Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

LUCAS PERES

CRIMES CIBERNÉTICOS:

A HISTÓRIA DA INTERNET E A PROTEÇÃO LEGAL FRENTE À CRIMINALIDADE VIRTUAL

ASSIS/SP

2023

LUCAS PERES

CRIMES CIBERNÉTICOS:

A HISTÓRIA DA INTERNET E A PROTEÇÃO LEGAL FRENTE À CRIMINALIDADE VIRTUAL

Projeto de pesquisa apresentado ao curso de Direito do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Orientando: Lucas Peres

Orientador: Claudio José Palma Sanches

ASSIS/SP

2023

FICHA CATALOGRÁFICA

Peres, Lucas

P437c Crimes cibernéticos: a história da internet e a proteção legal frente à criminalidade virtual / Lucas Peres. -- Assis, 2023.

33p.

Trabalho de Conclusão de Curso (Graduação em Direito) -- Fundação Educacional do Município de Assis (FEMA), Instituto Municipal de Ensino Superior de Assis (IMESA), 2023.

Orientador: Prof. Me. Cláudio José Palma Sanchez.

1. Crime por computador. 2. Direito penal informático. 3. Legislação. I Sanchez, Cláudio José Palma. II Título.

CDD 341.53

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

CRIMES CIBERNÉTICOS:

A HISTÓRIA DA INTERNET E A PROTEÇÃO LEGAL FRENTE À CRIMINALIDADE VIRTUAL

LUCAS PERES

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

Orientador: Claudio José Palma Sanches

Analisador:

ASSIS/SP

2023

AGRADECIMENTOS

Agradeço aos meus queridos pais, Raimunda Vieira Da Silva e Sérgio Rodrigo Bavaresco, por serem a base sólida que me sustentou durante toda essa trajetória acadêmica. Seu apoio incansável e incentivo constante foram fundamentais para que eu alcançasse cada um dos meus objetivos.

Minha gratidão também se estende aos professores de Direito que tanto admiro e respeito. Suas trajetórias profissionais são exemplos inspiradores do profissional que almejo me tornar.

Expresso minha gratidão a Deus por todas as bênçãos concedidas, pelas valiosas lições aprendidas e pelas oportunidades que se abriram diante de mim ao longo dessa jornada.

Aos amigos e colegas de curso, meu mais sincero agradecimento por compartilharem comigo essa jornada de aprendizado e crescimento. Seu apoio e encorajamento foram verdadeiramente inestimáveis.

Agradeço a todos que de alguma forma contribuíram para minha jornada acadêmica. Suas presenças e incentivos fizeram toda a diferença.

“O fim do Direito não é abolir nem restringir, mas preservar e ampliar a liberdade” (John Locke).

RESUMO

Este trabalho tem como objetivo central realizar um estudo sobre os diversos tipos de crimes cibernéticos, suas classificações e os efeitos que essas ações criminosas têm na sociedade. Explora a evolução constante das tecnologias que possibilitaram a existência desses delitos virtuais.

Uma análise da legislação vigente é apresentada, considerando que, no passado, não havia uma proteção jurídica específica contra os crimes cibernéticos, e apesar dos avanços significativos que tivemos, como por exemplo a promulgação da Lei Carolina Dieckmann ou Marco Civil da Internet, ainda ficamos carentes de legislação especifica, que efetivamente preencha as lacunas existentes na tipificação desses delitos.

Através dessa abordagem, busco ampliar o entendimento sobre os crimes cibernéticos e suas consequências na sociedade moderna e promover uma reflexão sobre a necessidade contínua de atualização e aprimoramento da legislação, a fim de garantir uma proteção adequada contra as ameaças virtuais em constante evolução. Afinal, a crescente sofisticação das tecnologias exige uma resposta efetiva para enfrentar os desafios impostos pela criminalidade digital.

Palavras-chaves: Crimes Cibernéticos; Constante Evolução; Legislação Especifica.

ABSTRACT

The main objective of this work is to carry out a study on the different types of cyber crimes, their classifications and the effects that these criminal actions have on society. It explores the constant evolution of the technologies that made possible these virtual crimes.

An analysis of the current legislation is presented, considering that, in the past, there was no specific legal protection against cyber crimes, and despite the significant advances we have had, such as the promulgation of the Carolina Dieckmann Law or the Civil Rights Framework for the Internet, we are still lacking specific legislation, which effectively fills the existing gaps in the classification of these crimes.

Through this approach, I seek to broaden the understanding of cybercrime and its consequences in modern society and promote a reflection on the continuous need to update and improve legislation, in order to guarantee adequate protection against constantly evolving virtual threats. After all, the increasing sophistication of technologies requires an effective response to face the challenges posed by digital crime.

Keywords: Cyber Crimes; Constant Evolution; Specific Legislation.

