade. Proporcionando inúmeros benefícios, facilitando a disseminação de conhecimento e informações, transcendendo fronteiras geográficas. É possível acessar informações de qualquer lugar do mundo de forma instantânea, o que contribui para a transformação da cultura humana em uma cultura cibernética[10].

O panorama atual de avanços exponenciais reflete numa sociedade imersa em um mundo digital em constante transformação, que continuará a moldar nossa percepção do ambiente virtual e suas implicações na sociedade, o que tem redefinido, nas últimas décadas, a maneira como interagimos e percebemos o mundo. Basicamente, à medida que a tecnologia se integra cada vez mais à rotina do cidadão, torna-se imperativo que este adquira um determinado conhecimento prévio para manejar as inovações, já que, indubitavelmente, avanços significativos acarretam novas obrigações e potenciais ameaças.

[9] A ascensão da Inteligência Virtual (IA) nos últimos tempos representa um marco significativo no avanço tecnológico, transformando a maneira como interagimos com sistemas e serviços. Nesse contexto, vale destacar notoriamente a criação de agentes virtuais capazes de simular comportamentos humanos e oferecer respostas personalizadas.

[10] LÉVY, Pierre. Cibercultura. 1 ed. São Paulo: 34, 1999, p. 16.

A era virtual é uma esfera particularmente influente dessa mudança de paradigma no quesito da vida humana, tratando de um domínio digital que se expande e se transforma incessantemente, alterando nossa percepção da realidade e reconfigurando nossas experiências. Por isso, a compreensão desse progresso é fundamental para antever o futuro e gerenciar os desafios e oportunidades que essa evolução incessante traz consigo.

A influência dessa nova era nas relações jurídicas é onipresente, abrangendo uma diversidade de esferas da vida cotidiana. No âmbito profissional, por exemplo, a internet e as tecnologias digitais proporcionaram novas formas de trabalho e colaboração, demandando a adaptação e criação de normas para regular contratos virtuais, direitos e obrigações dos trabalhadores remotos, e questões relacionadas à propriedade intelectual em um ambiente cada vez mais globalizado.

A evolução tecnológica e a interconexão global proporcionaram uma revolução digital, transformando o mundo virtual em um ambiente sofisticado, interativo e multifacetado. Sendo assim, o âmbito cibernético se tornou uma extensão integral da vida cotidiana, permeando todos os aspectos da sociedade moderna, desde comunicações e transações comerciais até o armazenamento de informações críticas.

1.2 O Impacto do mundo virtual na autonomia da vítima

Nesse viés, é nítido que a rápida transformação do mundo virtual não se limita apenas ao contexto tecnológico, todavia, ela também desempenha um papel significativo na autonomia dos indivíduos, especialmente quando consideramos as situações em que as vítimas de crimes envolvendo o âmbito cibernético se prestam.

Ora, a autonomia, entendida como a habilidade de tomar decisões informadas e agir de acordo com a própria vontade, representa um pilar central na vida de qualquer pessoa. Dentro do mundo virtual, essa autonomia se evidencia na capacidade de controlar a própria presença online, gerenciar informações pessoais e decidir sobre a participação em atividades virtuais.

A pacificidade na sociedade virtual é fundamental, sendo a autonomia social um elemento crucial para isso. De modo que, trazendo ao campo do Direito, vê-se que este desempenha um papel fundamental favorecendo os relacionamentos

harmoniosos entre indivíduos e grupos sociais, contribuindo, assim, para o progresso desse meio[11].

O impacto do mundo virtual na autonomia individual é profundo, tendo em vista que o aumento da presença e da atividade no ambiente digital pode tanto fortalecer quanto minar a autonomia das pessoas. Por um lado, a exposição a uma ampla gama de informações e a oportunidade de conectar-se com diferentes perspectivas podem enriquecer o processo de tomada de decisões. Por outro lado, a exposição excessiva, a coleta não consensual de dados e a manipulação de informações representam ameaças à privacidade e, consequentemente, à autonomia.

Dessa forma, no âmbito do direito penal, vê-se que uma esfera proeminente destinada ao exercício da autonomia é o instituto do consentimento, que coloca a vontade do indivíduo acima da proibição estabelecida em determinados tipos penais, conferindo, no aspecto material, legitimidade a esse instituto.

A abrangência do consentimento, contudo, se estende a bens jurídicos indisponíveis que, em certas circunstâncias, podem ser voluntariamente cedidos por seu titular. Esse destaque ao consentimento como expressão da vontade individual é fundamental para um entendimento mais aprofundado das dinâmicas que envolvem as relações jurídicas no âmbito tecnológico e, por extensão, na proteção do direito à autonomia de cada indivíduo.

Este aspecto da autonomia é de suma relevância, pois resguarda a integridade e a decisão consciente dos indivíduos em contextos que envolvem a legitimidade de suas atuações e, consequentemente, no bem-estar. A discussão sobre os limites e as nuances do consentimento representa um campo jurídico enriquecedor e essencial para a efetivação da justiça e do respeito aos direitos individuais.

Logo, essa crescente dependência da sociedade contemporânea em relação ao mundo virtual também trouxe consigo uma série de desafios e riscos, destacando-se entre estes, os crimes cibernéticos[12], cerne central deste artigo. Os quais afetam significativamente a segurança e o bem-estar das vítimas, principalmente por se tratar de um campo ainda pouco explorado por grande parcela da população mundial. O presente capítulo, então, busca justamente explorar essa correlação entre o

[11] NADER, Paulo. Introdução ao Estudo do Direito. 24 ed. Rio de Janeiro: Forense: 2004, p. 25.
[12] “Atividade criminosa ligada diretamente a qualquer ação ou prática ilícita na Internet”. INTERPOL. Cybercrime. Disponível em: https://www.interpol.int/Crimes/Cybercrime. Acesso em: 15 ago. 2023.

desenvolvimento do mundo virtual e os malefícios advindos da ilusória autonomia das vítimas desses tipos de delitos.

No contexto atual, entender o complexo relacionamento entre o mundo virtual e a autonomia é de extrema importância. Entretanto, a busca por estratégias eficazes para promover e preservar a autonomia dos indivíduos nesse espaço demanda ações coordenadas, envolvendo não apenas os próprios usuários, mas também regulamentações governamentais e iniciativas educacionais voltadas para a segurança digital.

Desse modo, a identificação e a prevenção desses crimes têm se mostrado um desafio complexo para o sistema jurídico, envolvendo alguns fatos como exemplo da natureza transnacional, do anonimato e da rápida evolução das técnicas empregadas pelos criminosos cibernéticos.

É interessante observar que, apesar de o Brasil estar em um estágio incipiente de popularização digital comparado a outras grandes potências mundiais, os dez grupos de crackers mais ativos do mundo têm origem aqui, o que evidencia o altamente avançado potencial do nosso país para crimes cibernéticos. A esse fato, acresce-se que, em 2022, o Brasil foi classificado como o segundo país do mundo com mais ocorrências de ciberataques, ficando apenas atrás dos EUA[13].

Os crimes cibernéticos emergiram como uma ameaça contemporânea, alimentados pela proliferação do desenvolvimento dos mecanismos digitais e se tornando um desafio global. Portanto, a falta de cuidado e do devido reconhecimento adequado por parte da atuação das vítimas de crimes no âmbito virtual, pode amplificar os malefícios desses delitos, principalmente pois pode acabar gerando consequências devastadoras a essas, seja pela exposição e roubo de dados sensíveis, por fraudes financeiras, por extorsões, por difamação online ou por violações de privacidade[14] - crimes que serão melhor delineados alhures.

Um aspecto crucial na análise dessa perspectiva é essa notória vulnerabilidade de grande parte das pessoas no universo virtual, emergindo diretamente à concepção

[13] O Brasil assumiu a segunda posição entre os maiores alvos globalmente, atrás apenas dos Estados Unidos, que lidera o ranking com mais de 1,33 milhão (21,7%), segundo um relatório da empresa especializada Netscout.
"Brasil é 2º maior alvo mundial de ciberataques, revela estudo". Disponível em: https://noticias.r7.com/tecnologia-e-ciencia/brasil-e-2-maior-alvo-mundial-de-ciberataques-revela-estudo-27062022. Acesso em: 05 set. 2023

[14] Holt, T. J., A. M. Bossler, and K. C. Seigfried-Spellar. Cybercrime and Digital Forensics: An Introduction. 2nd ed. New York: Routledge, 2018.

ilusória de autonomia de muitas vítimas desses delitos. Nesse contexto, vê-se que esses crimes expõem consideravelmente os indivíduos a situações de risco, sobretudo os mais jovens, podendo resultar em uma significativa perda de autonomia, uma vez que as vítimas se veem coagidas ou manipuladas devido à intimidação ou ao temor da exposição de informações sensíveis.

Haja vista que, paralelamente à conveniência proporcionada pela tecnologia, surgiram também os ônus e malefícios associados à esta, como exposto. Nessa conjuntura, o indivíduo ampliou seu período de isolamento, interagindo e se comunicando de forma virtual, principalmente diante de um monitor ou de um celular. A presença física foi sucedida pela "presença virtual", na qual os computadores interagem, sob a orientação de seus operadores, fazendo com que cada vez mais este meio virtual seja utilizado de maneira irresponsável e impulsiva.

Desse modo, ao serem amparados pelas telas, os seres humanos passam a figurar como usuários anônimos em um universo virtual sem fronteiras, pautados ainda por uma ilusória percepção de segurança, situação a qual muitas vezes acaba ocasionando na facilitação da atuação de pessoas mal intencionadas nesse âmbito, justamente por um certo descuido de uma considerável parcela das pessoas que são vítimas desses delitos.

Dessarte, nesse contexto tecnológico, observa-se nitidamente o quão reduzido é o contingente de usuários que exploram integralmente todas as funcionalidades de suas máquinas. Divergente disso, com frequência vê-se que muitas vezes os utilizadores jamais consultaram o manual de instruções de seu dispositivo celular, muito menos averiguaram os termos de compromisso antes de se cadastrar em sites e redes sociais.

A grande maioria dos usuários desses aparelhos tecnológicos tendem a limitar-se a adquirir conhecimento básico para facilitar a comunicação, buscando com celeridade começar a explorar superficialmente páginas de interesse limitado e, possivelmente, utilizar recursos multimídia, sem reconhecer plenamente o potencial completo e negligenciando as amplas possibilidades que esses dispositivos podem proporcionar. Cenário esse que destaca a necessidade de promover a educação e a conscientização dos usuários sobre o pleno aproveitamento dos recursos disponíveis em suas tecnologias.

Diante do exposto, sendo incontestável o eminente avanço da tecnologia e da popularização da internet, vale ressaltar que, cada vez mais, peculiaridades e

mecanismos estão disponíveis com facilidade para qualquer explorador desse ramo, de modo que o mundo virtual se tornou uma parte significativa da vida cotidiana das pessoas, como fora exposto. Dessa maneira, tal situação, por consequência, também abre margens para constantes expansões de novas formas de criminalidade no âmbito virtual. Resta aparente, portanto, a imprescindível necessidade de analisar-se de uma maneira mais aprofundada e criteriosa do ponto de vista doutrinário a respeito da notável atuação da conduta da vítima perante determinados delitos.

1.3 Perspectiva vitimodogmática na abordagem de crimes cibernéticos com enfoque na vítima

Em princípio, sabe-se que a grande maioria das vítimas de crimes cibernéticos são cidadãos leigos que, de maneira majoritária, não possuem uma compreensão precisa do ambiente em que estão inseridos, tampouco das complexidades e dos danos que podem ser causados a eles por meio da tecnologia, perpetrados por outro utilizador anônimo.

De modo que, essas vítimas, muitas vezes, não estão plenamente conscientes das nuances intrincadas do ambiente digital, incluindo suas vulnerabilidades e as táticas utilizadas pelos criminosos cibernéticos para explorá-las. Consequentemente, estão sujeitas a serem lesadas, alheias às ameaças que a eletrônica pode representar quando manipulada por indivíduos mal-intencionados. Cenário este que realça a necessidade premente de conscientização e educação sobre segurança cibernética para o público em geral, a fim de proteger os usuários e minimizar os danos causados por crimes perpetrados através dos meios eletrônicos, como fora exposto.

Diante disso, a sociedade contemporânea, impulsionada pela ubiquidade da internet e das redes sociais, enfrenta um cenário complexo de crimes cibernéticos, onde uma importante teoria designada como vitimodogmática pode ser especialmente acentuada para análise desta temática.

Este vocábulo, derivado da combinação de "vítima" e "dogmática", descreve uma postura em que a condição de vítima é consideravelmente enfatizada, muitas vezes instrumentalizada para legitimar ações ou buscar vantagens sociais e legais. Conceito o qual se torna cada vez mais relevante em um mundo digitalizado, onde as fronteiras entre a realidade e o virtual se tornam mais difusas.

À vista desta conjuntura, bem designa Greco que esta teoria: “surgiu da necessidade de se abandonar uma visão simplista do fenômeno criminoso, em que de um dos lados teríamos uma pessoa totalmente inocente (vítima), e de outro, uma pessoa totalmente culpada (criminoso)”.[15]

A ideia da vitimodogmática é um importante marco no campo do direito penal, tendo ganhado destaque significativo na segunda metade do século XX, ao propor uma abordagem que reconhece e valoriza a experiência da vítima no processo penal, buscando atender de forma adequada às suas necessidades. Tais avanços foram impulsionados por pesquisas focadas no âmbito dos interesses materiais, especialmente nos crimes relacionados à divulgação de informações confidenciais, fraude e apropriação indevida.

Baseada na Dogmática Penal, esta teoria parte do pressuposto de que a vítima é parte integrante do processo penal[16], devendo ser considerada não apenas como um objeto passivo do crime, mas como um sujeito ativo com direitos e interesses legítimos a serem protegidos. Assim, se busca uma compreensão mais abrangente do crime, incorporando a perspectiva da vítima e levando em consideração suas necessidades e reivindicações ao longo do processo.

Isto posto, investiga-se neste tópico o impacto profundo desse fundamento citado, no contexto das vítimas de crimes cibernéticos, destacando como as interações virtuais podem moldar percepções de vitimização e influenciar políticas e ações correlatas.

No contexto dos crimes cibernéticos, fundamentar-se a partir do conceito da vitimodogmática é crucial, uma vez que essa teoria representa um avanço significativo na compreensão e tratamento desses delitos, os quais, muitas vezes deixam marcas profundas e duradouras nas vítimas. Urge, assim sendo, de uma análise mais criteriosa e doutrinária acerca da temática, tendo em vista que a natureza virtual desses crimes acarreta em que muitas vezes as vítimas enfrentam desafios que pouco foram explorados anteriormente.

De forma similar, a análise direcionada à vítima indica que a mera prevenção, que tenha como propósito de evitar que o transgressor cometa infrações penais acaba por se mostrar insuficiente e inadequada, haja vista que inúmeras vítimas não

[15] GRECO, Alessandra Orcesi Pedro; GRECO, Vicente. A autocolocação da vítima em risco. São Paulo: Revista dos Tribunais, 2004, p. 39
[16] ROXIN, Claus. "Derecho Penal Parte General", Madrid: Civitas, 1997

percebem que, em muitos cenários, desempenham um papel de partícipes ou facilitadoras do cometimento de um cibercrime. Ou seja, demonstra-se imprescindível que haja um enfoque que reforce a necessidade de considerar não apenas o comportamento do transgressor, mas também o papel e a compreensão da vítima na dinâmica do crime, já que simplesmente restringir a prevenção às ações do infrator não aborda a complexidade da interação entre as partes envolvidas, incluindo a vítima.

Nesse quesito, a abordagem centrada na vítima reconhece a vítima como uma peça central na compreensão e na resolução de um crime. Especificamente, no contexto dos crimes cibernéticos, essa abordagem adquire relevância primordial, uma vez que esses crimes frequentemente causam danos significativos não apenas à vítima, mas também à sua vida cotidiana, à sua privacidade, à sua segurança e ao seu bem-estar emocional. Portanto, adotando uma perspectiva centrada na vítima, é possível entender melhor a extensão total do impacto de um crime cibernético.

Assim, ao se basear na análise das vítimas, considerando suas características individuais e suas interações com o contexto social, a teoria em espeque amplia essa abordagem, ao trazer à tona a necessidade de compreender o sofrimento e as consequências físicas, emocionais e sociais enfrentadas pelas vítimas de crimes cibernéticos. Propondo, desse modo, uma abordagem mais humanizada, voltada para a compreensão dos danos sofridos e a implementação de políticas e estratégias de prevenção e reabilitação mais eficazes.

Seria, no caso, um componente fundamental para o estímulo da elaboração de políticas públicas e de estratégias de combate a esses crimes. Considerando a perspectiva da vítima não apenas no momento da investigação e julgamento, mas também ao longo de todo o processo, desde a prevenção até a reparação dos danos, sendo crucial para promover uma justiça mais eficaz.

Vale ressaltar que uma análise aprofundada das vítimas dos delitos mostra-se fundamental para serem devidamente destacados novos elementos no contexto criminal, como a contribuição da vítima para a consumação do crime, a maneira como é escolhida pelo transgressor, os lugares mais suscetíveis à vitimização, as interações da vítima com o agressor, entre outras situações, que refletem ainda mais a urgência de serem desenvolvidos mais métodos de prevenção e educação voltados para a vítima.