SUMÁRIO

INTRODUÇÃO.....10

1. PROCESSO EVOLUTIVO DA INTERNET.....11
1.1. TCP/IP.....11
1.2. WORD WIDE WEB.....12
1.3. A INTERNET COMERCIAL.....13

2. O QUE É UM CRIME CIBERNÉTICO?.....14
2.1. TIPOS DE CRIMES CIBERNÉTICOS.....14

3. CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS.....16
3.1. CRIMES CIBERNÉTICOS PRÓPRIOS.....16
3.2. CRIMES CIBERNÉTICOS IMPRÓPRIOS.....17

4. SUJEITOS DOS CRIMES CIBERNÉTICOS.....18
4.1. SUJEITO ATIVO.....18
4.2. SUJEITO PASSIVO.....20

5. LEGISLAÇÕES.....20
5.1. MARCO CIVIL DA INTERNET - LEI Nº 12.965, DE 23 DE ABRIL DE 2014.....20
5.2. LEI CAROLINA DIECKMANN.....22
5.3. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD).....24

6. METAVERSO: TERRENO FÉRTIL PARA CRIMES CIBERNÉTICOS.....24
6.1. POTENCIALIZAÇÃO DOS CRIMES VIRTUAIS NO METAVERSO.....26

7. INEFICÁCIA DA LEGISLAÇÃO FRENTE AOS CRIMES CIBERNÉTICOS.....27

8. OUTROS DESAFIOS ENFRENTADOS NO COMBATE A CIBERCRIMINALIDADE.....29

9. CONCLUSÃO.....31

REFERÊNCIAS.....32

INTRODUÇÃO

A evolução da Internet, desde sua criação como ARPANET durante a Guerra Fria, até se tornar a onipresente World Wide Web, trouxe consigo inúmeras transformações na forma como interagimos, trabalhamos e nos comunicamos. No entanto, essa rápida expansão também deu origem a uma série de desafios relacionados à segurança cibernética.

Os crimes cibernéticos, também conhecidos como crimes virtuais ou digitais, são atividades criminosas que ocorrem por meio da internet e de dispositivos eletrônicos, abrangendo a prática de furtos, fraudes, estelionatos e uma série de outras condutas ilícitas. Esses crimes exploram a tecnologia para ganho financeiro, danos a sistemas, violações de privacidade e outros fins.

Normas como o Marco Civil, Lei Carolina Dieckmann e Lei Geral de Proteção de Dados são importantes instrumentos legais para combater crimes cibernéticos, proteger a privacidade dos usuários e regulamentar o tratamento de dados pessoais no ambiente digital. Contudo, é necessário atualizar as leis conforme a evolução tecnológica e novos desafios surgem.

A ausência de leis específicas para crimes cibernéticos cria lacunas na legislação, permitindo que criminosos escapem da responsabilidade. A adaptação jurídica é necessária para proteger os direitos dos usuários virtuais e proporcionar punições adequadas e proporcionais aos crimes cometidos no ambiente digital. A criação de tipos penais específicos, é uma abordagem proporcional e razoável para combater a ineficácia da legislação atual.

Em resumo, os desafios dos crimes cibernéticos incluem rápida evolução das ameaças, atuação transnacional, identificação de criminosos, leis inadequadas e falta de conscientização. A colaboração entre governos, empresas, sociedade civil e especialistas, além da atualização constante das leis, são fundamentais para proteger a sociedade digital em constante expansão.

1. PROCESSO EVOLUTIVO DA INTERNET

Para compreender melhor os delitos que podem ser cometidos no âmbito cibernético, devemos primeiramente percorrer o processo evolutivo da internet, sendo impossível registrar cada marco, sem se especificar nas tecnicalidades.

A internet, ou ARPANET (Advanced Research Projects Agency Network), como era chamada, foi criada durante a Guerra Fria, um embate entre Estados Unidos e União Soviética em termos ideológicos, econômicos, políticos, militares e tecnológicos.

Teve seu nascimento a partir de um projeto de acadêmicos desenvolvido na agência norte-americana ARPA (Advanced Research and Projects Agency), proveniente da necessidade de proteção das informações e comunicações nos Estados Unidos, em caso de um ataque nuclear partido da União Soviética.

Assim, no dia 29 de outubro de 1969, foi estabelecida a primeira conexão entre a Universidade da Califórnia e o Instituto de Pesquisa de Stanford, onde o primeiro e-mail da história seria enviado, marcando historicamente o nascimento da internet. Não demorou para que o projeto se expandisse já que em 1970, a ARPANET estava consolidada com dezenas de computadores conectados.

No ano de 1971, uma equipe de acadêmicos chamada Network Working Group desenvolve o primeiro controle de protocolo: NPC (Network Control Protocol), que permitia o desenvolvimento de aplicativos a partir dos computadores conectados à ARPANET, o que possibilitou que, mais tarde, em 1972, Ray Tomlinson criasse o primeiro software básico de e-mail, o aplicativo que revolucionou o modo de comunicação entre pessoas naquela época.

Com o tempo, a ARPANET ultrapassou apenas o uso militar, fazendo com que fosse utilizada no âmbito cientifico para disseminação de informações, já que em 1974, mais de 50 universidades americanas estavam conectadas a ela.

1.1. TCP/IP

Entre as décadas de 70/80, os meios de comunicação se expandiram para rádio e a comunicação por satélite, meios estes que a ARPANET era incapaz de se comunicar. Foi então que entre 1973 e 1974, Robert Kahn e Vinton Cerf desenvolveram um novo

protocolo de comunicação, o TCP/IP (*Transmission Control Protocol - Internet Protocol),* consolidando a “rede das redes”, com a premissa de que eram necessárias regras para o seu melhor funcionamento.

> A Internet era uma rede aberta, com quatro regras básicas: novas redes poderiam interconectar-se a ela, sem modificações internas; as comunicações seriam feitas na base do melhor esforço possível (“best effort”) e se um pacote transmitido não chegasse ao destino este simplesmente seria repetido; os equipamentos para interligar as redes (roteadores e gateways) seriam simples e não preservariam a informação transferida; finalmente, não haveria uma supervisão centralizada da rede (LEINER 1997, p. 104; ISAACSON 2014, p. 256-259 apud LINS, 2013, p. 16).

Em 1983, foi estipulado que ARPANET mudaria seu protocolo do NPC para o mais novo e melhorado, TCP/IP.
No final dos anos 80, a Fundação Nacional de Ciências em Washington D.C, começou um projeto de uma rede de área ampla inovadora chamada NSFNET (National Science Foundation Network) que tinha como objetivo, interconectar redes de universidades e instituições de pesquisa nos Estados Unidos, de forma rápida e eficaz.
Em 1990 a ARPANET é desativada e a NSFNET se torna a espinha dorsal da comunicação de longa distância e alta velocidade de redes, padronizando também, o protocolo TCP/IP.

1.2. WORD WIDE WEB

É com a criação do cientista, físico e professor britânico Tim Berners-Lee que começamos a observar o nascimento da internet como conhecemos hoje, já que até a década de 1990, a Internet continuava a ser uma rede restrita à comunidade acadêmica e às agências governamentais. Dois desenvolvimentos vieram modificar essa concepção. O primeiro foi o conceito de World Wide Web. O segundo, a criação do browser, o navegador. (LINS, 2013, P. 24).
A criação se tratava de um sistema de distribuição de documentos de hipertexto (HTTP), ou seja, “documentos” ou “paginas” interligadas, acessadas por um ponto de referência *(hyperlinks)*.
Foi em 1992 que um grupo de programadores deram o próximo passo com a criação do primeiro *web browser* funcional, o Mosaic, que permitia que os navegadores se deslocassem de uma pagina para outra em um só *click,* de forma rápida e eficaz.

1.3. A INTERNET COMERCIAL

Não demorou para que mais páginas e portais fossem criados. A gama de conteúdo era extensa, com infinitas possibilidades.

Surge AOL e Yahoo, salas de bate-papo, serviços de e-mail gratuitos como Hotmail, sites de pesquisa como Google, e muito mais.

Ao chegar nos anos 2000, o sucesso da internet se consolida, nunca deixando de evoluir.

Com o passar do tempo não só o conteúdo online se aperfeiçoa, mas sim a conexão também. A Internet discada da lugar à Banda Larga, o acesso é possível através do telefone celular. Tudo caminha para que a internet passe a não ser mais uma ferramenta, e sim uma necessidade diária.

A Internet se tornou essencial em nossas vidas, transformando a maneira como nos comunicamos, trabalhamos, aprendemos e nos divertimos. Ela nos conecta com pessoas em todo o mundo, oferece acesso a uma quantidade imensa de informações e serviços, e permite que realizemos atividades sem sair de casa.

A acessibilidade da Internet é uma característica importante hoje em dia. Com smartphones e tablets cada vez mais disponíveis, mais pessoas têm acesso à Internet. Isso resultou em uma sociedade mais conectada, onde podemos interagir virtualmente com pessoas de diferentes culturas e ampliar nossas perspectivas.

Além disso, a Internet se tornou uma ferramenta poderosa para o comércio. O comércio eletrônico cresceu bastante, permitindo que as pessoas comprem e vendam produtos e serviços de maneira rápida e conveniente. Empresas de todos os tamanhos podem alcançar um público global e expandir seus negócios além das fronteiras físicas.

A disseminação de informações e conhecimentos é outro papel crucial da Internet. As redes sociais, sites de notícias e blogs facilitam o compartilhamento de informações em tempo real, possibilitando acesso a notícias, pesquisas acadêmicas, tutoriais e muito mais. Isso incentiva o aprendizado contínuo e o desenvolvimento pessoal.

No entanto, a Internet também traz problemas e desafios. A privacidade e a segurança dos dados são questões fundamentais, devido à quantidade crescente de informações pessoais compartilhadas online. É necessário um equilíbrio entre o acesso livre à informação e a proteção dos dados pessoais tanto pelo usuário como pelo Estado, frente aos perigos acarretados.

Nesse sentido, aponta Guilherme de Souza Brambilla, sobre a ameaça que surge junto a internet:

> À medida que a internet crescia de maneira incontrolável, passou a ser alvo dos agora existentes hackers. São considerados “vilões virtuais”, que usam desse meio para invadir, roubar, piratear e outros incontáveis atos que geraram graves problemas de segurança na “rede”. Enquanto que os computadores e a internet passaram a ser um bem indispensável nas casas da sociedade, tais crimes tomaram espaço e agora fazem parte da chamada da internet (BRAMBILLA, 2015, p. 2).

2. O QUE É UM CRIME CIBERNÉTICO?

Também chamados de crimes virtuais ou digitais, são condutas criminosas cometidas por meio da internet e de dispositivos eletrônicos, se utilizando dessas ferramentas para pratica de furtos, fraudes e estelionatos, por exemplo.

O site Kaspersky traz a presente definição:

> O crime cibernético é uma atividade criminosa que tem como alvo ou faz uso de um computador, uma rede de computadores ou um dispositivo conectado em rede. Não todos, mas a maioria dos crimes cibernéticos é cometida por cibercriminosos ou hackers que querem ganhar dinheiro. No entanto, ocasionalmente, o crime cibernético visa danificar computadores ou redes por outros motivos que não o lucro. Nesses casos, os motivos podem ser pessoais ou políticos.

Ainda, Ivette Senise Ferreira, classifica da seguinte forma:

> Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial (FERREIRA, 2005, p.261 apud CARNEIRO, 2012).