Desse modo, vê-se a importância de examinar minuciosamente a vítima no contexto do crime, reconhecendo seu papel e suas interações dentro deste cenário, já que isso vai além da análise convencional centrada no infrator, mas também abrange uma compreensão holística das variáveis envolvidas na dogmática penal. Que consolidam, de certo modo, a aprimoração das ciências penais acerca da temática, partindo de um reconhecimento dessa inter-relação entre a vítima e o autor, como bem destaca Beristain nesse sentido:

> Ainda hoje muitos e eminentes penalistas opinam que o Código Penal é o código dos delinquentes, mas não o código das vítimas. Outros, ao contrário, opinam que já não cabe manter vigente um Código Penal que se apoia na dogmática pela qual se possam entender e compreender a sanção e o delinqüente sem uma constante e radical referência às vítimas. Estas são a outra face da única moeda que atualmente tem curso legal. Basta ler um livro de vitimologia para ver que o delinquente está, inseparável e consubstancialmente, relacionado com a vítima, mais que o corpo com sua sombra.[17]

Em suma, pode-se dizer que a teoria da vitimodogmática oferece uma abordagem inovadora para o direito penal, em que o papel central do indivíduo está alinhado com a teoria constitucional do bem jurídico-penal, que destaca a natureza instrumental de sua proteção em prol do desenvolvimento da personalidade.

De acordo com SCHÜNEMANN (1948)[18], a vitimodogmática constitui uma abordagem voltada a reconhecer as responsabilidades atribuídas à vítima e a delimitar a concepção de delito. Nesse sentido, ela passa a coexistir de maneira paralela aos debates vitimológicos, discutindo a contribuição da vítima para a ocorrência do ato criminoso e a sua importância para a dogmática penal.

Conforme a análise do renomado jurista alemão[19], a vitimodogmática representa uma diretriz voltada para a exclusão da esfera de punição do comportamento da vítima que não merece ou não demanda proteção. Em outras palavras, é uma forma de limitação da concepção de crime, na qual se avalia a responsabilidade da vítima.

---

[17] BERISTAIN, Antonio. Nova criminologia à luz do direito penal e da vitimologia. Brasília: Editora Universidade de Brasília, 2000, p. 191.

[18] PRITTWITZ, Cornelius. La resurrección de La víctima em La teoria penal. *In*: La víctima en el sistema penal. Dogmática, proceso e política criminal. Traducción del Prof Dr. Luís Miguel Reyna Alfaro. Lima: Editora Jurídica Grijley. p.65.

[19] SCHÜNEMANN, Bernd. Temas actuales y permanentes del derecho penal después del milênio. Madrid: Tecnos, 2002, p.116.

O entendimento de SCHÜNEMANN evidencia a necessidade de analisar com cautela os comportamentos da vítima para determinar se merecem ser considerados como parte integrante do crime ou se devem ser excluídos da esfera penal. Uma abordagem com essa busca assegurar que a aplicação das leis penais seja justa e proporcional, evitando a punição de ações da vítima que não merecem ser enquadradas como delito. Dessa forma, a vitimodogmática proporciona uma visão mais refinada da dinâmica dos delitos, considerando não apenas a conduta do agente, mas também a participação da vítima na ocorrência do crime, enfoque que é essencial para uma justiça criminal coerente com os princípios jurídicos fundamentais.

Nessa perspectiva, destaca-se a necessidade de considerar não apenas o agente infrator, mas também a participação e a influência da vítima no contexto do delito. Assim, o entendimento da colaboração da vítima no ato delituoso e sua integração à dogmática penal são aspectos cruciais para uma análise abrangente e justa da ocorrência do crime, proporcionando uma compreensão mais completa das dinâmicas envolvidas nos eventos delitivos. Esta conjuntura representa um avanço no estudo do fenômeno criminal, incorporando uma visão mais holística e inclusiva das relações entre autor e vítima no âmbito jurídico-penal.

Sendo assim, diante dos fatores que foram expostos, é possível entender que estes mencionados fazem com que a possível vítima dos crimes informáticos se distingue das outras vítimas comuns, tendo em vista a mera utilização da Internet por si só possibilita a ocorrência de crimes, por proporcionar a imersão num mundo virtual com uma falsa concepção de segurança.

Além disso, outro aspecto a se considerar da “autovitimização” repousa no fato de que, ao contrário dos crimes comuns – em que o indivíduo conhece as formas de se precaver -, no delito informático não existe um mecanismo de proteção infalível e cada usuário ainda assim o utiliza sem uma devida cautela, mesmo ciente da ineficácia da noção de proteção total, que ainda mais agravada por atitudes inadequadas dos usuários.

Com efeito, a vitimodogmática no contexto abordado representa uma espécie de reformulação, considerando as devidas ressalvas pertinentes à época atual, da abordagem tradicional da vitimologia baseada na "culpa" atribuída à vítima. Essa redefinição traz uma perspectiva contemporânea de buscar uma categoria jurídica

para essa "corresponsabilidade", seja dolosa ou culposa, da vítima[20]. De modo que, nesse mesmo sentido, Meliá designa a investigação sobre possível impacto dessa "corresponsabilidade da vítima" na avaliação jurídico-penal do ato cometido pelo autor como ponto central da vitimodogmática.[21]

Outrossim, nesse viés, passa a ser reconhecida a concepção de que a "culpa" da vítima precisa ser reavaliada e atualizada à luz das complexidades e evoluções sociais. Há uma busca por compreender a participação consciente ou negligente da vítima no evento, incorporando-a à dogmática penal e, ressaltando assim, a importância de considerar a conduta da vítima como parte relevante da análise do crime, evitando julgamentos unilaterais e promovendo uma justiça mais contextualizada.

Pois bem, à vista disso, resta nítido que não há incertezas de que o criminoso não seleciona seu alvo de maneira aleatória, em verdade, cada vítima desse âmbito tem um foco apropriado, se tornando um alvo que se destaca preferencialmente seja por quem ela é, por sua conduta, por suas posses ou por sua localização. Como bem delimita, de modo exemplificativo, as três seguintes classificadoras de vítimas[22]: as vítimas que são buscadas a partir de um perfil de uma pessoa; as vítimas que são buscadas a partir de um objeto de interesse - de algum modo direta ou indiretamente em seu poder -; e ainda, as vítimas que são buscadas pelo local em que ela frequenta.

Destarte, esta delimitação é crucial para que se tenha uma compreensão clara de que as análises apresentadas neste contexto se coadunam com as circunstâncias em que a vítima encontra no âmbito digital. Delimita-se, em verdade, individualmente, e existe a viabilidade de proteção individual dos bens jurídicos[23], fazendo com que haja um maior arcabouço investigatório ao explorar de maneira mais detalhada as estratégias e considerações relevantes para a proteção efetiva nestes cenários.

Como delineado por ora, a internet se revela um ambiente propenso de maneira contínua para a prática de delitos informáticos, principalmente devido à sua estrutura

---

[20] OLIVEIRA, Ana Sofia Schmidt de. A vítima e o direito penal. Uma abordagem do movimento vitimológico e de seu impacto no direito penal. São Paulo: Revista dos Tribunais, 1999.
[21] SILVA SÁNCHEZ, Jesús María. La víctima en el futuro de la dogmática. Victimología. San Sebastián: Universidad del País Vasco/Euskal Herriko Unibertsitatea, 1990, p. 234- 235.
[22] Cohen e Felson, 1979 *apud* SCHMALLEGER, Frank e PITTARO, Michael. Routine Activity Theory and Internet Crime. In Crimes of the Internet. Pearson Prentice Hall, New Jersey, 2008, p. 304.
[23] HASSEMER, Winfried. Introdução aos Fundamentos do Direito Penal. Sergio Antonio Fabris Editor, Porto Alegre, 2005, p. 123.

multifacetada, considerando que a própria contemporaneidade atrai a vítima para o ambiente digital e a torna vulnerável.

Tendo em vista que esses crimes estão caracterizados por um envolvimento direto do próprio usuário, que se torna uma possível vítima pelo simples ato de navegar na rede, mas principalmente ao realizar uma exposição ativa online. Portanto, é de fácil constatação que assumir riscos por meio de uma conduta negligente pode implicar na realização efetiva ou parcial do próprio bem jurídico, e não necessariamente sua total afetação na perspectiva penal.

Portanto, no contexto em que se inserem os crimes cibernéticos, entender o parâmetro supracitado implica reconhecer a forma como as vítimas são afetadas, não apenas em termos de danos materiais, mas também emocionais, psicológicos e sociais, ocasionados por situações que poderiam muitas vezes ser precavidas.

Sendo assim, torna-se evidente que a era virtual tem desafiado a autonomia das vítimas, refletindo efetivamente sobre a sua conduta em um multifacetado parâmetro. Diante desse cenário, a vitimodogmática revela-se um utilitário indispensável para compreender a base doutrinária que envolve os crimes informáticos, tanto os relacionados ao patrimônio quanto aqueles próprios e impróprios. Ademais, emerge também como um meio de fortalecer a doutrina penal em relação ao valor constitucional do livre desenvolvimento do indivíduo, reconhecendo assim o impacto que vai de encontro à autonomia da vítima, a qual carece de um devido enfoque.

Para tanto, direcionaremos em seguida nossa atenção para a incógnita do risco no mundo virtual, sob lentes teóricas e filosóficas, oportunidade em que investigaremos como essas teorias lançam luz sobre a natureza das implicações dessa abordagem, para que se haja uma maior compreensão destinada ao enfrentamento dos desafios emergentes no ambiente digital em constante evolução.

2. A INCÓGNITA DO CONHECIMENTO DO RISCO NO MUNDO VIRTUAL

No vasto e interconectado universo digital contemporâneo, a ascensão do ciberespaço trouxe consigo uma teia complexa de interações e transações, moldando a forma como indivíduos e organizações interagem, aprendem e se desenvolvem. Entretanto, como visto, essa expansão não ocorre isenta de desafios.

À medida que a sociedade se adapta a essa nova era digital, também surge uma inquietante incógnita a ser refletida, acerca do conhecimento do risco, que emerge como um enigma inescrutável, desafiando as bases da compreensão humana sobre a natureza e a amplitude das ameaças digitais.

O entendimento e a percepção do risco inerente ao mundo virtual, que será aprofundado neste capítulo, se propõem a adentrar as entranhas dessa incerteza, explorando os fundamentos que circundam a consciência dos riscos no ambiente digital e examinando a complexa dinâmica do devido conhecimento.

A incógnita do conhecimento do risco no mundo virtual é uma questão premente no contexto contemporâneo, influenciada pela rápida evolução da tecnologia e pela disseminação ubíqua das interações digitais. Desse modo, através de uma análise aprofundada, pretende-se desvelar as nuances que circundam a conscientização do risco no ciberespaço, delineando as variáveis que influenciam essa percepção, examinando as nuances psicossociais, educacionais e tecnológicas que determinam a assimilação do conhecimento do risco no universo digital.

A partir de uma investigação minuciosa, visa lançar luz sobre a complexidade desse fenômeno, utilizando-se de bases sólidas e autores conceituados que tratam acerca da problemática.

2.1 Reflexões acerca do risco virtual sob à ótica de teorias de Claus Roxin

O fenômeno dos crimes cibernéticos tem se tornado uma questão crítica no mundo hodierno, com a crescente digitalização da sociedade e de uma notória dependência tecnológica. A presença ubíqua e incontestável da tecnologia tem suscitado discussões acerca da consciência e do conhecimento do risco das pessoas no ambiente virtual, sendo uma incógnita tão nítida, mas também tão pouco abordada.

Assim sendo, é imprescindível a compreensão dessa dinâmica, motivo pelo qual este capítulo visa oferecer uma análise crítica mais aprofundada sobre como a vítima, por suas ações ou omissões, pode influenciar o seu nível de vulnerabilidade diante das ameaças digitais, acarretando muitas vezes em situações de se colocarem em risco.

Pois bem, essa dificuldade em determinar o grau de consciência que um indivíduo possui sobre os potenciais riscos e consequências de suas ações online urge de um maior aprofundamento, tendo em vista que em muitas situações a vítima de um crime cibernético pode não ter o pleno entendimento das vulnerabilidades que está sujeita, seja por falta de informação, educação digital ou subestimação dos perigos existentes.

Por isso, faz-se necessário uma abordagem com um viés doutrinário para iluminar essa compreensão da relação entre o indivíduo e o risco no mundo virtual sob as mais diferentes óticas, além da vitimodogmática. É nesse contexto que alguns ideais de Claus Roxin a respeito da participação da vítima no delito podem ser pertinentes para entendermos a responsabilidade do sujeito em relação à sua consciência dos riscos no mundo virtual. Tendo em vista que Roxin foi um dos primeiros juristas a formular uma abordagem doutrinária sobre a conduta da vítima, ganhando ampla aceitação internacional tanto na doutrina quanto na jurisprudência.

De acordo com sua perspectiva, o comportamento da vítima assume relevância no contexto da imputação, sendo considerado um terceiro elemento na análise da imputação objetiva do resultado. Em outras palavras, após a identificação da criação do risco proibido, que culmina no resultado e está inserida no âmbito de proteção da norma e do dever de cuidado violado, examina-se o chamado alcance do tipo[24]. Nesse aspecto, pode se dizer que é aparente uma distinção entre autocolocação, heterocolocação, abordando situações objetivas a respeito da importante análise da vítima em cada caso.

Assim sendo, é imperativo considerar a necessidade de uma efetiva contribuição de conhecimentos práticos no âmbito da doutrina penal, visando possibilitar uma concretização eficaz dos princípios funcionalistas moderados propostos por Roxin. Quando aplicado de maneira adequada, a vantagem do

[24] ROXIN, Claus. Funcionalismo e imputação objetiva no direito penal. Tradução de Luís Greco. Rio de Janeiro: Renovar, 2002. p. 352 e SS.

funcionalismo reside em sua orientação para metas político-criminais, proporcionando uma maior concretude aos fundamentos penais.

Dessa maneira, o tipo penal vai além de simplesmente descrever uma atividade final como um dado ontológico, mas realiza uma seleção dos valores merecedores de proteção penal. O objetivo é implementar mecanismos preventivos contra delitos de forma empiricamente eficaz, através de abordagens político-criminais, mantendo o devido respeito às garantias do sistema penal[25].

Os ideais de Roxin referentes à colocação da vítima em perigo são notoriamente possíveis de fazer-se uma alusão ao caso concreto com os riscos cibernéticos, tendo em vista que esses conceitos, ao considerarem o grau de participação consciente da vítima na exposição aos riscos e a influência de terceiros, fornecem uma base analítica crucial para compreender a conduta da vítima, a imputação de responsabilidade e a necessidade de medidas preventivas nesse cenário específico de delitos virtuais.

Roxin destaca a importância da causalidade adequada e da previsibilidade objetiva nas ações dos agentes[26]. Assim, podemos considerar que a avaliação da consciência do risco, ou sua falta, pode ser um elemento crucial para a imputação de responsabilidade em crimes cibernéticos.

A autocolocação da vítima em risco nos crimes cibernéticos, portanto, diz respeito à uma situação em que a vítima é a personagem central, ou seja, situações em que ela, conscientemente ou não, adota comportamentos ou práticas que a tornam mais suscetível a possíveis ataques. Por exemplo, ao negligenciar a proteção de suas informações pessoais online ou ao compartilhar excessivamente dados sensíveis em redes sociais. Nesses casos, a vítima assume um papel relevante em sua exposição ao perigo digital, caso não adquira o devido conhecimento para precaver-se de determinadas situações indesejadas.

Para o enfoque funcionalista, a autocolocação da vítima em risco assume um papel como elemento subjetivo do tipo, significando que ela desempenha um papel

[25] SILVA SÁNCHEZ, Jesús María. Politica criminal en la dogmática: algunas cuestiones sobre su contenido y límites. In: Política criminal y nuevo derecho penal: Libro homenaje a Claus Roxin. Barcelona: Bosch, pp. 17-30, 1997, pp. 22-23.
[26] ROXIN, Claus. *Op. Cit.* Nota 16.

na avaliação da extensão da participação da vítima na conduta, podendo até mesmo, em certos casos, influenciar na tipificação do ato.[27]

Nessa linha de pensamento, Luís Greco argumenta que a ação da vítima em se colocar em risco está relacionada ao seu domínio do fato[28], ou seja, ao domínio da ação de se autocolocar em risco, sendo crucial que a pessoa prejudicada tenha um nítido domínio e uma autoria instantânea perante a situação. Logo, o fato de o agente facilitador possuir um entendimento mais abrangente do que a vítima sobre as circunstâncias da situação arriscada resultaria em uma capacidade de avaliação inferior por parte do ofendido, que não está ciente do verdadeiro perigo da empreitada.

Isto é, a teoria da autocolocação da vítima em risco se baseia no princípio de que, em certas circunstâncias, a própria vítima pode assumir a responsabilidade por colocar-se em situações de perigo. No contexto virtual, isso pode se manifestar quando a vítima, por suas ações, negligencia medidas de segurança ou compartilha informações sensíveis, expondo-se a ameaças cibernéticas.