A gama das condutas ilegais praticadas neste âmbito é extensa, crimes tais como o acesso não autorizado a sistemas de computadores, danos deliberados a esses sistemas, interceptação de comunicações, manipulação de dados, violação de direitos autorais, incitação ao ódio e discriminação, ridicularização religiosa, disseminação de pornografia infantil, atos de terrorismo, entre outros. Em suma, trata-se de atividades ilegais realizadas por meio de tecnologia digital e internet. (CRESPO, 2011, p. 20).

2.1. TIPOS DE CRIMES CIBERNÉTICOS

Abaixo, segue alguns dos principais crimes cibernéticos e suas possíveis tipificações:

Acesso não autorizado: Invadir ilegalmente sistemas de computador ou redes sem a permissão do proprietário.

- Artigo 154-A do Código Penal Brasileiro - Lei nº 2.848/1940.

Ataques cibernéticos: Realizar ataques como negação de serviço (DDoS), que sobrecarregam um sistema ou rede, tornando-o inacessível aos usuários legítimos.

- Pode ser tipificado em diversos artigos, tais como, artigo 266 (Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública) e artigo 163 (Dano), ambos do Código Penal Brasileiro - Lei nº 2.848/1940.

Phishing: Tentativa de enganar usuários para obter informações confidenciais, como senhas, detalhes bancários ou números de cartão de crédito, por meio de mensagens fraudulentas ou sites falsos.

- Artigo 171 do Código Penal Brasileiro - Lei nº 2.848/1940 (Estelionato), por exemplo.

Ransomware: Bloquear o acesso aos arquivos ou sistemas de uma vítima e exigir um resgate em troca de sua liberação.

- Pode ser tipificado em diferentes artigos, como extorsão, dano ou acesso não autorizado.

Fraude eletrônica: Realizar atividades fraudulentas online, como esquemas de phishing, falsificação de identidade, venda de produtos falsificados ou não entregues e manipulação de transações financeiras.

- Artigo 171 do Código Penal Brasileiro - Lei nº 2.848/1940 (Estelionato) e Lei nº 12.737/2012 (Lei Carolina Dieckmann - Crimes Cibernéticos).

Furto de identidade: Roubar informações pessoais de terceiros para cometer fraudes ou atividades ilegais em nome da vítima.

- Artigo 307 do Código Penal Brasileiro - Lei nº 2.848/1940 (Falsa Identidade).

Violência virtual e assédio online: Praticar atos de violência, ameaças, difamação ou assédio por meio de plataformas digitais.

- Artigos 138,139 e 140 do Código Penal podem ser aplicados (difamação, calúnia e injúria).

Pornografia infantil: Produção, distribuição ou posse de material pornográfico envolvendo crianças.

- Artigos 240 e 241 da Lei nº 8.069/1990 (Estatuto da Criança e do Adolescente).

Violação de direitos autorais: Reproduzir, distribuir ou compartilhar conteúdo protegido por direitos autorais sem autorização do detentor dos direitos.

- Lei nº 9.610/1998 (Lei de Direitos Autorais).

Extorsão online: Usar informações pessoais ou comprometedoras para chantagear as vítimas, exigindo dinheiro ou outros favores em troca.

- Artigo 158 do Código Penal Brasileiro - Lei nº 2.848/1940 (Extorsão).

E a lista não se encerra por aqui, já que novos tipos de crimes cibernéticos podem surgir à medida que a tecnologia e as práticas criminosas evoluem. É importante observar que as leis e definições específicas podem variar de acordo com cada sistema jurídico.

3. CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

Dentre as várias classificações doutrinárias utilizadas para definir crimes virtuais, a mais adotada é aquela que os divide em duas categorias: crimes virtuais próprios e impróprios. Essa classificação é considerada a mais próxima da realidade dos fatos e mais didática, quando se trata dos crimes cometidos no ambiente virtual.

3.1. CRIMES CIBERNÉTICOS PRÓPRIOS

Os crimes cibernéticos puros ou próprios, são aqueles que tem como objeto, o próprio sistema computacional. São crimes onde a execução e a consumação ocorrem exclusivamente no ambiente digital.

Temos como exemplo as invasões de sistemas, phishing, ataques de negação de serviço (DDoS), propagação de malware e o cyberbullying.

Vejamos o que o doutrinador Damásio Evangelista de Jesus, afirma sobre os crimes cibernéticos próprios:

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado (apud CARNEIRO, 2012, [n.p.]).

3.2. CRIMES CIBERNÉTICOS IMPRÓPRIOS

Os crimes cibernéticos impuros ou impróprios, são delitos que possuem início ou estão relacionados ao ambiente digital, mas acabam produzindo efeitos no mundo físico ou possuem conexão com ações reais. Neste, o sistema de informática e seus componentes são utilizados como meio para a pratica de um ato ilícito final.

Ainda utilizando-me das sabias palavras de Damásio Evangelista de Jesus, podemos chegar à conclusão que:

> Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não-computacionais ou diversos da informática (DAMÁSIO apud CARNEIRO, 2012, [n.p.]).

Ao contrário dos crimes cibernéticos próprios, que ocorrem exclusivamente no ambiente virtual, os crimes cibernéticos impróprios têm consequências que transcendem o mundo digital. São exemplos desses crimes, a falsificação de documentos, os furtos virtuais, as ameaças e os crimes contra a honra.