Tais situações podem decorrer tanto da falta de conhecimento sobre os riscos quanto de comportamentos imprudentes ou confiança excessiva na segurança digital. A sua aplicação teórica no contexto digital demanda uma análise cuidadosa das ações e comportamentos da vítima. É necessário avaliar se a vítima possuía informações adequadas sobre os riscos envolvidos e se agiu de maneira negligente ou imprudente diante dessas informações. Além disso, é essencial examinar a presença de intenção por parte da vítima em assumir o risco, mesmo que esta intenção seja muitas vezes sutil ou inconsciente.

A incógnita do conhecimento do risco no mundo virtual, relacionada à teoria da autocolocação da vítima em risco, suscita reflexões fundamentais sobre a interação entre as ações da vítima e sua vulnerabilidade ao risco digital. Torna-se evidente, dessarte, que se devidamente aplicada, essa teoria é um elemento que pode influenciar positivamente a análise jurídica dos crimes cibernéticos.

Por outro lado, a heterocolocação da vítima em risco ocorre quando o agente permanece como figura central, no entanto, a vítima concorda tacitamente com a ação

---

[27] SYDOW, Spencer Toth. Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática. Dissertação (Mestrado em Direito Penal). Universidade de São Paulo, São Paulo, 2009.

[28] GRECO, Luís; LEITE, Alaor. O que é e o que não é a teoria do domínio do fato. Sobre a distinção entre autor e partícipe no direito penal. *In*: GRECO, Luís et al. Autoria como domínio do fato: estudos introdutórios sobre o concurso de pessoas no direito penal brasileiro. São Paulo: Marcial Pons, 2014, p. 19-30.

por ele desempenhada. Essa conjuntura abarca cenários em que a pessoa em questão não se expõe intencionalmente ao perigo, mas permite que outro a coloque em situação de risco, estando ciente desse perigo[29].

Nesse viés, abordando o caso prático em questão, pode-se dizer que envolve situações em que terceiros, como hackers ou criminosos cibernéticos, deliberadamente exploram vulnerabilidades no ambiente digital da vítima para perpetrar crimes. Essas vulnerabilidades podem ser falhas de segurança em sistemas, falta de atualizações ou desconhecimento sobre práticas seguras na internet. Assim, a vítima, em grande parte, está à mercê das ações maliciosas de outros.

A teoria da heterocolocação da vítima em risco consentido, à luz do contexto digital, parte do princípio de que, em certos casos, a própria vítima, voluntariamente ou não, contribui para sua exposição ao risco. No mundo virtual, isso pode ser interpretado como a aceitação inconsciente ou até mesmo consciente de certos riscos ao adotar determinados comportamentos online.

Contudo, ao aplicar essa teoria nesse contexto, deparamo-nos com desafios únicos. O ambiente virtual muitas vezes apresenta uma ilusão de segurança, levando os usuários a subestimar os riscos reais associados a suas atividades online. A ampla variedade de ameaças cibernéticas, muitas vezes camufladas sob a aparência de sites e comunicações legítimas, torna difícil para a vítima discernir os perigos.

É importante considerar que, no mundo virtual, os usuários podem ser vítimas involuntárias de crimes cibernéticos, mesmo quando suas ações parecem indicar um consentimento aparente. Por exemplo, a manipulação psicológica de um golpe online pode levar a vítima a compartilhar informações confidenciais, mesmo sem uma compreensão completa do risco.

Desse modo, destaca-se a importância de avaliar a conduta da vítima e sua relação com a exposição ao risco. No entanto, ao considerar o mundo virtual, é essencial levar em conta a influência dos ambientes digitais altamente dinâmicos e da engenharia social sofisticada que pode falsear a percepção da vítima sobre o risco.

Além disso, a heterocolocação da vítima em risco apresenta um desafio para a responsabilização legal, pois a vítima pode não ter controle sobre as ações dos perpetradores. As teorias de Roxin sobre a culpabilidade fornecem um entendimento

[29] ROXIN, Claus. Funcionalismo e imputação objetiva no direito penal. Tradução de Luís Greco. Rio de Janeiro: Renovar, 2002. p. 367.

que auxilia na compreensão da relevância da intenção e do conhecimento da vítima na configuração de sua vulnerabilidade perante os criminosos cibernéticos.

No entanto, vale ressaltar que a complexidade da temática também reside no fato de que as vítimas podem ser responsabilizadas injustamente ou culpabilizadas por suas próprias vulnerabilidades, resultando em um fenômeno conhecido como "vitimização secundária"[30], fato que ocorre quando as vítimas são estigmatizadas, desacreditadas ou não recebem o apoio adequado de instituições e sistemas jurídicos, havendo um descaso às suas garantias e aos seus direitos fundamentais no curso da investigação ou do processo penal.

Conforme enfatizado por Roxin, a clara finalidade da imputação objetiva reside em identificar quais relações causais configuram ações objetivamente típicas. Somente após esse discernimento, prossegue-se à avaliação da tipicidade subjetiva, isto é, a averiguação da presença do dolo[31]. Busca-se, desse modo, determinar se uma determinada ação é imputável ao autor ou se advém do acaso, de terceiros ou da própria vítima.

A teoria da imputação objetiva, formulada por Claus Roxin, fundamenta-se na noção de que a imputação penal deve se basear em critérios objetivos de causalidade e previsibilidade. No contexto da incógnita do conhecimento do risco no mundo virtual, a imputação objetiva ganha relevância ao tentar determinar em que medida o sujeito poderia e deveria ter previsto e evitado os riscos inerentes às suas atividades digitais.

Roxin destaca a importância da imputação objetiva no direito penal, considerando a causalidade adequada, que leva em conta o comportamento da vítima[32]. Nesse contexto, a análise das ações ou omissões da vítima na esfera digital é crucial para determinar sua contribuição para a ocorrência do crime cibernético.

Entretanto, aplicar a imputação objetiva ao mundo virtual não é uma tarefa trivial. A dinâmica e a complexidade desse ambiente, aliadas à rápida evolução tecnológica, desafiam a tradicional abordagem da imputação objetiva. Ainda assim, é

---

[30]Também chamada de “Revitimização” ou de “Sobrevitimização”, é aquela causada pelas instâncias formais que detêm o controle sobre o âmbito social (isto é, em delegacias, no Ministério Público etc.). Abrange os custos pessoais derivados da intervenção do sistema legal que podem aumentar o sofrimento da vítima. Ocorre quando há desrespeito às garantias e aos direitos fundamentais das vítimas de crime no curso da investigação ou do processo penal. “Vitimização” em: https://www.cnmp.mp.br/defesadasvitimas/vitimas/vitimizacao#:~:text=Vitimiza%C3%A7%C3%A3o%20secund%C3%A1ria&text=Abrange%20os%20custos%20pessoais%20derivados,investiga%C3%A7%C3%A3o%20ou%20do%20processo%20penal. Acesso em: 25 set. 2023

[31] ROXIN, Claus. Politica Criminal y estrutura del delito. Trad. Juan Bustos Ramirez e Hernan Hormozabal Malarée. Barcelona: PPU, 1992, p. 363.

[32] ROXIN, Claus. *Op. Cit.* Nota 29.

essencial reconhecer que, em muitas situações, a imputação objetiva pode fornecer uma estrutura sólida para analisar a responsabilidade dos agentes envolvidos.

No contexto marcado por uma incógnita do conhecimento do risco no mundo virtual, é possível considerar também que, dependendo do caso, a imputação objetiva pode ser aplicada na avaliação da conduta da vítima e do agente. Por exemplo, ao analisar uma vítima de um golpe de *phishing*[33] que não tinha conhecimento suficiente para identificar a fraude, o entendimento da imputação objetiva pode auxiliar na determinação do grau de previsibilidade que se poderia razoavelmente esperar dela.

Contudo, a imputação objetiva, ao lidar com o mundo virtual, precisa ser flexível o suficiente para incorporar as particularidades desse ambiente. A tecnologia pode superar a capacidade média de compreensão e previsão do usuário comum, o que implica que a responsabilidade precisa ser adaptada em conformidade.

Além disso, a imputação objetiva deve considerar o papel das instituições e do desenvolvimento tecnológico na mitigação do conhecimento do risco. Empresas e governos têm responsabilidades na proteção dos indivíduos contra riscos cibernéticos e na educação sobre segurança digital.

A relevância de os usuários assumirem um papel central é destacada por Sydow[34], o qual frisa que estes não atuam apenas como coadjuvantes, mas como protagonistas. Afastando assim, o viés paternalista do direito penal devido à sua autocolocação em situação de risco e sinalizando a necessidade crucial de os usuários assumirem obrigações diretas.[35]

É importante ressaltar, por exemplo, que ao discutir a autocolocação da vítima em risco, não está se alegando que a vítima tenha a intenção de ter seu direito prejudicado. Na verdade, apesar de gerar uma situação de risco, a vítima acredita que o desfecho em relação aos seus direitos não a prejudicará. Além disso, não estamos defendendo a ideia de que a atitude da vítima justifique a conduta do autor, eximindo-o de responsabilidade pelos prejuízos causados em qualquer caso, o que se busca ao abordar esse conceito, em verdade, é analisar as circunstâncias que podem modular a censurabilidade da conduta do autor em casos de crimes cibernéticos,

[33] O crime de *phishing* é uma atividade criminosa em que os perpetradores tentam enganar pessoas, geralmente por meio de mensagens eletrônicas ou sites falsos, para obter informações confidenciais, como senhas, números de cartão de crédito ou outras informações pessoais.
[34] SYDOW, Spencer Toth. Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática. Dissertação (Mestrado em Direito Penal). Universidade de São Paulo, São Paulo, 2009.
[35] BRITO, Auriney. Direito Penal Informático. São Paulo: Saraiva, 2013, pp. 697-698.

especialmente quando a vítima contribui de alguma forma para o dano ao seu próprio bem particular, o que pode ter implicações no âmbito penal.[36]

As reflexões fundamentais sobre a interação entre as ações da vítima e sua vulnerabilidade ao risco digital, é visto que compreender a contribuição da vítima para sua própria exposição a ameaças cibernéticas é crucial para a formulação de estratégias eficazes de prevenção e conscientização.

O contexto da vítima perante a imersão numa sociedade de riscos revela primordialmente que aqueles que são afetados hão de se ter um entendimento mais aprofundado do âmbito em que estão inseridos, reconhecendo que a atitude e comportamento nesse contexto devem ser extremamente prudentes e conscientes. Os riscos considerados, nesse cenário, são de natureza coletiva e representam uma preocupação essencial para uma convivência harmoniosa. Navegar em meio à incerteza demanda uma atenção redobrada e passos cuidadosos, assim como a utilização de outros métodos de orientação, cujos olhos se mostram de escassa relevância.

Destarte, a incógnita do conhecimento do risco no mundo virtual apresenta desafios incalculáveis no campo jurídico, particularmente no que diz respeito ao entendimento à luz das teorias expostas que são defendidas por Claus Roxin. Embora essa teoria ofereça uma estrutura valiosa para avaliar a responsabilidade no ambiente digital, é fundamental adaptá-la às particularidades e dinâmicas desse cenário em constante evolução, que nem sempre se coadunam. Motivo pelo qual há entendimentos filosóficos contemporâneos que contrapõem os ideais anteriormente expostos, que serão dispostos no próximo tópico.

2.2 Conscientização da vítima no ambiente virtual: Perspectiva filosófica contemporânea

Em primeiro lugar, o contexto do risco, manifestado de modo evidente no mundo virtual, propicia uma analogia ao agente delituoso nesse ambiente. Todavia, ao reconhecer a vulnerabilidade na percepção social do ciberespaço pela coletividade,

[36] SYDOW, Spencer Toth. *Op. Cit*. Nota 34.

acresce-se à análise da vantagem na execução do delito o elemento de que a conduta inadequada dos cibernautas potencializa ainda mais as ações criminosas[37].

À vista disso, é essencial mencionar que a complexidade do mundo digital traz desafios à aplicação do teor central das teorias expostas por Roxin. O ambiente virtual é dinâmico e constantemente evolutivo, o que pode dificultar a determinação precisa da consciência do risco. Além disso, a rápida inovação tecnológica pode superar o conhecimento médio do usuário, tornando a análise da consciência do risco um desafio substancial.

É importante considerar que a culpabilidade, segundo Roxin, também se baseia na avaliação subjetiva do agente[38]. No entanto, no contexto digital, a subjetividade pode ser influenciada por diversos fatores, como a familiaridade com a tecnologia, a idade, a cultura e a formação educacional. Estes fatores podem moldar a percepção individual do risco, tornando a análise da culpabilidade uma tarefa complexa de ser analisada primordialmente.

Ora, para Roxin[39], no que tange à exposição voluntária ao perigo, para além da completa ciência dos riscos envoltos na empreitada, é imperativo, como condição crucial, que a pessoa afetada seja responsável por suas ações. Tendo em vista que, para o filósofo, a vítima precisa ter um preciso conhecimento do risco que ela está inserida.

O contexto que se insere o risco amplamente presente na internet proporciona uma lógica análoga para o criminoso no ambiente virtual. Entretanto, considerando a vulnerabilidade existente na percepção social do ambiente virtual por parte da coletividade, acrescenta-se à consideração da vantagem no cometimento do delito o aspecto de que o comportamento inadequado dos usuários da internet torna as práticas criminosas ainda mais facilitadas.

Sendo de válida constatação para nossa análise a seguinte afirmação de Lisboa:

> Essas facilidades estão tão em evidência no cotidiano que não há uma percepção clara de que se vive em uma sociedade informatizada, onde os

[37] SYDOW, Spencer Toth. *Op. Cit*. Nota 34.
[38] ROXIN, Claus. *Op. Cit.* Nota 29.
[39] ROXIN, Claus. *Op. Cit.* Nota 31.

> dados fluem a velocidades inimagináveis há alguns anos, e tudo isso influi em nos valores sociais e econômicos.[40]

Nessa perspectiva, um termo como o da modernidade líquida[41], cunhado pelo sociólogo Zygmunt Bauman, descreve a condição atual da sociedade, caracterizada pela fluidez e volatilidade das relações e estruturas sociais. Bauman argumenta que a modernidade líquida é marcada pela transitoriedade, pela fragilidade dos laços sociais e pela falta de estabilidade. Esta concepção reflete-se nas relações digitais[42] e no universo cibernético, onde as interações são efêmeras e mutáveis, dificultando a construção de conexões sociais sólidas.

No contexto dos crimes cibernéticos, essa fluidez torna-se um elemento crítico, em virtude de tantos desafios e peculiaridades, sendo um fenômeno intrínseco ao mundo contemporâneo. As vítimas muitas vezes não possuem estruturas sólidas de apoio ou de segurança no mundo virtual. Os perpetradores de ataques cibernéticos se aproveitam dessa falta de estabilidade, causando danos em uma realidade que se assemelha à água, escorrendo por entre os espaços virtuais.

A efemeridade das relações online também se reflete na impessoalidade típica da modernidade líquida. As interações digitais, muitas vezes desprovidas de contato físico ou emoções palpáveis, podem levar a uma impessoalidade, tanto dos agressores quanto das vítimas, para os impactos reais de suas ações e sofrimentos, principalmente no que diz respeito aos delitos de cunho sexual no ambiente virtual.

Aludindo ao caso prático, o aplicativo Tinder, por exemplo, é uma popular aplicação de encontros que utiliza geolocalização para conectar usuários com base em preferências e localização física. Embora tenha facilitado a introdução de pessoas com interesses semelhantes, também foi associado a situações de assédio, exploração e até crimes mais graves. É nesse viés que a Secretaria da Segurança Pública de São Paulo (SSP) afirmou à BBC News Brasil que "mais de 90% dos sequestros registrados em São Paulo são feitos a partir de relacionamentos formados

---

[40] LISBOA, Roberto Senise. Direito na Sociedade da Informação, 2016. Disponível em:http://www.egov.ufsc.br/portal/conteudo/direito-na-sociedade-da-informa%C3%A7%C3%A3o. Acesso em: 28 set. 2023.

[41] BAUMAN, Zygmunt. Modernidade Líquida. Tradução, Plínio Dentzien. Rio de Janeiro: Jorge Zahar Ed., 2001.

[42] BAUMAN, Zygmunt. Amor Líquido: Sobre a Fragilidade dos Laços Humanos. Rio de Janeiro: Zahar, 2004.

a partir de perfis falsos criados em aplicativos como o Tinder"[43]. Sendo nítido, portanto, que usuários desses aplicativos enfrentam riscos consideráveis tomados por descuidos, valendo ressaltar a importância de considerar essas questões ao utilizar tais aplicativos.

Bauman também aponta a tendência de individualização na modernidade líquida, onde os indivíduos são levados a se preocupar mais consigo mesmos do que com o bem comum[44]. No âmbito dos crimes cibernéticos, essa individualização pode se traduzir na busca por autoproteção digital, mas também na negligência das consequências prejudiciais que ações individuais podem ter para a coletividade.

A crítica de Zygmunt Bauman ao tratar acerca da modernidade líquida, trazida aos tempos hodiernos, lança luz sobre as características sociais e comportamentais que permeiam o cenário dos crimes cibernéticos. A fluidez, impessoalidade e individualização presentes na modernidade líquida moldam e influenciam as dinâmicas dos crimes cibernéticos.

Diante de uma situação como essa, é imprescindível a compreensão da interação do mundo virtual e do mundo real, sendo, atualmente, difícil separar o virtual do real, pois ambos estão intrinsecamente entrelaçados.

A fronteira entre esses dois mundos está se tornando cada vez mais tênue, haja vista que, com a crescente influência do mundo virtual em vários aspectos da vida, como relacionamentos, trabalho, entretenimento e até mesmo na formação da identidade pessoal, surge exponencialmente mais uma necessidade indubitável da busca por uma devida percepção no que tange a interação entre esses dois espaços. Para assim, que haja um maior entendimento e prevenção de qualquer situação indesejada num vasto e ainda pouco conhecido mundo cibernético.

Pierre Lévy, uma figura de destaque nesse campo, costuma traçar essas diferentes perspectivas sobre essa relação[45]. De modo que, por um lado, há aqueles que erroneamente acreditam que o mundo virtual é uma mera ilusão, onde as interações e experiências não possuem a mesma importância ou valor do mundo físico. Por outro lado, há aqueles que reconhecem a relevância do mundo virtual como

---

[43] “9 em cada 10 sequestros de SP são 'golpes do Tinder'”. Disponível em: https://www.bbc.com/portuguese/brasil-63733202. Acesso em: 02 out. 2023.
[44] BAUMAN, Zygmunt. *Op. Cit.* Nota 41.
[45] LÉVY, Pierre. O Que é Virtual? Rio de Janeiro: Editora 34, 1996.

um espaço de interações sociais legítimas e experiências reais, que com certeza se sobressaem no quesito da prevenção à vulnerabilidade no ambiente digital.

O filósofo destaca a importância de compreendermos essa natureza complexa e interconectada do mundo virtual e real, deixando nítido que não devemos negar a realidade do mundo virtual, mas sim abraçá-la como parte integrante da nossa experiência atual. Este defende ainda que a compreensão e o equilíbrio entre esses dois mundos são essenciais para uma participação consciente e significativa na sociedade contemporânea.

Levy argumenta que vivemos em um mundo altamente imerso em conexões, onde a informação flui em uma velocidade sem precedentes. Assim sendo, o ciberespaço representa um meio de comunicação resultante da interconexão global de computadores. Denominação essa que não apenas descreve a infraestrutura de comunicação digital, mas também engloba o conjunto de informações hospedadas e os indivíduos que utilizam esse sistema.

Entretanto, essa hiper conexão também traz uma falta de consciência sobre os riscos associados às nossas atividades no mundo virtual. O desconhecimento do risco, na perspectiva de Levy, advém da velocidade e complexidade do ambiente digital, que muitas vezes supera nossa capacidade de compreensão.

A crítica de Levy reflete a importância de compreendermos a dinâmica do mundo virtual e das suas inúmeras implicações. O mesmo ressalta a necessidade de educação e conscientização para lidar com os riscos inerentes às interações online[46]. Como também, que a consciência sobre o risco é essencial para o desenvolvimento de uma sociedade imersa ao ambiente virtual, mas, ao mesmo passo em que seja devidamente responsável e informada dos incontáveis riscos nesse meio.

Ademais, torna-se evidente que o engajamento da mente humana com a tecnologia amplia seus limites, transcendendo a esfera cerebral e corporal. Tal extensão pode resultar em uma percepção distorcida dos riscos, levando a comportamentos arriscados no contexto virtual.

Assim, o conceito de extensão da mente para além do cérebro e do corpo, conforme enfatizado por Andy Clark[47], tem implicações profundas no modo como os seres humanos interagem com a tecnologia e percebem o mundo ao seu redor. Essa

[46] LÉVY, Pierre. Cibercultura. 1 ed. São Paulo: 34, 1999, p. 16.
[47] CLARK, Andy. Natural-Born Cyborgs: Minds, Technologies, and the Future of Human Intelligence. Oxford University Press, 2003.

ideia rompe com a visão tradicional de que a mente está contida dentro do cérebro e que a interação com o ambiente é meramente uma entrada de informações para esse órgão central. Pelo contrário, Clark propõe que a mente se estende para além dos limites físicos do corpo e incorpora objetos e ferramentas externas, incluindo a tecnologia.

A interação cotidiana com a tecnologia moderna é um exemplo claro dessa extensão da mente. Os smartphones, computadores e outros dispositivos digitais não são meramente ferramentas externas, mas se tornaram extensões integradas da nossa cognição e da maneira como percebemos o mundo, facilitando o acesso a vastas quantidades de informações, nos ajudam a resolver problemas, aprimoram nossa comunicação e permitem a realização de tarefas complexas.

No entanto, como visto, essa extensão da mente para o domínio digital também tem implicações para a percepção do risco. A natureza da interação com o ambiente virtual pode distorcer nossa compreensão e avaliação dos perigos presentes nesse contexto. A sensação de segurança e desapego físico que o mundo virtual proporciona pode levar a uma percepção subestimada do risco. Isso pode, por sua vez, desencadear nos tantos comportamentos de descuido que muitos dos usuários perpassam, pois as consequências parecem menos imediatas e tangíveis quando comparadas com a realidade física.

A perda da noção de consequências reais pode ser exacerbada pela separação entre as ações virtuais e suas repercussões no mundo físico. Assim sendo, as pessoas podem se envolver em atividades perigosas sem sentir as reais implicações dessas ações no âmbito virtual, podendo resultar em comportamentos imprudentes e, em alguns casos, viciantes.

Portanto, é fundamental considerar essa extensão da mente ao interagir com a tecnologia e garantir que haja uma compreensão equilibrada e consciente dos riscos associados a essas interações, retando nítido mais uma vez o quão crucial é educar as pessoas sobre as implicações de suas ações no mundo virtual e promover uma cultura de responsabilidade e consciência ao utilizar a tecnologia como uma extensão de suas mentes e comportamentos.

As críticas apontam para a necessidade de uma abordagem mais incisiva e reflexiva em relação à nossa interação com a tecnologia. A falta de consciência dos riscos pode resultar em vulnerabilidade e exposição indevida no mundo digital. Assim, resta cada vez mais aparente o quão fundamental é a promoção da alfabetização

digital e da consciência dos riscos cibernéticos como parte integrante da educação contemporânea.

Desse modo, faz-se incontestável o entendimento de que o equilíbrio entre esses dois mundos é algo intrínseco à realidade da sociedade hodierna. Devemos aprender a navegar nesse espaço interconectado com discernimento, compreendendo suas nuances e impactos em nossa vida diária. Isso implica considerar as implicações éticas, sociais, psicológicas e culturais dessa interação, e promover práticas responsáveis e éticas ao nos engajarmos no mundo virtual. Em última análise, a compreensão e a sabedoria na interação entre esses mundos nos capacitam a usar a tecnologia de forma construtiva e a moldar um futuro onde ambos coexistem de maneira harmoniosa e benéfica.

Para tal, enquanto as teorias anteriormente citadas oferecem uma base conceitual útil para entender a responsabilidade da vítima em relação à sua exposição ao risco, é necessário adaptá-las considerando as peculiaridades e os inúmeros desafios desencadeados por um descaso no tocante à devida valoração do papel da vítima do crime e de um ineficaz controle penal dos crimes cibernéticos, que serão melhor delineados nos tópicos seguintes.

2.3 A Relevância da conduta da vítima e o seu impacto perante à dogmática penal informática

A princípio, desvendou-se a importância dos cuidados que a vítima deve observar na era virtual, valendo-se de abordagens funcionalistas e filosóficas que esclareceram essa complexa questão. Constatamos que a conduta da vítima desempenha um papel significativo na dinâmica dos crimes cibernéticos e na busca por soluções eficazes.

Desse modo, ao mesmo passo, neste tópico busca-se um maior aprofundamento da relevância conduta da vítima sob perspectiva da dogmática penal, explorando assim como essa abordagem modela a resposta do sistema jurídico aos crimes cibernéticos e fornecendo uma visão abrangente e crítica sobre o papel fundamental da vítima no âmbito do direito penal.

No âmbito do sistema jurídico penal, o estudo da conduta da vítima de crime emerge como um tema de relevância inegável, tendo em vista seu potencial impacto

na aferição da responsabilidade penal do autor. A vítima[48], muitas vezes vista como um elemento passivo, pode, em determinados contextos, desempenhar um papel crucial na configuração da ilicitude e culpabilidade do agente. Nesse contexto, a presente análise crítica visa explorar a interação entre a conduta da vítima e a responsabilidade penal do autor do crime, embasando-se em referências conceituadas que contribuem para a compreensão aprofundada desta dinâmica complexa.

A dogmática penal, enquanto sistema teórico que busca explicar e sistematizar os elementos constitutivos do crime, tradicionalmente enfoca a conduta do autor como fator central na análise da responsabilidade penal. No entanto, uma crescente corrente de pensamento defende que a conduta da vítima também deve ser considerada, especialmente em casos que envolvem situações onde a vítima tenha tido um papel ativo ou negligente que possa influenciar o desfecho do evento.

Nesse sentido, um dos pioneiros penalistas a desenvolver melhor acerca do comportamento da vítima foi Claus Roxin[49], como exposto anteriormente, que designava que a análise da conduta da vítima é fundamental para a identificação da causalidade e da imputação objetiva. O renomado jurista lança luz sobre a importância de não apenas analisar a conduta do autor, mas também a da vítima, para estabelecer esta relação de causalidade e aferir se a ação do autor é efetivamente criminosa a ponto de ser o único pretexto a ser levado em conta na aferição da responsabilidade do crime.

A responsabilidade penal do autor não deve ser encarada de forma isolada, mas sim como parte de um contexto mais amplo que inclui a interação entre as partes envolvidas no evento delitivo. A vítima, como parte dessa equação, pode influenciar de maneira significativa a avaliação da culpabilidade do autor. Nesse contexto, a abordagem do direito comparado, exemplificada pelo sistema alemão, enfatiza a análise da "culpa da vítima" como um elemento que pode atenuar a responsabilidade penal do autor.

É nesse ponto que o jurista e filósofo do direito alemão, Hans Welzel[50], traz uma perspectiva interessante, argumentando que, em certos casos, a conduta imprudente

---

[48] ANDRADE, Manuel da Costa. O*p. Cit*., nota 1, p. 50.
[49] Roxin, Claus. Autoría y dominio del hecho en el derecho penal. Madrid: Marcial Pons, 2000.
[50] WELZEL, Hans. Derecho penal alemán. Tradução de Juan Bustos Ramírez y Sergio Yáñez Pérez. 11. ed. Santiago: Editorial Jurídica de Chile, 2003.

ou negligente da vítima pode contribuir para reduzir o grau de culpabilidade do autor. Esta abordagem, embora não seja aplicada uniformemente em todas as jurisdições, levanta questões importantes sobre a influência mútua entre as ações da vítima e do autor na determinação do desfecho do crime.

A análise crítica aqui apresentada destaca a importância da conduta da vítima de crime na dogmática penal e na aferição da responsabilidade penal do autor. Através da exploração das contribuições de reconhecidos juristas, observamos como a interação entre ações da vítima e do autor pode ser um elemento fundamental na determinação da ilicitude e da culpabilidade. A conduta da vítima não deve ser negligenciada, especialmente em casos onde sua ação, omissão ou negligência tenham influenciado a dinâmica do evento delitivo.

Em linha tênue, no que se refere ao ordenamento jurídico brasileiro vigente, observa-se que há uma escassez de originalidade no que tange à devida análise da conduta da vítima, aliada a restrições legislativas e limitada assimilação das teorias modernas do crime que poderiam impulsionar o avanço na análise da criminalidade eletrônica. A evolução das teorias sobre o delito no contexto do Direito Penal Brasileiro deixa algumas incertezas quanto à aplicabilidade do comportamento da vítima em situações concretas, gerando uma instabilidade no parâmetro normativo citado.

Além disso, é nítido que o legislador, em geral, não buscou, frente à doutrina estrangeira mais atualizada, alinhar suas propostas de reforma do Código Penal com os novos conceitos sobre risco advindos do funcionalismo positivado europeu.

Este cenário da doutrina jurídica brasileira, no entanto, empenha-se para conhecer e compreender essas novas teorias, buscando também avaliar os crimes já existentes, geralmente ancorados em uma legislação que, em muitos aspectos, se mostra desatualizada e necessitada de revisão.

Os delitos informáticos, por sua vez, dada a sua natureza recente, permanecem envoltos em uma aura de incompreensão. Portanto, é notória a necessidade de um esforço intelectual concentrado e uma postura mais dinâmica no âmbito legislativo, a fim de que sejam devidamente atualizadas as abordagens referentes à criminalidade eletrônica, proporcionando uma compreensão mais abrangente e atualizada das dinâmicas criminais referentes à vítima, principalmente no que diz respeito à era digital.

Embora haja desafios práticos e teóricos na aplicação sistemática desses conceitos, a abordagem crítica e multidimensional apresentada neste artigo contribui

para a reflexão e o debate sobre a evolução da dogmática penal e da responsabilidade penal do autor no cenário jurídico contemporâneo, principalmente no que diz respeito aos crimes cibernéticos, que serão abordados com um maior enfoque no capítulo seguinte.

Em outras palavras, vale considerar, que intensas discussões acerca dessa temática em questão predominam investigações europeias, principalmente, em debates jurídicos germânicos e espanhóis[51]. Que se concentra tanto na contribuição da vítima para o resultado lesivo quanto nas consequências dessa contribuição no tocante ao injusto, especialmente na determinação da punição ao agente, tendo em vista que pode levar tanto à sua redução ou até mesmo à sua isenção.

Nesse contexto, divergem os estudiosos: de um lado, há defensores da simples diminuição da pena (com consideração pontual para a possibilidade de uma causa acima das leis que exclua a ilegalidade), e, por outro lado, há aqueles que enxergam, além da redução, a possibilidade de isenção completa da responsabilidade do autor, negando a tipicidade de sua conduta.

Nesse viés, Celso Delmanto[52] trata que tão somente à primeira vista o dispositivo penal serve para abrandar a sanção no tocante ao quesito em espeque. Haja vista que, em verdade, o Código Penal brasileiro não vê o comportamento da vítima como atenuante, mas o considera somente como uma das circunstâncias judiciais a serem avaliadas na valoração da pena-base, tal como, vale a ressalva de que raramente é utilizada para minorar a pena do sentenciado.

Assim sendo, na visão de Delmanto[53], o comportamento da vítima deve ser avaliado de forma abrangente, levando em conta a censurabilidade da conduta do agente, podendo tanto diminuí-la, quanto, eventualmente, agravá-la.

Diante disso, é notório nos tempos hodiernos que um importante fator que contribuiu para que a vítima não tivesse a devida ênfase na análise criminal foi o foco exclusivo da criminologia, que se dedicava a estudar empiricamente o fenômeno penal, concentrando-se, de forma tradicional, na pessoa que pratica o comportamento ilícito, ou seja, no autor do crime.

---

[51] SCHÜNEMANN, Bernard. Teoria de la imputación objetiva. Traduccion de Mariana Sacher de Köser. *In*: Revista de política criminal e ciências penais. n. I, especial. Mexico, 1999. p.33
[52] DELMANTO, Celso. *et al.* Código Penal Comentado. 8. ed. São Paulo: Saraiva, 2010. p. 275
[53] DELMANTO, Celso. *Op. Cit*. Nota 52.

Nesse ritmo, a vítima teve um papel consideravelmente reduzido, sendo vista apenas como uma observadora, enquanto toda a atenção era voltada para o criminoso, o que acabou escanteando a relevante atuação da vítima em determinados delitos, sendo nítido, sobretudo, em inúmeros crimes envolvendo o mundo virtual.

Outrossim, partindo dessa ideia central por ora delineada, deixamos de lado a questão de quem é mais importante para o resultado, que é o cerne do debate tradicional sobre autoria e participação. Em vez disso, focamos na conduta independente, dando-lhe um papel principal. O que importa, em verdade, é verificar se a interação entre o autor e a vítima leva a uma ação que pode ser atribuída à vítima e que não seja típica tão somente do autor[54].

Desse modo, mesmo que a vítima não saiba do risco ao se envolver em certa ação, a conduta do autor pode ser considerada atípica, desde que a atividade conjunta se dirija claramente à área de responsabilidade da vítima, com base na relação entre autonomia e responsabilidade.

Frente a essa situação, recorreremos às doutrinas de alcance internacional, notadamente de maneira majoritária oriundas da Alemanha e Espanha, a fim de que, inseridos no contexto de pensamentos funcionalistas, seja possível incluir o elemento da “conduta da vítima" na análise da tipicidade penal.

Nesse contexto, em uma sociedade caracterizada por sua exposição a riscos e pela interligação global, na qual a comunicação se expande através de uma ampla troca cultural, ocorre uma evolução e atualização contínuas das perspectivas jurídicas. Nesse sentido, torna-se de tal modo inconcebível acatar a presença de estruturas lógico-objetivas[55].

Pois bem, no contexto em constante evolução dos crimes cibernéticos, é fundamental reconhecer a importância do papel da vítima no âmbito da dogmática penal. Não podemos nos ater exclusivamente a considerações sistêmicas abstratas que, embora sejam cruciais para garantir a legalidade e a segurança jurídica, não podem se transformar em um pensamento que negligencia a investigação e adaptação das leis diante de situações complexas e mutáveis[56].