Como dito anteriormente, há diversas classificações para os crimes virtuais na doutrina, e após a análise da mais adotada, fica importante uma breve exposição das outras discutidas. Para isso, segue um quadro elaborado por Josefa Cristina Tomaz Martins Kunrath, com algumas classificações, suas descrições e os autores que as disseminam:

Autor	Classificação	Descrição
Ulrich Sieber (1986)	1) crimes econômicos;	Ilícitos praticados contra os sistemas de processamento de dados com o propósito de obter proveito econômico
	2) ofensas contra direitos individuais	Invasão de dados pessoais para manipulação, destruição ou divulgação,
	3) ofensas contra interesses supraindividuais.	manipulação de dados das instituições públicas, afetando a interesses coletivos.

Vianna (2003)	Crimes informáticos impróprios:	Aqueles nos quais o computador é usado como instrumento para a execução do crime, mas não há ofensa ao bem jurídica inviolabilidade da informação automatizada (dados),praticados nas redes sociais ou através do envio de um e-mail.
	Crimes informáticos próprios	Aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas
	Delitos informáticos mistos	São crimes complexos em que, além da proteção da inviolabilidade dos dados, a norma visa a tutelar bem jurídico de natureza diversa.
	Crimes informáticos mediatos ou indiretos	É o delito-fim não informático que herdou esta característica do delito-meio informático realizado para possibilitar a sua consumação
Ferreira (2010),	(a) Puro	A conduta ilícita do delinquente atinge o sistema de informática da vítima, seus programas e/ou a parte física dos computadores.
	(b) Misto	O objetivo da conduta não é diretamente o sistema ou dados, mas o infrator tem que, essencialmente, utilizar a informática para alcançar seu objetivo.
	(c) Comum	Delito já previsto na legislação penal, e que foi realizado através da informática, porém não necessariamente necessita da informática para alcançar seu resultado.
Ivete Senise Ferreira (2000) e Vicente Greco Filho (2000	(a) condutas perpetradas contra um sistema informático.	
	(b) condutas perpetradas contra outros bens jurídicos.	

(KUNRATH, 2017, p. 49-50 apud SILVA JUNIOR, 2021.)

4. SUJEITOS DOS CRIMES CIBERNÉTICOS

Os sujeitos dos crimes cibernéticos referem-se às pessoas ou entidades envolvidas nas práticas ilícitas na internet.

4.1. SUJEITO ATIVO

O sujeito ativo do crime cibernético é o indivíduo ou grupo responsável por realizar a ação criminosa em ambiente virtual. É crime comum, ou seja, pode ser praticado por qualquer pessoa. Vejamos:

> No crime em questão, adicionado ao Código Penal pela Lei 12.737/12, considera-se que pode incorrer como sujeito ativo qualquer pessoa, já que o seu tipo penal não exige nenhuma qualidade especial do seu agente, sendo, portanto, um crime comum (HARAKEMIV; VIEIRA, 2014, p.424 apud COSTA e SILVA, 2021, p. 189).

São os agentes que executam atividades ilegais ou maliciosas utilizando a tecnologia da informação e a internet. O sujeito ativo é quem pratica as ações delituosas, buscando obter ganhos financeiros, prejudicar outros, roubar informações, danificar sistemas ou cometer outras atividades criminosas utilizando o meio digital.

A imputação dos crimes no âmbito cibernético é bem dificultosa, portanto, os sujeitos do crime cibernético podem ser variados e abrangem diferentes tipos de agentes.

Citando algum dos principais sujeitos do crime cibernético, temos como exemplo os hackers, indivíduos com habilidades avançadas de computação e tecnologia da informação, que de forma errônea são reconhecidos tão somente como pessoas que exploram a vulnerabilidade de sistemas e redes de computadores para obter acesso não autorizado, roubar informações confidenciais, distribuir malware ou causar danos

No entanto, nem todos os hackers optam por se envolver em atividades ilegais ou imorais.

Damásio De Jesus argumenta:

> Não podemos consentir com esta cultura. Um hacker é um profundo conhecedor de informática, podendo ser um profissional de segurança da informação ou pesquisador, que não utiliza seus conhecimentos para fins ilegítimos. Assim, é erro grave classificar hacker como um bandido. Na verdade, qualquer pessoa pode cometer um crime digital (DAMÁSIO e MILAGRE, 2016, p. 59).

Já os chamados crackers, são hackers que se envolvem em atividades maliciosas, como invasões de sistemas e roubo de informações, com o objetivo de prejudicar ou obter ganhos ilegais. Para Dámasio (apud MILAGRE, 2016, p. 59) “Seriam os verdadeiros criminosos da rede. Utilizam seus conhecimentos de tecnologia para más finalidades.”

Interessante também citar os phishers, criminosos que enviam mensagens de e-mail, mensagens instantâneas ou páginas falsas para enganar as pessoas e obter informações confidenciais, como senhas e números de cartões de crédito.

Não são apenas pessoas com grande conhecimento técnico que cometem crimes na rede de computadores. Os chamados *script kiddies* são indivíduos sem muitas habilidades técnicas, que se utilizam de ferramentas e scripts desenvolvidos por outros para realizar atividades destrutivas ou ilegais na internet.

Há diversos tipos de criminosos nesse âmbito, e o que se pode notar, é que o mundo do crime cibernético é complexo e dinâmico, e essas categorias podem se sobrepor ou se desdobrar em outras classificações.