---

[54] SILVA JÚNIOR, Délio Lins e. Imputação e a conduta da vítima. Curitiba: Juruá, 2008.
[55] BITENCOURT, Cezar Roberto. Tratado de Direito Penal: Parte Geral. 19ª ed. São Paulo: Saraiva, 2012, p. 121.
[56] FONSECA, Ana Clara Montenegro. Conduta da vítima de crime na dogmática penal: análise crítica sobre a posição da vítima na aferição da responsabilidade penal do autor à luz da vitimodogmática e da imputação à vítima. Dissertação (Mestrado em Direito) - Faculdade de Direito do Recife, Recife,

A dogmática jurídico-penal desempenha um papel essencial na construção de uma sociedade justa e segura. No entanto, sua importância não reside na mera reverência à norma ou na aplicação mecânica das leis à realidade. Em vez disso, a verdadeira relevância do dogmatismo jurídico está na capacidade de reconstruir e efetivar as normas em contextos sociais concretos, que estão sempre em evolução e moldados pela história[57]. Isso se torna particularmente evidente nas perspectivas das vítimas, onde as complexidades das experiências individuais da vítima não podem ser ignoradas.

Assim, a abordagem sensata para o dogmatismo jurídico-penal envolve a um paradigma mais nítido das normas jurídicas e da busca do seu significado atual por meio de interpretações doutrinárias e jurisprudenciais. Essa abordagem visa integrar as normas em um sistema coerente e, ao mesmo tempo, adaptá-las às circunstâncias em constante mudança que surgem na prática. No que diz respeito às ações da vítima, a abstração conceitual das normas deve ser ajustada para acomodar as complexidades e singularidades dos problemas enfrentados pela vítima em questão[58].

Portanto, é fundamental reconhecer que a dogmática penal não deve ser inflexível ou dogmática no sentido pejorativo, mas sim flexível o suficiente para se ajustar às realidades em constante mutação do mundo cibernético. Esse entendimento é essencial, pois as vítimas de crimes cibernéticos muitas vezes enfrentam desafios únicos e complexos que não podem ser tratados com uma abordagem genérica.

O Direito deve ser sensível às experiências das vítimas e adaptar-se para proporcionar uma resposta justa e eficaz às violações que ocorrem no ambiente digital em constante evolução. Portanto, a dogmática penal deve ser uma ferramenta dinâmica que busca constantemente garantir a justiça e a proteção de todos os envolvidos no cenário dos crimes cibernéticos.

Observamos uma crescente instabilidade em decorrência do aumento da impunidade, resultando em uma preocupante insegurança jurídica, o que, por conseguinte, acaba gerando uma desconfiança no papel do Estado e representando um perigo latente passível de gerar conflitos. Em resposta a esses desafios, é

2009. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/4736/1/arquivo6332_1.pdf. Acesso em: 10 ago. 2023.

[57] FONSECA, Ana Clara Montenegro. *Op. Cit*. Nota 56.

[58] FONSECA, Ana Clara Montenegro. *Op. Cit*. Nota 56.

imprescindível a compreensão dos tamanhos riscos e descuidos em que as vítimas estão imersas, como fora cuidadosamente discutido ao longo deste estudo.

Destarte, o critério a ser observado primordialmente é a interação entre o autor e a vítima em cada situação específica, como um ofendido tem muitas vezes uma considerável participação na configuração de vários crimes cibernéticos. Partindo de um contexto do aspecto objetivo, sem considerar inicialmente elementos subjetivos, como intenção ou culpa, para garantir que não nos afastemos do objetivo principal deste estudo: a reformulação do aspecto objetivo com base em critérios objetivos e regulamentares.

Assim sendo, ao longo desta pesquisa exploramos a complexa questão do papel da vítima e da segurança cibernética sob o prisma de abordagens vitimodogmáticas, funcionalistas e filosóficas, visando compreender os cuidados necessários nessa era digital. Através dessas perspectivas, analisamos como a interação entre vítima e o sistema jurídico se desdobra no contexto dos crimes cibernéticos, ressaltando a importância da conduta da vítima como fator determinante a ser analisado no parâmetro criminal.

À medida que encerramos este capítulo, fica claro que o papel da vítima desempenha um papel fundamental no enfrentamento dos desafios advindos da criminalidade digital, reverberando em tipos penais já consolidados na legislação brasileira. De maneira que esta compreensão prepara o terreno para o próximo capítulo, que abordará minuciosamente acerca da ineficácia do controle penal dos crimes cibernéticos, destacando a necessidade de reformas e estratégias mais eficazes no âmbito da segurança cibernética.

3. A INEFICÁCIA DO CONTROLE PENAL DOS CRIMES CIBERNÉTICOS

Pelo que estudamos nos capítulos anteriores, resta absolutamente notório o quanto o avanço da tecnologia revolucionou profundamente a forma como as pessoas interagem, trabalham, consomem, e até mesmo cometem crimes. Neste cenário, as relações jurídicas encontram-se cada vez mais imersas nesse ambiente digital, moldando um novo panorama para o Direito.

Por isso, é necessário compreender a magnitude dessa transformação para apreciar a complexidade e a amplitude que essa nova realidade impõe ao campo jurídico, haja vista que, tal situação, consequentemente, abriu margens para uma constante expansão de novas formas de criminalidade no âmbito virtual, fazendo com que os chamados crimes cibernéticos representem uma ameaça crescente na sociedade contemporânea, utilizando-se das mais variadas tecnologias de informação e de comunicação.

No entanto, vale destacar que a eficácia do controle penal nesse contexto se vê muitas vezes limitada, não apenas pelas particularidades intrínsecas do mundo virtual, mas também por barreiras legais e por haver uma limitada cooperação internacional. Haja vista que são crimes que abrangem uma ampla variedade de atividades ilegais e que apresentam complexidades únicas, dificultando a identificação e o controle penal desses crimes, tendo se mostrado um desafio complexo às autoridades, aos legisladores e à sociedade em geral.

Sabendo que o ponto mais frágil de todo sistema de proteção no ambiente da informática é o ser humano, de fato, resta o entendimento de que a maioria das invasões a dispositivos informáticos ocorre, direta ou indiretamente, por meio de ações humanas. Tal fato, se dá porque muitas pessoas acreditam que os mecanismos de segurança, em si, oferecem proteção suficiente, o que as leva a uma ilusão de segurança[59].

Outrossim, devido ao ritmo acelerado de vida da sociedade, acaba resultando em desgastes mentais e na carência de tempo por parte dos usuários, fazendo com que, muitas vezes, as decisões sejam tomadas de maneira precipitada, sem uma reflexão aprofundada, levando a respostas automáticas mesmo em questões

[59] MITNICK, Kevin D.; SIMON, William L. A arte de enganar. Tradução: Kátia Aparecida Roque. São Paulo: Pearson Education do Brasil, 2003, p. 15.

imprescindivelmente relevantes, as quais podem gerar inúmeros efeitos prejudiciais ao longo da vida.

Dessa forma, após uma análise profunda da conduta da vítima na era virtual, explorando abordagens funcionalistas, filosóficas e dogmáticas, o presente capítulo lança luz sobre os impactos significativos que surgem a partir da dissonância da vulnerabilidade da vítima no contexto da evolução normativa dos crimes cibernéticos, impactando a eficácia das leis e regulamentações relacionadas aos referidos crimes. Compreender os desafios resultantes da vulnerabilidade da vítima é essencial para a formulação de estratégias e políticas eficazes para a prevenção e combate a esses delitos no ambiente digital em constante mutação.

A natureza dinâmica e evolutiva dos crimes cibernéticos e a falta de conscientização das vítimas desses delitos representam um grande desafio para a aplicação da lei e dos sistemas judiciais. Para tal, resta imprescindível uma análise mais aprofundada acerca dos quesitos por ora citados. Sendo assim, este capítulo se propõe a analisar mais especificamente os crimes cibernéticos e as dificuldades inerentes à identificação e ao controle penal. Além disso, serão apresentadas possíveis soluções e estratégias para enfrentar esses desafios, visando contribuir para um entendimento aprofundado desse fenômeno e para o avanço nas estratégias de combate a esse tipo de crime que, infelizmente, se torna mais sofisticado e disseminado a cada dia.

3.1 Breve exposição do arcabouço normativo dos crimes cibernéticos

A crescente dependência da internet na sociedade moderna trouxera consigo um novo campo de desafios jurídicos: os crimes cibernéticos. Nesse contexto, é fundamental compreender o arcabouço normativo atual que rege as ações e consequências desses delitos no ambiente digital. Assim, este capítulo visa fornecer uma breve exposição do atual quadro legal que envolve os crimes cibernéticos, abordando as principais leis e regulamentações que buscam lidar com esses desafios, sendo fundamental para destacar as lacunas e desafios que ainda persistem no controle e na punição dessas práticas delitivas, lançando as bases para as discussões subsequentes neste trabalho.

Nessa perspectiva, *a posteriori*, procede-se à enumeração de uma série de ações praticadas no ambiente virtual que demandam reflexão quanto ao enquadramento atualmente previsto ou mesmo à necessidade (ou não) de criação de novas leis penais, à luz do princípio da intervenção mínima.

No âmbito da informática, observa-se que a evolução legislativa no Brasil ocorreu de forma bastante tardia, iniciando-se efetivamente em 2012, com a promulgação de leis novas leis criminais referentes à temática em questão, contrariando o princípio da subsidiariedade. A Lei nº 12.735/12, conhecida como "Lei Carolina Dieckmann", foi sancionada em 2012 recebendo esse nome devido a um ataque cibernético à atriz brasileira, Carolina Dieckmann. Nesse ataque, hackers tentaram extorquir R$ 10.000,00 da atriz para não divulgar fotos íntimas. No entanto, Carolina Dieckmann não cedeu às ameaças e acabou sendo exposta pelos criminosos.

De fato, a Lei Carolina Dieckmann representou um avanço significativo no contexto digital, mas ainda é considerada insuficiente do ponto de vista doutrinário majoritário, pois não aborda adequadamente a invasão de dispositivos eletrônicos. O ambiente digital apresenta uma série de desafios e riscos, e a exposição de dados pessoais pode ter consequências devastadoras.

Assim, mesmo diante de inúmeros casos de exposições desde então, ainda nos dias atuais vê-se em um descontrole nesse âmbito, tendo em vista, por exemplo, a facilidade com que informações bancárias do ex-presidente do Brasil, Jair Bolsonaro, foram compartilhadas e utilizadas para realizar compras fraudulentas, ilustrando ainda mais a vulnerabilidade das pessoas no mundo virtual[60]. Muitas vezes, esses ataques são perpetrados por grupos anônimos que atuam no ciberativismo, expondo informações sigilosas de indivíduos, a exemplo dos "*Anonymous*"[61], figurando o quão frágil é a proteção normativa no âmbito virtual, facilitando a atuação dos perpetradores.

A falta de regulamentação eficaz e a capacidade de operar de forma anônima tornam esses grupos difíceis de rastrear e prender, para tanto, é essencial que os

[60] G1. "Grupo de hackers vaza em rede social supostos dados pessoais de Bolsonaro, filhos e ministros". Disponível em: https://g1.globo.com/politica/noticia/2020/06/02/grupo-de-hackers-vaza-em-rede-social-supostos-dados-pessoais-de-bolsonaro-filhos-e-apoiadores.ghtml. Acesso em: 05 out. 2023.

[61] "O Grupo *Anonymous* foi criado em meados de 2003 e é um tipo de Comunidade virtual com o propósito de Ciberativismo e Vigilantismo na Internet". Disponível em: https://www.infoescola.com/atualidades/grupo-anonymous/. Acesso em: 05 out. 2023.

usuários estejam cientes dos perigos que enfrentam ao navegar na internet e tomem precauções, como evitar o compartilhamento de informações sensíveis. Por sua vez, voltando ao caráter normativo, a Lei Carolina Dieckmann carece de clareza em relação à invasão de dispositivos eletrônicos, abordando principalmente a invasão com intenções ilícitas diretas. Sendo aparente a necessidade de uma regulamentação mais abrangente para combater com eficácia os crimes cibernéticos.

Dando prosseguimento, outra norma que marcou um avanço ao ordenamento jurídico brasileiro foi o Marco Civil da Internet, Lei 12.965/2014 no Brasil, que representou um marco regulatório significativo na governança da internet, estabelecendo princípios, direitos e deveres que moldam a interação dos usuários e provedores do âmbito virtual.

Dentre os benefícios do Marco Civil, destaca-se a consolidação dos direitos fundamentais nessa esfera, sendo crucial ressaltar pilares como a proteção da privacidade do usuário, a garantia da liberdade de expressão e a asseguração da neutralidade da rede, visando impedir discriminações injustificadas e reforçando para que sejam estabelecidos limites bem definidos para a coleta e uso de dados pessoais por parte dos provedores.

Contudo, mesmo com seus avanços notáveis que representaram uma evolução na proteção dos direitos digitais, é imprescindível ressaltar que o Marco Civil não tem um enfoque penal, abordando apenas aspectos do direito cível e social. Para tanto, a eficácia dos princípios regulatórios fornecidos pela referida norma é desafiada por uma série de fatores hodiernamente, a exemplo do anonimato e do alcance global dos criminosos, da rápida evolução tecnológica, da falta de colaboração e compartilhamento de informações, dos recursos limitados e de uma complexidade tanto da jurisdição, como das próprias leis, que serão melhor delineados em tópico posterior.

Além disso, muitas atividades prejudiciais e ilícitas não foram contempladas pelos tipos penais estabelecidos, e tampouco o foram com a implementação da Lei n. 14.155/2021, que é a norma mais recente em vigência na seara penal. Tratando especificamente da referida lei, sancionada em 27 de maio de 2021, esta representou um marco significativo na resposta do Brasil à crescente onda de crimes cibernéticos, que ganhou força especialmente durante a pandemia. Antes dessa legislação, as penas eram consideradas ainda mais brandas e havia inúmeras dificuldades técnicas em enquadrar algumas situações, refletindo a necessidade premente de atualização

e aprimoramento do arcabouço legal para lidar com a complexidade e a gravidade dos crimes digitais.

A nova lei promoveu alterações substanciais, ampliando o escopo e a gravidade do tipo penal relacionado a crimes cibernéticos. Primeiramente, destaca-se que houve uma ampliação do tipo penal, com a modificação da redação dos *caput*s, visando abranger uma gama mais ampla de ações criminosas. Ademais, a lei aumentou de forma significativa as penas de base, refletindo a necessidade de endurecer as punições e desencorajar a prática desses crimes. Os limites máximos e mínimos de pena também foram elevados, demonstrando a intenção de conferir maior gravidade ao delito e estabelecer penas proporcionais. Adicionalmente, foram introduzidas algumas causas de aumento de pena com intuito de agravar a punição em situações com circunstâncias agravantes e intensificar esta repressão aos crimes cibernéticos.

Essas medidas, de fato, visaram fortalecer o combate à criminalidade digital e garantir a proteção da sociedade contra os potenciais danos advindos dessas práticas ilícitas. Sendo uma resposta legislativa significativa ao aumento alarmante dos crimes cibernéticos, ao fortalecer as penalidades e ampliando a incidência do tipo penal. Entretanto, os desafios não foram sanados, mostrando a premente necessidade de adaptações constantes das legislações e das estratégias de enfrentamento, o que é fundamental para manter a eficácia no combate à criminalidade cibernética. Para tanto, é essencial que essa legislação seja acompanhada por esforços contínuos na educação, conscientização e capacitação dos órgãos responsáveis pela aplicação da lei.

A análise comparativa das redações do dispositivo revela uma evolução significativa. A exemplo, o crime de invasão de dispositivo informático alheio, estabelecido pelo artigo 154-A do Código Penal brasileiro, emerge como uma conduta criminosa intrinsecamente vinculada ao universo digital, adquirindo uma crescente relevância diante do avanço tecnológico e da perversidade da informática em nosso cotidiano. A trajetória legislativa deste tipo penal, marcada pelas modificações promovidas pelas Leis 12.737/2012 e 14.155/2021, demonstra uma tentativa de adaptação e melhoria diante dos desafios impostos pelo ambiente digital.

A redação original, apresentada pela Lei 12.737/2012, definiu a invasão de dispositivo informático alheio como a violação indevida de mecanismo de segurança, com a intenção de obter, adulterar ou destruir dados ou informações sem a devida

autorização do titular do dispositivo. Esta infração era punida com detenção de três meses a um ano, além de multa.

Por outro lado, a Lei 14.155/2021 promoveu uma reformulação na redação, ampliando sua abrangência. Manteve-se a tipificação da invasão de dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o propósito de obter, adulterar ou destruir dados ou informações sem a permissão do usuário do dispositivo ou de instalar vulnerabilidades para alcançar vantagem ilícita. Embora o texto tenha se tornado mais conciso, a pena foi substancialmente aumentada, passando a ser reclusão de um a quatro anos, além de multa.

Este avanço na legislação reflete o início de uma compreensão da importância de proteger não apenas os titulares dos dispositivos, mas todos os usuários potencialmente afetados por tais invasões. O aumento da pena para reclusão denota uma resposta mais rigorosa do sistema penal, sinalizando a necessidade de dissuadir e coibir invasões de dispositivos informáticos. Essa alteração reflete a seriedade com que a sociedade e o legislador enfrentam os crimes cibernéticos.

A evolução da legislação relativa à invasão de dispositivo informático espelha uma maior compreensão dos desafios impostos pelo cenário digital e a busca por uma normatização mais eficaz. Contudo, a dinâmica do mundo digital requer uma constante atualização da legislação, aliada a uma abordagem multidisciplinar que incorpore aspectos técnicos, jurídicos e sociais. A proteção dos usuários e a segurança digital devem ser prioridades, com medidas que busquem equilibrar a inovação tecnológica com a garantia dos direitos individuais. Este é o desafio e a direção que a sociedade contemporânea deve trilhar para promover um ambiente digital seguro e ético.

Outro crime comumente visto no âmbito virtual e que foi acrescido por uma maior ênfase pela Lei 14.155/2021 foi o crime de perseguição, também conhecido como *stalking*, que se trata de uma conduta que tem se tornado cada vez mais frequente na era digital, impulsionado pelo uso generalizado das tecnologias de informação e comunicação. Essa forma de violência, agora devidamente tipificada no Código Penal brasileiro pelo artigo 147-A, reflete um avanço na legislação ao reconhecer e punir a perseguição persistente que ocorre em ambientes virtuais, conhecida como *cyberstalking*.

O *cyberstalking* é uma manifestação moderna e insidiosa de perseguição, caracterizada pela repetição de comportamentos intimidadores e ameaçadores por

meio de recursos digitais, tais como redes sociais, e-mails, mensagens instantâneas e outros meios eletrônicos. Essa prática pode ter consequências devastadoras para as vítimas, afetando não apenas sua integridade psicológica, mas também sua vida cotidiana e sensação de segurança.

A inclusão do artigo 147-A no Código Penal representou um passo significativo na proteção das vítimas de perseguição digital, oferecendo uma definição clara do crime, abrangendo ações que ameaçam a integridade física ou psicológica da pessoa, restringindo sua liberdade de locomoção ou invadindo sua privacidade. Ao estabelecer penas de reclusão e multa, a legislação busca desencorajar e punir de forma eficaz os perpetradores desse tipo de violência, ainda que tais medidas sejam ainda insuficientes.

No entanto, é fundamental reconhecer que o desafio de enfrentar o *cyberstalking* vai além da legislação. A conscientização da sociedade sobre os impactos negativos dessa prática é crucial, mostrando o quão necessário é educar as pessoas sobre a seriedade do problema, seus efeitos devastadores na saúde mental das vítimas e a importância de denunciar tais situações.

Além disso, demonstra-se como essencial que as autoridades estejam preparadas para investigar e combater os casos de *cyberstalking* de maneira eficaz, garantindo que as vítimas recebam o apoio necessário e que os perpetradores sejam devidamente responsabilizados perante a lei. Para tanto, a colaboração entre diferentes instituições, como polícia, justiça, organizações da sociedade civil e provedores de serviços online, é um importante ponto para enfrentar esse desafio de forma mais abrangente.

O avanço tecnológico continuará a moldar a natureza dos crimes e, consequentemente, a legislação precisa se manter dinâmica e adaptável. O *cyberstalking* é um exemplo de como a sociedade está enfrentando novas formas de perseguição, e a tipificação desse crime no Código Penal é um passo importante para garantir que as vítimas recebam a proteção e a justiça que merecem. A evolução da legislação deve ser acompanhada de uma abordagem educacional e de aplicação coerente da lei para criar um ambiente digital mais seguro e consciente.

Outrossim, insta salientar que, embora essa transição legislativa represente um avanço nos parâmetros normativos, ainda não são suficientes para erradicar de maneira considerável o ciclo da violência nesse âmbito. A reclassificação de algumas contravenções penais em crimes, por exemplo, é apenas um dos muitos passos

necessários para combater a criminalidade de maneira eficaz. A efetividade das leis está intrinsecamente ligada à sua aplicação eficiente, à capacidade de investigação e ao sistema prisional.

Observa-se uma tendência de progresso no campo jurídico, com a busca por melhores formas de lidar com a criminalidade e minimizar seus impactos. Novas leis, políticas e abordagens estão sendo constantemente estudadas e implementadas para adaptar-se às mudanças sociais e tecnológicas que influenciam diretamente os padrões de criminalidade.

É crucial reconhecer que, com o avanço tecnológico, novas formas de crimes emergem, exigindo uma abordagem legal e penal atualizada e condizente com a realidade contemporânea. Nessa perspectiva, os crimes cibernéticos representam uma fronteira desenfreada que demanda de uma atenção especial das autoridades e da legislação, uma vez que muitos desses crimes não são contemplados de forma mais abrangente nos códigos penais tradicionais.

Nesse contexto, para entender essa premente necessidade de atualização de uma constante e adaptativa atualização normativa, é fundamental um aprofundamento no que diz respeito a um melhor entendimento das motivações que impulsionam esses indivíduos a adentrarem no mundo do cibercrime. Investigar suas raízes psicológicas e sociais pode lançar luz sobre estratégias de prevenção e combate a essas práticas. Além disso, promover iniciativas educacionais que direcionam a curiosidade de maneira ética e construtiva pode representar um caminho para desviar esses potenciais habilidades prejudiciais para atividades legítimas e benéficas à sociedade.

3.2 Desafios acerca do controle penal e da identificação dos crimes cibernéticos

O panorama dos crimes cibernéticos no Brasil é permeado por diversas incógnitas que refletem a complexidade desse ambiente digital, se tornando um tema bastante desafiador na sociedade vigente. Como visto, o rápido avanço da tecnologia e a crescente dependência da sociedade em sistemas digitais desencadeou no fato de que estes crimes têm se tornado cada vez mais frequentes e sofisticados.

No âmbito da motivação, observa-se a presença de indivíduos altamente habilidosos tecnicamente, dotados de mentes aguçadas que utilizam a tecnologia para perpetrar danos e prejuízos às outras pessoas. Esses indivíduos, muitas vezes,

permanecem ocultos dentro do vasto ciberespaço, engajados em atividades ilícitas ainda não plenamente reveladas.

É notável a existência de uma subcultura dentro desse universo digital, composta por aqueles que possuem uma afinidade especial com a tecnologia e suas nuances. Alguns desses indivíduos investem tempo e esforço em aprimorar suas habilidades, buscando, muitas vezes, cursos e materiais que os auxiliem a aprofundar seus conhecimentos na arte do cibercrime. Surpreendentemente, há até mesmo uma tendência de alguns deles compartilharem esse conhecimento, ministrando cursos e disseminando técnicas de roubo e invasão, fomentando uma cultura de delinquência digital.

A motivação subjacente a esse comportamento muitas vezes é enraizada na curiosidade e no desejo de desvendar o desconhecido. Muitos indivíduos são atraídos por desafios intelectuais e técnicos oferecidos pelo mundo digital, buscando compreender e explorar a extensão das capacidades da tecnologia. Essa curiosidade pode se manifestar na busca por novas técnicas para violar a privacidade alheia, como acessar dados armazenados, interceptar comunicações e explorar vulnerabilidades em sistemas e redes.

Tal problemática tem se intensificado bastante nos últimos anos, sendo resultante da existência de diversos fatores que são discorridos ao longo da presente pesquisa, os quais, contribuem diretamente para essa expansão dos crimes cibernéticos. Assim, acaba tornando esse tipo de crime em um desafio complexo para governos, empresas, especialistas em segurança e, principalmente, para os internautas leigos na temática. Tendo em vista que esses crimes englobam uma gama de atividades ilícitas, como roubo de informações pessoais, fraudes financeiras, ataques a infraestruturas críticas e disseminação de conteúdos maliciosos.

É essencial reconhecer que, mesmo que o Estado empregue recursos consideráveis para retirar delinquentes das ruas, isso teria pouco efeito se houvesse indivíduos que continuassem provocando e incentivando a conduta delinquente de outras pessoas.

Nesse viés, vale considerar que um dos principais fatores que desencadeiam essa situação é o anonimato e o alcance global dos criminosos cibernéticos. Os quais, têm a capacidade de operar de forma completamente anônima, utilizando técnicas como o uso de redes privadas virtuais (VPNs) e serviços de ocultação de identidade,

habilidades essas que intensificam a permanência do anonimato e dificulta a identificação e a captura dos criminosos.

Além disso, a natureza da internet permite que estes perpetradores ataquem vítimas em qualquer parte do mundo, tornando a coordenação entre diferentes jurisdições um desafio complexo. Ao mesmo ponto em que a legislação, embora preveja a retenção de logs por parte dos provedores, esbarra em limitações temporais e na utilização de ferramentas avançadas de ocultação de identidade pelos criminosos, resultando assim numa dificuldade substancial na identificação e na responsabilização desses agentes, comprometendo a capacidade de combate aos delitos virtuais.

Outro fator primordial a ser ressaltado é a rápida evolução tecnológica ao redor do mundo, como fora muito debatido anteriormente, essas inovações transformaram a maneira como vivemos, trabalhamos e nos relacionamos, havendo cada vez mais peculiaridades disponíveis com facilidade para qualquer explorador desse ramo, fazendo com que o mundo virtual tenha se tornado uma parte significativa da vida cotidiana das pessoas.

De maneira que, na medida em que a tecnologia avança, consequentemente novas vulnerabilidades são descobertas e exploradas pelos criminosos cibernéticos. Eles se adaptam rapidamente às medidas de segurança existentes, criando técnicas cada vez mais sofisticadas para burlar sistemas de proteção. Tal situação exige que as agências de aplicação da lei estejam constantemente atualizadas e adquiram conhecimentos especializados para enfrentar os desafios em constante evolução, o que é difícil, considerando a celeridade da situação.

Os crimes cibernéticos apresentam uma complexidade ímpar, seja pela diversidade de modalidades existentes, seja pela velocidade com que podem ser executados. A ação dos criminosos no mundo virtual ultrapassa qualquer fronteira, desafiando as limitações geográficas tradicionais, o que complica a cooperação internacional e a aplicação uniforme da lei. A criptografia e a utilização de redes anônimas dificultam ainda mais a identificação dos perpetradores desses crimes. Restando nítido que os criminosos, as vítimas e a infraestrutura técnica abrangem múltiplas jurisdições, trazendo muitos desafios às investigações e ações penais[62].

[62] INTERPOL. *Op. Cit*. Cybercrime. Disponível em: https://www.interpol.int/Crimes/Cybercrime. Acesso em: 15 ago. 2023

A falta de colaboração e compartilhamento de informações também é um obstáculo significativo no combate aos crimes cibernéticos. O enfrentamento desse problema requer uma cooperação estreita entre governos, setor privado, organizações internacionais e especialistas em segurança. No entanto, muitas vezes há uma certa relutância em compartilhar informações sensíveis devido a preocupações com privacidade e segurança nacional. Essa falta de colaboração dificulta ainda mais a identificação e a prisão dos criminosos, uma vez que as informações necessárias podem não ser compartilhadas de forma efetiva.

Outrossim, pode se dizer que os recursos destinados ao combate aos crimes cibernéticos são ainda muito limitados, algo que também contribui consideravelmente com essa vigente problemática. Essa luta exige recursos significativos, incluindo pessoas altamente treinadas, disponibilização de tecnologias avançadas e de um maior investimento em pesquisa e em desenvolvimento. Infelizmente, muitas agências governamentais e empresas não possuem os recursos adequados para lidar efetivamente com esses crimes, sendo assim, são resultantes lacunas na capacidade de detecção, prevenção e resposta a incidentes desse tipo.

A escassez de normas específicas no contexto do Direito Digital é um desafio considerável que permeia o desenvolvimento e a aplicação efetiva da legislação no universo virtual. Ao comparar com outros ramos do Direito, observamos uma disparidade evidente em relação à quantidade e à precisão das normas que regem as atividades digitais.

A existência de um número limitado de regulamentações específicas no âmbito do Direito Digital é um reflexo da velocidade exponencial com que as tecnologias avançam, superando a capacidade do legislativo de acompanhar e regular adequadamente todas as novas dinâmicas que surgem no mundo virtual. Por consequência, o Direito Digital frequentemente se depara com um descompasso entre a inovação tecnológica e a capacidade do sistema legal de fornecer uma resposta normativa.

Essa falta de leis específicas cria um cenário onde a orientação da conduta no ambiente digital muitas vezes depende da interpretação jurisprudencial. As decisões dos tribunais tornam-se uma referência vital para compreender os modelos de comportamento aceitáveis e os limites das atividades virtuais. Os casos judiciais anteriores servem como precedentes importantes, ajudando a determinar quais normas são aplicáveis e como interpretá-las em contextos digitais.

Nesse sentido, a jurisprudência assume um papel de destaque, preenchendo as lacunas normativas e fornecendo diretrizes para advogados, empresas, usuários e demais envolvidos no universo digital. No entanto, essa dependência da jurisprudência para a orientação normativa também pode gerar incertezas e inconsistências, uma vez que as interpretações podem variar entre diferentes tribunais e casos.

Para superar essa escassez de normas e proporcionar maior segurança jurídica, é essencial que o legislador acompanhe de perto as transformações tecnológicas, antecipando e promovendo uma regulamentação ágil e específica para o ambiente digital. A colaboração entre especialistas em tecnologia e juristas torna-se fundamental para criar regulamentações que reflitam a realidade digital de maneira precisa e atenda às necessidades da sociedade.

Além disso, a complexidade da jurisdição também representa um desafio significativo a ser amparado. Os crimes cibernéticos muitas vezes transcendem fronteiras, o que levanta questões complexas acerca da jurisdição, tendo em vista que as leis que dizem respeito aos crimes cibernéticos podem variar de um país para outro, dificultando a cooperação entre as autoridades e a persecução dos infratores.

Insta salientar, dessarte, a imprescindível importância que se deve dar ao cumprimento das colaborações entre as jurisdições transnacionais, já que a natureza global da internet impõe desafios extras às autoridades brasileiras na persecução de criminosos que operam em territórios estrangeiros. A cooperação internacional se torna crucial, mas a falta de padrões globais e a divergência nas legislações dificultam a eficácia das ações conjuntas.

O Direito, por natureza, é de uma área tradicionalista e resistente a mudanças abruptas, o que gera desafios consideráveis ao tentar incorporar as novas realidades virtuais e tecnológicas. O enfrentamento dessa resistência filosófica é crucial para garantir que a regulamentação seja eficaz, justa e pertinente ao contexto atual, tendo em vista que a legislação hodierna muitas vezes não acompanha adequadamente os avanços tecnológicos, deixando brechas legais que acabam dando margem para que os criminosos acabem explorando.

Nesse contexto, fazendo uma conexão com o relevante papel vítima na política criminal, é possível considerar as atitudes anteriormente expostas ao longo do presente estudo como potencial incentivadora da dificuldade do controle penal

informático, por tamanha falta de cuidado, de conscientização ou de compreensão de grande parte dos envolvidos.

A transformação da sociedade com base nas ideias desenvolvimentistas trazidas pela tecnologia da informação, aliada à crescente dependência da automatização e à velocidade dos avanços tecnológicos, introduziu um novo conjunto de riscos, bens jurídicos, valores individuais e comportamentos. No entanto, o convívio nesse novo ambiente digital trouxe consigo novas obrigações, a necessidade de um cuidado aprimorado e precauções adicionais. Dado que o ciberespaço é um ambiente novo, amplo e amplamente utilizado para a evolução e interação humanas, compreender esse ambiente e agir com a devida cautela tornou-se imperativo.[63]

O anonimato do ciberespaço, a sensação de agir sem restrições e o isolamento em relação ao mundo físico deixam os usuários em uma situação de vulnerabilidade dupla. De um lado, o ambiente aparenta favorecer a liberdade sobre as normas legais, atraindo indivíduos para a prática de atos ilícitos. Por outro lado, o ciberespaço os torna suscetíveis a acreditar nas informações que encontram e nas promessas que lhes são feitas. Portanto, mostra-se essencial a abordagem tida nesta pesquisa a essa complexa dinâmica de riscos e comportamentos no ambiente cibernético.[64]

Essas lacunas jurídicas, ambiguidades e inconsistências na aplicação das leis, acabam resultando em situações em que as condutas virtuais não são adequadamente regulamentadas ou punidas. Portanto, urge a necessidade de uma legislação atualizada, dinâmica e flexível, capaz de abordar essas peculiaridades e desafios, proporcionando orientações claras e eficazes para os cidadãos e as organizações que atuam no mundo digital.

Assim sendo, em suma, a dificuldade em combater os crimes cibernéticos decorre de uma combinação de fatores, incluindo o anonimato e o alcance global dos criminosos, a rápida evolução tecnológica, a falta de colaboração (principalmente das próprias vítimas) e do irresponsável compartilhamento de informações, assim como os recursos limitados e a complexidade da jurisdição e das leis. Para tanto, resta imprescindível uma análise abrangente das medidas de prevenção e combate aos crimes cibernéticos, considerando estratégias técnicas, legais e políticas, bem como a importância de uma abordagem multidisciplinar na resposta a essas ameaças.

---

[63] SYDOW, Spencer Toth. *Op. Cit*. Nota 34.
[64] SYDOW, Spencer Toth. *Op. Cit*. Nota 34.

3.3 Medidas de prevenção e combate aos crimes cibernéticos

O cenário dos crimes cibernéticos no Brasil é vasto e complexo, refletindo a interseção da tecnologia digital com questões sociais, econômicas e culturais que permeiam todo parâmetro da sociedade. Haja vista que as barreiras digitais praticamente desapareceram, fazendo com que esses crimes representam uma realidade contemporânea intrínseca à sociedade virtual em que vivemos.