4.2. SUJEITO PASSIVO

O sujeito passivo, ou seja, a vítima do crime em sede virtual pode ser qualquer pessoa, tanto indivíduos comuns (pessoas físicas) como empresas e organizações (pessoas jurídicas) que tem seus bens desviados, seu patrimônio danificado ou suas informações violadas. Essas ações criminosas podem causar prejuízos financeiros, perda de propriedade ou danos à reputação.

Vejamos o que diz a jurista Sônia Maria Chaves Haracemiv:

> Quanto ao sujeito passivo dos crimes informáticos considera-se que possa ser qualquer pessoa que utilize ou não o meio eletrônico, podendo existir mais de um indivíduo desde que tenham seus bens jurídicos ameaçados ou lesados pela mesma conduta delituosa, como por exemplo, uma série de e-mails contendo o mesmo conteúdo viral cujo objetivo é lesar quem os recebe (HARAKEMIV; VIEIRA, 2014, p.424 apud COSTA e SILVA, 2021, p. 189).

5. LEGISLAÇÕES

É fundamental discorrer acerca das legislações mais específicas que garantem a proteção dos direitos no âmbito digital, das quais destacam-se três como as mais relevantes.

5.1. MARCO CIVIL DA INTERNET - LEI Nº 12.965, DE 23 DE ABRIL DE 2014

O Marco Civil da Internet, também conhecido como a "Constituição da Internet", é a uma Lei que veio para garantir direitos e liberdades aos usuários da rede mundial de computadores no Brasil. É uma legislação muito importante no enfrentamento dos crimes

cibernéticos. Desde seu nascimento em 2014, essa lei tem se mostrado essencial para garantir a segurança dos usuários e a proteção da sociedade no ambiente digital, bem como para estabelecer regras para a atuação dos provedores de serviços online.

> Em análise à Lei do Marco Civil da Internet, nota-se que a Lei estabelece princípios, direitos e deveres dos usuários da internet. Alguns textos sobre a referida Lei, com maior destaque para os jornalísticos, expressam que esta Lei seria uma espécie de "Constituição da Internet" e que a elaboração de um projeto desse porte e tema surgiu pelo fato de que, após 18 anos de uso da internet no Brasil, não havia qualquer lei que regulasse e estabelecesse diretrizes para proteger os seus direitos. Em outras palavras, essa argumentação entende que, sem o chamado Marco Civil, o Judiciário se via carente de legislação para fundamentar suas decisões em casos de disputas judicias (LEITE, G. S. e LEMOS, 2014).

Uma das principais contribuições do Marco Civil da Internet é o estabelecimento da neutralidade da rede. Esse princípio garante que todas as informações e dados da internet sejam tratados de forma igualitária, sem discriminação por parte dos provedores de acesso. Isso é crucial para evitar que os criminosos cibernéticos possam ser favorecidos em suas ações ilícitas, garantindo que todos os usuários tenham acesso livre e justo a internet.
Além disso, o Marco Civil estabelece a proteção da privacidade e a segurança dos dados pessoais dos usuários e essa proteção é fundamental para evitar o uso indevido de dados e prevenir crimes cibernéticos como o roubo de identidade, a fraude e o phishing. Ao determinar que os provedores devem coletar apenas os dados necessários para a prestação do serviço e respeitar a privacidade nas comunicações.

George Salomão Leite e Ronaldo Lemos fazem uma análise especifica de tal garantia, que está disposta no art. 7° da Lei 12.965:

> .... o artigo 7° deve ser interpretado sob duas óticas; numa primeira leitura estão preservados os direitos da privacidade e intimidade do indivíduo que recebem salvaguarda constitucional e são as prerrogativas subjetivas do indivíduo num estado democrático de direito. Uma segunda leitura revela que esses direitos permanecem preservados quando inseridos num banco de dados que trafega pela internet. Ou seja, a proteção objetiva conferida pelo Marco Civil aos dados pessoais é, por reflexo, a mesma proteção conferida pela lei ao titular dos dados LEITE, G. S. e LEMOS, 2014).

Outro ponto importante é a responsabilização dos provedores de internet pelo conteúdo produzido por terceiros em suas plataformas. Embora os provedores não sejam responsáveis pelo que seus usuários publicam, o Marco Civil estabelece que mediante ordem judicial, eles devem retirar conteúdos considerados ilegais, como discurso de ódio,

pornografia infantil e incitação à violência. Essa medida ajuda a combater crimes cibernéticos que envolvam a divulgação de material ilegal ou prejudicial.

O armazenamento de registros de conexão dos usuários também é uma importante ferramenta no combate aos crimes cibernéticos. Esses registros permitem que, em casos de investigações criminais, as autoridades tenham acesso a informações que possam ajudar a identificar os responsáveis por atividades ilícitas na internet.

Explica Damásio De Jesus:

> Deste modo, diante do uso criminoso de um serviço, ainda que de forma anônima, como, por exemplo, na criação de uma comunidade, grupo, ou página destinada à pornografia infantil, sabe-se que o provedor dos serviços (pago ou gratuito) registra os dados de acesso à aplicação (em alguns casos, até mesmo as atividades realizadas – embora muitos afirmem que não), porém tais registros só são fornecidos como ordem judicial. Obtendo-se os dados de acesso às aplicações daquele que utilizou o serviço para más finalidades, pode-se, através do IP (Internet Protocol), que será fornecido, descobrir qual o Provedor de Acesso associado ao IP (caso o usuário não tenha mascarado a conexão), e, com isto, oficiá-lo, para que apresente os dados físicos (nome, endereço, RG, CPF, CNPJ, dentre outros) da pessoa responsável pela conta de Internet a qual estava atribuído o referido IP, na exata data e hora da atividade maliciosa (DAMÁSIO e MILAGRE, 2016, p. 184).