Para entender a extensão desses crimes, é fundamental considerar o comportamento dos usuários em relação às medidas de segurança digital, diante de todo o exposto ao longo dessa pesquisa no que concerne ao relevante papel da vítima. A falta de atenção e a negligência no que diz respeito à proteção dos dispositivos são fatores primordiais que propiciam a ocorrência desses delitos. Muitos indivíduos não adotam as devidas precauções, subestimando a sofisticação e a frequência dos ataques cibernéticos.

A proteção eficaz contra os crimes digitais requer uma abordagem multifacetada. Primeiramente, é essencial priorizar a segurança dos sistemas e dispositivos, implementando medidas de proteção, como firewalls, antivírus atualizados e políticas de segurança robustas. Além disso, a conscientização dos usuários sobre a importância de práticas seguras, como a utilização de senhas fortes e únicas, não compartilhar informações pessoais sensíveis online e adotar a autenticação de dois fatores, é crucial.

A autenticação de dois fatores é uma das medidas mais eficazes para mitigar riscos de invasões e ataques. A utilização de verificação por SMS, e-mail ou aplicativos de autenticação oferece uma camada adicional de segurança, dificultando significativamente o acesso não autorizado às contas. Ao implementar essa autenticação, os usuários criam uma barreira extra para os hackers, aumentando a segurança de suas informações e dados.

É importante destacar que os crimes digitais próprios estão em constante evolução, acompanhando o avanço tecnológico e se adaptando às contramedidas de segurança. Portanto, é fundamental que os usuários estejam sempre atualizados sobre as melhores práticas de segurança digital e estejam dispostos a se adaptar a novas tecnologias e técnicas de proteção.

Diante desse contexto, a compreensão aprofundada dos crimes digitais próprios e das medidas de prevenção torna-se essencial para a construção de uma

sociedade digital mais segura e resiliente. A educação e a conscientização continuada dos usuários são elementos-chave na mitigação dos impactos desses crimes e na promoção de uma utilização responsável e segura da tecnologia.

A FBI, principal agência federal na investigação de ataques e invasões cibernéticas dos Estados Unidos, elenca dicas essenciais de segurança cibernética[65], em meio a um quadro de carência de segurança virtual que requer uma abordagem abrangente e atenta, que serão delineadas abaixo.

Primeiramente, a agência trata que é imperativo manter os sistemas e software atualizados, bem como instalar um programa antivírus robusto e confiável, pois estes atuam como defesas essenciais contra ameaças cibernéticas. Além disso, ao se conectar a uma rede Wi-Fi pública, precaução é fundamental, evitando transações confidenciais, como compras online, para mitigar o risco de exposição a possíveis violações de privacidade. A criação de senhas robustas e únicas para cada conta online, com alterações periódicas, representa uma medida vital, fortalecendo a segurança dos acessos também é estritamente importante. Complementarmente, é essencial implementar a autenticação multifator em suas aplicações sempre que possível, elevando a barreira de segurança. Ademais, a prudência ao examinar o endereço de e-mail em correspondências e verificar os URLs antes de interagir com mensagens ou sites é um procedimento recomendado para evitar cair em armadilhas. Aconselha-se veementemente não clicar em links de e-mails ou mensagens não solicitadas.

Como também, o veículo informativo da FBI[66] designa que a divulgação cuidadosa de informações pessoais em perfis online e redes sociais é crucial, pois dados como nomes de animais de estimação, instituições educacionais e familiares podem ser utilizados por agentes mal-intencionados para acessar contas privadas. Vale salientar também que é importante evitar realizar pagamentos a pessoas ou organizações desconhecidas que buscam apoio monetário e exigem ação imediata, é um princípio de precaução que resguarda contra possíveis fraudes financeiras. Estas orientações compõem uma estratégia abrangente para a segurança digital, preservando a integridade e privacidade dos usuários.

---

[65] FBI - Federal Bureau of Investigation. Cyber Crime. Disponível em: https://www.fbi.gov/investigate/cyber. Acesso em: 29 de setembro de 2023.
[66] FBI – Federal Bureau of Investigation. *Op. Cit.* Nota 65.

As recomendações apresentadas pelo renomado órgão são de extrema importância para mitigar os riscos dos crimes cibernéticos e proteger os usuários no ambiente virtual. A segurança digital é um tema vital nos dias atuais, dada a crescente sofisticação dos cibercriminosos e a expansão constante das tecnologias digitais. No entanto, tão crucial quanto implementar medidas de segurança é compreender a importância da conscientização e entendimento por parte da vítima nesse cenário.

Manter sistemas e software atualizados e utilizar um programa antivírus forte são alicerces da segurança digital. A atualização constante de sistemas operacionais e aplicativos é essencial para corrigir falhas de segurança conhecidas. Da mesma forma, um antivírus confiável é uma barreira eficaz contra malware e outras ameaças. No entanto, compreender por que essas atualizações são necessárias e como funcionam é crucial para garantir que os usuários sigam essas práticas de maneira diligente.

A precaução ao utilizar redes Wi-Fi públicas é uma recomendação fundamental. Compreender os riscos associados à transmissão de dados em redes não seguras ajuda a evitar a exposição de informações confidenciais. É vital que os usuários compreendam o potencial de interceptação de dados em redes públicas e os perigos que isso representa para a segurança.

A criação de senhas fortes e exclusivas, juntamente com a implementação de autenticação multifator, é outro pilar essencial da segurança digital. No entanto, a compreensão de como essas práticas protegem as contas e dados pessoais é crucial para motivar os usuários a adotá-las como parte de sua rotina de segurança.

A atenção aos detalhes, como examinar URLs e endereços de e-mail, é uma habilidade importante que, quando desenvolvida, ajuda os usuários a identificar possíveis ameaças. Saber reconhecer e-mails ou mensagens suspeitas pode evitar a queda em armadilhas cibernéticas.

É imperativo que os usuários compreendam a necessidade de limitar as informações compartilhadas em perfis online e contas de redes sociais. A conscientização sobre como os cibercriminosos usam informações pessoais para ataques de engenharia social é crucial para a segurança nesse contexto.

Por fim, o entendimento de que não se deve enviar pagamentos a fontes desconhecidas é uma salvaguarda contra golpes financeiros. Compreender os riscos associados a transações com desconhecidos pode evitar perdas financeiras e proteger a vítima de atividades fraudulentas.

Assim, a compreensão e o entendimento das medidas de segurança digital são cruciais para garantir que os usuários as sigam de forma eficaz. Conscientizar as pessoas sobre os riscos, as técnicas e os princípios subjacentes à segurança digital são um passo essencial para criar uma sociedade online mais segura e resiliente contra os desafios dos crimes cibernéticos.

Não obstante, diante da complexidade e evolução constante dos crimes cibernéticos, só resta nítida a importância de compreender continuadamente esses desafios circundam a atual realidade, sendo essencial para desenvolver estratégias eficazes de prevenção, investigação e repressão, bem como garantir a proteção das vítimas e a segurança da sociedade em um cenário virtual cada vez mais interconectado.

Sendo assim, pode se afirmar ainda que para enfrentar esse desafio de forma eficaz, é crucial ressaltar também a necessidade uma abordagem multidisciplinar que envolva a cooperação entre governos, empresas, organizações internacionais e especialistas em segurança, haja vista que uma estreita colaboração entre parceiros públicos e privados é imprescindível para um devido enfrentamento.

Insta salientar que as cooperações internacionais são facilitadas por tratados e acordos bilaterais ou multilaterais que estabelecem os termos e condições para a troca de informações e evidências entre países. Para tanto, esses acordos frequentemente delineiam procedimentos para solicitar e executar cartas rogatórias[67], as quais, no contexto específico de crimes cibernéticos, se acionadas de maneira célere, podem ser essenciais para uma variedade de propósitos, incluindo a obtenção de registros de provedores de serviços online, a busca e apreensão de evidências digitais e a solicitação de depoimentos de testemunhas. A cooperação efetiva nesses casos é essencial para a investigação e persecução de criminosos cibernéticos, garantindo que a justiça seja feita e buscando superar cada vez mais as barreiras jurisdicionais, na busca por garantir que os perpetradores sejam responsabilizados.

A efeito exemplificativo, a INTERPOL, com o seu alcance global, desempenha um papel vital na construção de parcerias intersetoriais e na promoção da cooperação internacional na aplicação da lei. Através de operações coordenadas, a referida Organização Internacional de Polícia Criminal tem capacidade de mobilizar recursos

[67] Uma carta rogatória é um instrumento jurídico por meio do qual um tribunal de um país solicita a assistência de um tribunal em outro país.

e experiências de diferentes países para enfrentar ameaças cibernéticas específicas[68]. Essa coordenação eficaz busca possibilitar a troca de informações, o monitoramento de atividades suspeitas e a colaboração em investigações em âmbito internacional, o que deve ser um caminho cada vez mais estreito entre os países afetados.

Além disso, a INTERPOL oferece plataformas seguras para a partilha de dados, análise e formação[69]. Essas plataformas são essenciais para facilitar a colaboração entre os países membros, permitindo a troca rápida e segura de informações relevantes sobre ameaças cibernéticas, padrões de ataque e técnicas de combate. Ao proporcionar treinamento e capacitação especializada, há uma contribuição para o desenvolvimento de competências necessárias para a prevenção, detecção, investigação e desmantelamento eficazes dos crimes cibernéticos.

Através de iniciativas como essa de cooperação internacional fomentada pela INTERPOL, intenciona-se que os países sejam capacitados para enfrentar as ameaças cibernéticas de maneira mais eficiente[70]. Resultando assim, numa contínua busca de proteção das comunidades contra os danos causados pelos crimes cibernéticos e contribui para uma almejada segurança do mundo virtual. Portanto, o importante papel central desempenhado pela organização, na busca de facilitar essa colaboração e impulsionar a capacidade dos países membros para combater os crimes cibernéticos, deveria ser algo devidamente tratado na política criminal brasileira, principalmente no que concerne à criação de normas mais específicas.

Pois, vê-se uma tamanha necessidade de atualização e de fortalecimento das leis referentes aos crimes no ambiente virtual, assim como, de investimentos contínuos em recursos, para acompanhar o cenário em constante evolução dos crimes cibernéticos. Buscando assim, que haja regulamentações mais direcionadas no que diz respeito à segurança cibernética, para facilitar o compartilhamento de informações e promover a cooperação global para enfrentar efetivamente essa ameaça em constante evolução.

Essas adaptações não se limitam apenas a situações isoladas. Elas refletem a necessidade contínua de reavaliar e modernizar o arcabouço legal em face das transformações tecnológicas. O direito digital requer um profundo entendimento do

[68] INTERPOL. *Op. Cit.* Nota 62.
[69] INTERPOL. *Op. Cit.* Nota 62.
[70] INTERPOL, *Op. Cit,* Nota 62.

conjunto de leis existentes e uma habilidade especial para integrar conceitos complexos da tecnologia da informação às estruturas jurídicas tradicionais.

É evidente que a legislação brasileira tem se mostrado lenta em se adaptar a essas transformações. A natureza dinâmica e complexa da criminalidade no âmbito virtual requer uma abordagem legislativa que esteja em consonância com a rápida evolução das tecnologias e dos métodos dos criminosos virtuais, sendo imprescindível que o legislador esteja atento às mudanças e tendências na sociedade, bem como às novas técnicas e táticas dos hackers e criminosos digitais.

Uma solução viável seria a criação de um departamento específico dentro do congresso brasileiro voltado para o acompanhamento e análise das tendências e práticas relacionadas aos crimes cibernéticos[71]. Esse departamento poderia ser responsável por monitorar o cenário da segurança cibernética, coletar informações sobre os mais recentes incidentes e ameaças, bem como propor atualizações legislativas necessárias para combater os crimes cibernéticos de forma eficaz.

Essas atualizações podem envolver a modificação das leis existentes para refletir os desafios e nuances específicos dos crimes cibernéticos ou, em alguns casos, a criação de normas totalmente novas e específicas para enfrentar as complexidades do mundo digital. A rigidez e a clareza das leis são fundamentais para garantir que os criminosos enfrentem consequências significativas por suas ações, proporcionando um elemento dissuasório.

Além da criação de normas mais rígidas, é crucial que o legislador promova uma maior conscientização e educação sobre segurança cibernética na sociedade em geral. Isso pode ser feito por meio de campanhas de conscientização, programas educacionais e iniciativas que visem a aumentar o entendimento da população sobre os riscos e as melhores práticas de segurança na internet.

Assim sendo, para que o direito cibernético seja eficaz e equitativo, é fundamental que os profissionais jurídicos se mantenham atualizados e estejam abertos a aprender e adaptar-se a esse novo paradigma. A interdisciplinaridade entre o direito e a tecnologia se torna cada vez mais relevante, exigindo uma colaboração

[71] CASTRO, Thainer Cordeiro de. Crimes Virtuais: crimes cibernéticos e as considerações sobre a criminalidade na internet Conteúdo Jurídico. Brasília-DF: 03 jun 2022. Disponível em: https://conteudojuridico.com.br/consulta/artigos/58585/crimes-virtuais-crimes-cibernticos-e-as-consideraes-sobre-a-criminalidade-na-internet. Acesso em: 12 jul. 2023.

estreita entre advogados, legisladores, tecnólogos e a sociedade em geral para criar regulamentações que atendam às demandas de um mundo cada vez mais digital.

Nesse viés, resta imperativa a interação entre o Direito e a sociedade virtual, destacando a discrepância entre a dinâmica dos fatos sociais e a natureza conservadora do Direito, que frequentemente não consegue abarcar a complexidade das relações sociais. É crucial, portanto, que o Direito se adapte à evolução da sociedade, seja por meio de reformas legislativas ou interpretação judicial jurisprudencial, mas sempre fundamentado nos princípios da democracia e no respeito à dignidade humana. De maneira que essa adaptação esteja alinhada com o modelo atual de sociedade da informação, no qual estamos inseridos muitas vezes de forma quase imperceptível. A sintonia entre o Direito e a sociedade nesse contexto é essencial para garantir a efetividade do sistema jurídico e a proteção dos direitos individuais.

Destarte, através deste trabalho, que atravessa diversos domínios do conhecimento, almeja-se enriquecer a análise crítica e aprofundar a compreensão a respeito dos crimes cibernéticos e suas consequências para as vítimas e para a sociedade. Nesse processo, foram exploradas as complexidades dessas questões, com o intuito de melhor compreender os desafios enfrentados e, assim, fornecer uma base sólida e eficaz para aprimorar as respostas do sistema jurídico em relação aos crimes cibernéticos. Concluindo, em última análise, que a busca pelo equilíbrio entre inovação, proteção dos direitos e de uma efetiva justiça constitui um desafio essencial para a contemporaneidade.

CONSIDERAÇÕES FINAIS

O primeiro capítulo aborda a evolução do mundo virtual desde seu surgimento, relacionando-a ao avanço tecnológico e à criação dos primeiros computadores programáveis. Destaca-se a importância da Internet nesse ambiente complexo, especialmente durante a pandemia de COVID-19, evidenciando sua relevância para a comunicação e continuidade das atividades cotidianas. Sendo ressaltado que o mundo digital está cada vez mais integrado à sociedade contemporânea, exigindo um conhecimento prévio para lidar com suas inovações e complexidades.

Além disso, a interação entre o mundo virtual e a autonomia individual é explorada, analisando como a presença e atividade nesse ambiente podem tanto fortalecer quanto minar a autonomia das pessoas. O consentimento é destacado como um elemento crucial para o exercício da autonomia, especialmente no contexto tecnológico. Contudo, é reconhecido que a dependência crescente da sociedade no mundo virtual traz desafios e riscos, especialmente em relação aos crimes cibernéticos, que afetam significativamente a segurança e o bem-estar das vítimas. São apresentados desafios relacionados à identificação e prevenção desses crimes, bem como o aumento da vulnerabilidade das pessoas nesse universo, sublinhando a necessidade de uma análise mais aprofundada da conduta das vítimas diante desses delitos.

Outrossim, o tópico subsequente focaliza-se na importância da teoria da vitimodogmática - ressaltando seu papel na valorização da vítima no processo penal - para compreender os crimes cibernéticos e fortalecer a doutrina penal, encerrando a discussão sobre a complexa questão da vulnerabilidade das vítimas de crimes cibernéticos. As vítimas, muitas vezes desprovidas de compreensão sobre o ambiente digital e suas intricadas nuances, necessitam de uma abordagem que as integre ativamente no processo penal, reconhecendo seus direitos e necessidades.

Concluindo assim que é imprescindível a compreensão dessa interação complexa do desenvolvimento tecnológico em meio à autonomia individual na contemporaneidade. A relevância deste tema se baseia, sobretudo, na disseminação crescente dos crimes cibernéticos, que ocorreu em paralelo com o significativo avanço da tecnologia, conforme discutido anteriormente, destacando a importância de os usuários assumirem um papel central e independente nesse contexto. Notando, portanto, o relevante papel da vitimodogmática, que surge como uma ferramenta

fundamental na análise presente nesse estudo para compreender a da dinâmica da vítima nos crimes cibernéticos e promover o desenvolvimento individual, reconhecendo o impacto na autonomia das vítimas.

Ato contínuo, no segundo capítulo explorou-se o complexo universo digital contemporâneo e sua influência nas interações e desenvolvimento de indivíduos e organizações. Diante dessa expansão, surge a intrincada questão do conhecimento do risco, desafiando a compreensão humana das ameaças digitais. O capítulo propôs adentrar a respeito dessa incerteza, examinando os fundamentos que cercam a consciência dos riscos digitais e a dinâmica do conhecimento.

Foram apresentadas reflexões acerca do risco sob a ótica das teorias de Claus Roxin, adaptando-as às particularidades do ambiente digital em constante evolução. Tendo foco na responsabilidade da vítima diante das ameaças cibernéticas, destacando-se a autocolocação e a heterocolocação da vítima em situação de risco e suas relações com a problemática atual. A teoria de Roxin sobre a imputação objetiva também foi abordada, ressaltando sua relevância na análise da conduta da vítima e do agente no mundo virtual.

Ademais, decorreram perspectivas filosóficas contemporâneas sob a ótica de renomados nomes como de Zygmunt Bauman, Pierre Lévy e Andy Clark, fazendo uma conexão dos olhares e teorias desses filósofos com essa temática desafiadora e complexa que é o conhecimento do risco no mundo digital, influenciando a consciência e a culpabilidade dos indivíduos. Reflexões essas que proporcionam insights cruciais sobre a relação entre as ações da vítima e sua vulnerabilidade ao risco digital.

Como também, é abordado a respeito da vulnerabilidade das vítimas de crimes cibernéticos, destacando a necessidade de conscientização e educação em segurança cibernética. Explorando, desse modo, a necessidade de considerar a participação e a influência da vítima no contexto do delito, buscando uma justiça mais contextualizada e humanizada. Além disso, é enfatizada a influência da vítima na consumação do crime, aprimorando a compreensão das dinâmicas criminais e abordando a relevância de reconhecer a conduta da vítima como parte da análise do crime.

Conclui-se, dessa forma, enfatizando a importância da educação em massa dos usuários sobre os riscos cibernéticos e a necessidade de uma interação equilibrada entre os mundos virtual e real. Partindo para uma perspectiva em que reconheça o devido papel da vítima no crime cibernético e é essencial para uma justiça

mais contextualizada, que incorpore devidamente o papel da vítima na análise do crime e amplie a compreensão das dinâmicas envolvidas e fortalecendo a proteção dos bens jurídicos. Afinal, observou-se que o escopo principal deste estudo foi fornecer uma compreensão mais aprofundada e contextualizada da função da vítima nos crimes cibernéticos, enriquecendo o embasamento teórico, com o intuito de melhor preparar-se para os desafios intrínsecos a este campo jurídico dinâmico e complexo, já que se trata de um ponto que ainda se encontra em dissonância com o nítido ineficaz controle penal desses crimes.

No terceiro capítulo do presente trabalho, foram analisados os crimes cibernéticos, ressaltando o impacto da tecnologia na vida contemporânea e focando no consequente impacto proveniente da vulnerabilidade dos usuários em desacordo com a ainda ineficaz evolução normativa referente ao âmbito cibernético. Assim sendo, destacou-se a complexidade na identificação e controle penal desses crimes, devido à rápida evolução do mundo digital e barreiras legais e de cooperação internacional. Evidenciou assim que muitas invasões decorrem de ações precipitadas e falta de compreensão dos mecanismos de segurança. Explorou-se evolução legislativa no Brasil, em especial a Lei 14.155/2021, que ampliou as penas para crimes cibernéticos. Como também, discutiu-se a respeito dos desafios no enquadramento legal de ações no ambiente virtual, como invasão de dispositivo e perseguição, destacando a necessidade de educação e cooperação para mitigar tais práticas.

Além do mais, foram destacados fatores como a dificuldade proposta pelo anonimato dos criminosos, a evolução tecnológica, a falta de colaboração e a limitação de recursos dentre os principais desafios, tendo jurisdição transnacional e lacunas legais como fator ainda mais agravante para a situação. Propôs-se uma abordagem multidisciplinar e uma educação contínua para enfrentar essa realidade, incluindo medidas de proteção digital e conscientização dos usuários. São apresentadas diretrizes fundamentais de segurança cibernética para mitigar os riscos e promover uma utilização segura da tecnologia, ressaltando a importância do entendimento e da aplicação eficaz dessas medidas.

Conclui-se assim com a certeza do quão relevante esse é a análise normativa vigente e a constante necessidade de atualização legal e estratégica para enfrentar os desafios persistentes da criminalidade cibernética na sociedade moderna, enfrentados no âmbito do controle penal, especialmente no que diz respeito à identificação dos perpetradores, o que propicia nitidamente uma reavaliação das

estratégias atuais de política criminal para lidar com essa modalidade de delinquência virtual. Notando-se a importância de explorar as estratégias práticas de prevenção e repressão desses delitos em busca de se ter meios mais eficazes no combate desses obstáculos, visando estabelecer um equilíbrio entre a segurança cibernética e a proteção dos indivíduos.

Diante de todas as nuances desenvolvidas nessa pesquisa, em que se demonstram diversas situações que favorecem uma espécie de “escuridão virtual” e intensificam continuamente as dificuldades da identificação e punição dos criminosos, resta nítido que todo o arcabouço investigativo presente neste estudo, abordando diferentes áreas do conhecimento, é fundamental para o início de um efetivo enfrentamento a esse malefício que cresce exponencialmente.

Destarte, diante da constante inovação tecnológica e sua estreita relação com o direito penal, é imperativo que a legislação e as atuações jurídicas acompanhem essa evolução. A abordagem interdisciplinar, com destaque para os aspectos éticos, sociais e filosóficos, emerge como um caminho promissor para compreender, prevenir e reprimir os crimes cibernéticos. Assim, vislumbramos um futuro no qual a sinergia entre o direito, a tecnologia e as ciências sociais possam promover uma convivência segura e ética na era digital.

Este estudo, ao transitar entre diferentes campos do conhecimento, busca contribuir para a reflexão crítica e o aprofundamento do entendimento sobre crimes cibernéticos e suas implicações para a vítima e a sociedade. Tendo sido, dessa forma, exploradas as nuances dessas problemáticas, visando contribuir para a compreensão dos obstáculos enfrentados e, assim, fornecer subsídios para aprimorar as respostas do sistema jurídico diante dos crimes cibernéticos. Concluo, portanto, com a convicção de que a busca pelo equilíbrio entre inovação, proteção dos direitos e justiça é um desafio fundamental para o nosso tempo.

REFERÊNCIAS

ADACHI, Tomi. **Comitê Gestor da Internet no Brasil (CGI. br): uma evolução do sistema de informação nacional moldada socialmente**. Tese de Doutorado. Universidade de São Paulo, 2009.

AGENCIA BRASIL. "**Estudo mostra que pandemia intensificou uso das tecnologias digitais**". Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2021-11/estudo-mostra-que-pandemia-intensificou-uso-das-tecnologias-digitais. Acesso em: 05 set. 2023.

ANDRADE, Manuel da Costa. **A vítima e o problema criminal**. Coimbra: Coimbra Editora, 1980.

BAUMAN, Zygmunt. **Modernidade Líquida**. Tradução, Plínio Dentzien. Rio de Janeiro: Jorge Zahar Ed., 2001.

BAUMAN, Zygmunt. **Amor Líquido: Sobre a Fragilidade dos Laços Humanos**. Rio de Janeiro: Zahar, 2004.

BBC. "**9 em cada 10 sequestros de SP são 'golpes do Tinder'**" em https://www.bbc.com/portuguese/brasil-63733202. Acesso em 02/10 às 16h23.

BERISTAIN, Antonio. **Nova criminologia à luz do direito penal e da vitimologia**. Brasília: Editora Universidade de Brasília, 2000.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal: Parte Geral**. 19ª ed. São Paulo: Saraiva, 2012.

BRITO, Auriney. **Direito Penal Informático**. São Paulo: Saraiva, 2013.

BERNERS-LEE, T.J.; CAILLIAU, R.; LUOTONEN, A.; NIELSEN, H.F.; SECRET, A. **The World-Wide Web**. Communications of the ACM, v. 37, n. 8, Agosto de. 1994.

CASTRO, Thainer Cordeiro de. **Crimes Virtuais: crimes cibernéticos e as considerações sobre a criminalidade na internet Conteúdo Jurídico.** Brasília-DF: 03 jun 2022. Disponível em: https://conteudojuridico.com.br/consulta/artigos/58585/crimes-virtuais-crimes-cibernticos-e-as-consideraes-sobre-a-criminalidade-na-internet. Acesso em: 12 jul. 2023.

Cohen e Felson, 1979 *apud* SCHMALLEGER, Frank e PITTARO, Michael. **Routine Activity Theory and Internet Crime. In Crimes of the Internet.** Pearson Prentice Hall, New Jersey, 2008.

CLARK, Andy. **Natural-Born Cyborgs: Minds, Technologies, and the Future of Human Intelligence**. Oxford University Press, 2003.

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO. “**Vitimização**” em: https://www.cnmp.mp.br/defesadasvitimas/vitimas/vitimizacao#:~:text=Vitimiza%C3%A7%C3%A3o%20secund%C3%A1ria&text=Abrange%20os%20custos%20pessoais%20derivados,investiga%C3%A7%C3%A3o%20ou%20do%20processo%20penal. Acesso em: 25 ago. 2023.

“**Cyber Crime**”. Disponível em: https://www.fbi.gov/investigate/cyber. Acesso em: 26 set. 2023.

DELMANTO, Celso et al. **Código Penal Comentado**. 8. ed. São Paulo: Saraiva, 2010.

FERREIRA, M. **A (IN) EFICÁCIA DA LEGISLAÇÃO BRASILEIRA NO COMBATE AOS CRIMES VIRTUAIS E O SEUS IMPACTOS EM DECORRÊNCIA DA PANDEMIA DA COVID-19**. Guanambi-BA, 2022. Disponível em:

https://repositorio.animaeducacao.com.br/bitstream/ANIMA/32264/1/crimes%20cibern%C3%A9ticos%20-%20tcc%20II.pdf. Acesso em: 15 jul. 2023

Ferreira, Renan Azevedo Leonessa. **O papel da vítima nos crimes informáticos: contribuições da vitimodogmática e do funcionalismo penal em bens jurídicos disponíveis**. 2022. Dissertação (Mestrado em Direito) - Programa de Estudos Pós Graduados em Direito da Pontifícia Universidade Católica de São Paulo, São Paulo, 2022.

FONSECA, Ana Clara Montenegro. **Conduta da vítima de crime na dogmática penal: análise crítica sobre a posição da vítima na aferição da responsabilidade penal do autor à luz da vitimodogmática e da imputação à vítima**. Dissertação (Mestrado em Direito) - Faculdade de Direito do Recife, Recife, 2009. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/4736/1/arquivo6332_1.pdf. Acesso em: 10 ago. 2023.

FONSECA, Maria Guadalupe Piragibe. **Iniciação à pesquisa no direito: pelos caminhos do conhecimento e da invenção**. Rio de Janeiro: Elsevier, 2009.

GRECO, Alessandra Orcesi Pedro; GRECO, Vicente. **A autocolocação da vítima em risco**. São Paulo: Revista dos Tribunais, 2004.

GRECO, Luís; LEITE, Alaor. **O que é e o que não é a teoria do domínio do fato. Sobre a distinção entre autor e partícipe no direito penal**. In: GRECO, Luís et al. Autoria como domínio do fato: estudos introdutórios sobre o concurso de pessoas no direito penal brasileiro. São Paulo: Marcial Pons, 2014.

G1. “**Grupo de hackers vaza em rede social supostos dados pessoais de**

Bolsonaro, filhos e ministros”. Disponível em: https://g1.globo.com/politica/noticia/2020/06/02/grupo-de-hackers-vaza-em-rede-social-supostos-dados-pessoais-de-bolsonaro-filhos-e-apoiadores.ghtml. Acesso em: 05 out. 2023.

HASSEMER, Winfried. **Introdução aos Fundamentos do Direito Penal**. Sergio Antonio Fabris Editor, Porto Alegre, 2005.

HOLT, T. J., A. M. Bossler, and K. C. Seigfried-Spellar. **Cybercrime and Digital Forensics: An Introduction**. 2nd ed. New York: Routledge, 2018.

INFOMONEY. “**28,2 milhões de brasileiros não têm acesso à internet, diz IBGE**”. 19 set 2022. Disponível em: https://www.infomoney.com.br/consumo/282-milhoes-de-brasileiros-nao-tem-acesso-a-internet-diz-ibge/#:~:text=Apesar%20de%20a%20pandemia%20de,Geografia%20e%20Estat%C3%ADstica%20(IBGE). Acesso em: 05 set. 2023

INTERPOL. **Cybercrime**. Disponível em: https://www.interpol.int/Crimes/Cybercrime. Acesso em: 15 ago. 2023

JAKOBS, Günther. **A imputação penal da ação e da omissão**. Barueri: Editora Manole, 2003.

LÉVY, Pierre. **O Que é Virtual?** Rio de Janeiro: Editora 34, 1996.

LÉVY, Pierre. **Cibercultura**. 1 ed. São Paulo: 34, 1999.

LISBOA, Roberto Senise. **Direito na Sociedade da Informação**, 2016. Disponível em: http://www.egov.ufsc.br/portal/conteudo/direito-na-sociedade-da-informa%C3%A7%C3%A3o. Acesso em: 28 set. 2023.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar**. Tradução: Kátia Aparecida Roque. São Paulo: Pearson Education do Brasil, 2003.

NADER, Paulo. **Introdução ao Estudo do Direito**. 24 ed. Rio de Janeiro: Forense: 2004.

OLIVEIRA, Ana Sofia Schmidt de. **A vítima e o direito penal. Uma abordagem do movimento vitimológico e de seu impacto no direito penal**. São Paulo: Revista dos Tribunais, 1999.

OLIVEIRA, B. **O virtual, o real e o atual — como é viver numa sociedade virtual (baseado em Pierre Lévy)**. 23 Mar. 2020. Disponível em: https://medium.com/reflex%C3%B5es/o-virtual-o-real-e-o-atual-82fdd232fbc9. Acesso em: 12 jun. 2023.

OLIVEIRA, Bruno Henrique Borges de. **Vulnerabilidade digital e a proteção do indivíduo**. TCC - Pontifícia Universidade Católica de Goiás, Goiás, 16 nov. 2020. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/206/1/TCC%20BRUN

O%20HENRIQUE%20BORGES%20DE%20OLIVEIRA.pdf. Acesso em: 14 set. 2023.

PRITTWITZ, Cornelius. La resurrección de La víctima em La teoria penal. *In*: **La víctima en el sistema penal**. Dogmática, proceso e política criminal. Traducción del Prof Dr. Luís Miguel Reyna Alfaro. Lima: Editora Jurídica Grijley.

ROXIN, Claus. **Autoría y dominio del hecho en el derecho penal**. Madrid: Marcial Pons, 2000.

ROXIN, Claus. "**Derecho Penal Parte General**", Madrid: Civitas, 1997.

ROXIN, Claus. **Funcionalismo e imputação objetiva no direito penal**. Tradução de Luís Greco. Rio de Janeiro: Renovar, 2002.

ROXIN, Claus. **Política Criminal y estrutura del delito**. Trad. Juan Bustos Ramirez e Hernan Hormozabal Malarée. Barcelona: PPU, 1992.

R7 TECNOLOGIA E CIÊNCIA. "**Brasil é 2º maior alvo mundial de ciberataques, revela estudo**", 27 jun. 2022. Disponível em: https://noticias.r7.com/tecnologia-e-ciencia/brasil-e-2-maior-alvo-mundial-de-ciberataques-revela-estudo-27062022. Acesso em: 06 set. 23.

SILVA JÚNIOR, Délio Lins e. **Imputação e a conduta da vítima**. Curitiba: Juruá, 2008.

SILVA SÁNCHEZ, Jesús María. Política criminal en la dogmática: algunas cuestiones sobre su contenido y límites. *In*: **Política criminal y nuevo derecho penal: Libro homenaje a Claus Roxin**. Barcelona: Bosch, 1997.

SILVA SÁNCHEZ, Jesús María. **La víctima en el futuro de la dogmática**. Victimología. San Sebastián: Universidad del País Vasco/Euskal Herriko Unibertsitatea, 1990.

SCHÜNEMANN, Bernd. **Temas actuales y permanentes del derecho penal después del milênio**. Madrid: Tecnos, 2002.

SCHÜNEMANN, Bernard. **Teoria de la imputación objetiva**. Traduccion de Mariana Sacher de Köser. *In*: Revista de política criminal e ciências penais. n. I, especial. Mexico, 1999.

SYDOW, Spencer Toth. **Curso de Direito Penal Informático: Partes Geral e Especial. 2**. ed. Salvador: Juspodivm, 2021

SYDOW, Spencer Toth. **Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática**. Dissertação (Mestrado em Direito Penal). Universidade de São Paulo, São Paulo, 2009.

TURING, A. M. **On computable numbers, with an application to the Entscheidungsproblem**. Proceedings of the London Mathematical Society, 2 s. vol. 42, 1937.

WELZEL, Hans. **Derecho penal alemán**. Tradução de Juan Bustos Ramírez y Sergio Yáñez Pérez. 11. ed. Santiago: Editorial Jurídica de Chile, 2003.