Outra vantagem é a cooperação internacional no combate aos crimes cibernéticos. O Marco Civil estabelece regras claras para a colaboração entre países na investigação dessas ações criminosas que ultrapassam fronteiras.

Em suma, o Marco Civil da Internet é uma ferramenta poderosa no enfrentamento dos crimes cibernéticos, garantindo a liberdade, a privacidade e a segurança dos usuários, responsabilizando os provedores e facilitando a atuação das autoridades na prevenção e combate desses crimes. Entretanto, é essencial que as leis continuem sendo atualizadas e aprimoradas considerando que a tecnologia avança e novos desafios surgem, garantindo assim uma internet cada vez mais protegida contra os crimes cibernéticos.

5.2. LEI CAROLINA DIECKMANN

A Lei Carolina Dieckmann, também conhecida como Lei nº 12.737/2012, foi sancionada no Brasil em 30 de novembro de 2012 e recebeu esse nome em homenagem à atriz Carolina Dieckmann. Essa legislação surgiu após a atriz ter sido vítima de um crime cibernético, onde fotos íntimas suas foram roubadas e divulgadas na internet sem o seu consentimento.

Modifica o Código Penal para incluir os artigos 154-A e 154-B, que tratam da invasão de dispositivo informático e suas penalidades. Define a invasão de dispositivo informático alheio, conectado ou não à rede, com o objetivo de obter, adulterar, destruir dados ou instalar vulnerabilidades sem autorização expressa ou tácita do titular do dispositivo. Estipula as penalidades para essa conduta, considerando agravantes como prejuízo econômico, obtenção de conteúdo privado, segredos comerciais ou industriais, controle remoto não autorizado e aumenta as penas para crimes cometidos contra autoridades públicas. Também normatiza sobre como se procede a ação penal nos casos de crimes definidos no artigo 154-A da Lei.

Modifica os artigos 266 e 298 do Código Penal, tratando da interrupção ou perturbação de serviços telemáticos, informáticos e de informação de utilidade pública, bem como da falsificação de documento particular. Acrescenta a equiparação de cartões de crédito ou débito a documentos particulares.

Essa lei representa um marco importante no combate aos crimes virtuais, criminalizando a invasão de dispositivos eletrônicos, como computadores, smartphones, tablets e redes sociais. Ela também prevê penalidades para a divulgação não autorizada de conteúdos íntimos sem o consentimento da pessoa envolvida.

Antes da Lei Carolina Dieckmann, o Brasil necessitava de uma legislação específica para combater efetivamente esses tipos de crimes virtuais, o que dificultava muito a punição para esses delitos. A partir de sua promulgação, indivíduos que cometem tais delitos passaram a ser responsabilizados criminalmente, estando sujeitos a penas que podem variar de detenção a multas, dependendo da gravidade da infração.

Nesse sentido, explica a especialista em direito digital, Patrícia Peck Pinheiro:

> Desde 1999 o Brasil discutia o Projeto de Lei de Crimes Eletrônicos, e nem os ataques das quadrilhas fizeram o projeto andar, como fez o efeito “Carolina Dieckmann”, em que o vazamento de fotos íntimas de uma celebridade trouxe à tona novamente a importância de se aprovar uma lei como esta. Isso porque a liberdade de um vai até onde não fira o direito de outro (PINHEIRO, 2021, p. 43).

Além disso, a lei também trouxe dispositivos que visam garantir maior segurança e proteção às vítimas desses crimes, facilitando a retirada de conteúdos ofensivos ou íntimos da internet e preservando a dignidade e a privacidade das pessoas afetadas.

Vale ressaltar que a Lei Carolina Dieckmann não apenas pune os indivíduos que praticam crimes virtuais, mas também mostra a importância da segurança do mundo digital nos

tempos em que estamos vivendo. Com ela, o Brasil deu um passo significativo para enfrentar os desafios da criminalidade virtual e proteger os cidadãos de violações injustas e humilhantes de sua intimidade na internet.

Apesar do nascimento da Lei nº 12.737/2012 ter sido muito importante e significativo, é defendido por boa parte da doutrina e juristas, que existem lacunas não exploradas na Lei, tornando os dispositivos ainda insuficientes para punir os criminosos virtuais e proteger os usuários de forma verdadeiramente efetiva.

5.3. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

A Lei Geral de Proteção de Dados (LGPD) de 14 agosto de 2018, tem como objetivo garantir a privacidade e a segurança dos dados pessoais dos cidadãos, tanto no mundo físico quanto no mundo digital.

Regulariza todo o tratamento de dados, por pessoa natural ou por pessoa jurídica de direito público ou privado, como por exemplo a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração de dados (GOV.BR).

A Lei estabelece requisitos para o tratamento de dados pessoais, por pessoas, empresas e poder público. Dispõe sobre o consentimento dos titulares, da manipulação dos dados de crianças e adolescentes, dos direitos dos titulares, da interferência internacional de dados, das responsabilidades dos encarregados, das sanções em caso de descumprimento da Lei, das boas práticas no exercício desse tratamento, da segurança e etc.

Em suma, para seu propósito em especifico, cobre uma boa área do que não era tipificado anteriormente e tem como objetivo regulamentar a coleta, o tratamento, o armazenamento e o compartilhamento de dados pessoais por empresas e organizações no Brasil.

Foi projetada para garantir a privacidade, a segurança e os direitos dos titulares dos dados, dando-lhes maior controle sobre suas informações pessoais em um ambiente cada vez mais digital.

6. METAVERSO: TERRENO FÉRTIL PARA CRIMES CIBERNÉTICOS

O metaverso é um novo tipo de universo virtual que busca reproduzir a realidade por meio de tecnologias avançadas, como a realidade virtual, realidade aumentada, hologramas e etc. É um espaço tridimensional que proporciona a interação entre pessoas de forma completamente virtual e em tempo real. Um novo mundo utópico ainda em desenvolvimento, que promete criar um novo tipo de sociedade através de uma nova camada de realidade.

O termo "metaverso" veio do romance de ficção científica "Snow Crash" de Neal Stephenson, publicado em 1992, que conta a história de “Hiro Protagonist”, um jovem que se utiliza desse novo mundo virtual para escapar de sua realidade frustrante.

Embora o conceito de metaverso já existisse há algum tempo, foi apenas em 2021 que o termo ganhou popularidade e reconhecimento geral. Esse marco aconteceu quando Mark Zuckerberg, o fundador do Facebook e um dos maiores entusiastas da ideia, surpreendeu o mundo ao anunciar a decisão de renomear a empresa para "Meta". Além disso, ele deixou claro que a nova visão da empresa estava direcionada para a construção e desenvolvimento de um verdadeiro metaverso.

Durante uma coletiva de imprensa para a discussão da mudança do nome e foco da empresa, Mark explica:

> Você será capaz de fazer quase tudo que você possa imaginar, reunir-se com amigos e família, trabalhar, aprender, brincar, fazer compras, criar, bem como experiências completamente novas que realmente não se encaixam na forma como pensamos sobre computadores ou telefones hoje.

Na atualidade, apesar de ainda em desenvolvimento, o universo totalmente imersivo já é uma realidade, proporcionando aos seus usuários a oportunidade de criarem avatares em 3D e usufruírem desse ambiente verdadeiramente inovador. Permite aos seus usuários exercerem atividades como trabalho, estudo e desfruto de uma vida social, assim como a aquisição de bens e serviços virtuais através das chamadas "criptomoedas". Tais avanços estão impulsionando a criação de um mercado completamente novo, repleto de possibilidades e potencialidades.

Em uma análise mais profunda da moeda e economia virtual no metaverso, veja o que diz Fernando Eduardo Serec:

> Em um ambiente de economia virtual, moedas são trocadas entre usuários nas mais diversas operações, podendo envolver uma taxa transacional. Isso porque a empresa hospedeira do ambiente virtual será responsável por criar esta moeda,

> manter seu valor e, em alguns casos, pode até sentir a necessidade de regular a sua disponibilidade de modo a evitar inflação. Não se sabe ainda se o metaverso se organizará com base em uma economia análoga à economia física, na qual os Estados manterão suas moedas e taxas de conversão, ou se uma economia virtual completamente nova irá surgir — as duas possibilidades podem, por ora, ser consideradas (SEREC, 2022, P. 46).

Uma forma interessante de entender o conceito do metaverso é através do filme Matrix, dirigido por Lilly e Lana Wachowski. Na trama, os indivíduos habitam um mundo virtual criado por uma inteligência artificial malévola, que explora seus corpos como fonte de energia.

No universo de Matrix, as pessoas são mantidas em um estado de ilusão, enquanto suas mentes estão conectadas a uma realidade simulada.

Embora a realidade de Matrix seja uma obra de ficção, as ideias por trás dela provocam reflexões sobre os dilemas associados ao metaverso ou realidade virtual avançada. Será que essa nova realidade é realmente utópica? Quais os riscos que essa invenção inovadora pode causar contra nossa segurança, saúde mental e privacidade?

6.1. POTENCIALIZAÇÃO DOS CRIMES VIRTUAIS NO METAVERSO

Para atender ao foco do presente trabalho, trato sobre a problemática da potencialização de crimes nesse novo mundo imersivo. No metaverso, uma gama de crimes pode ocorrer, paralelos aos do mundo real, mas adaptados para o contexto digital.

Em meio aos crimes virtuais que podem ocorrer no metaverso, destacam-se, dentre outros, fraude, roubo de propriedade digital, assédio, difamação, injúria racial, exploração infantil, hacking, tráfico ilegal, incitação à violência, violação de direitos autorais, cyberbullying, stalking, falsificação de identidade, pedofilia, sabotagem, roubo de identidade, e até terrorismo virtual.

Em 2022, o Ministério da Justiça e da Segurança Pública anunciou a realização bem-sucedida do primeiro mandado de busca e apreensão dentro do metaverso, como parte da quarta fase da "Operação 404", destinada a combater a pirataria digital. A operação em conjunto com a Polícia Civil de 11 estados resultou em 30 mandados de busca e apreensão contra suspeitos de compartilhar conteúdo protegido por direitos autorais. Onze pessoas foram presas, 266 sites ilegais foram desativados no Brasil, 53 no Reino Unido e seis nos EUA. Além disso, 700 aplicativos de streaming e 461 de música foram bloqueados devido

a possíveis ameaças à segurança dos usuários. A ação também identificou 300 aplicativos com intenção de roubar dados pessoais dos usuários (COINTELEGRAPH, 2022).

Apesar do caso bem sucedido, é predominante os casos em que os indivíduos não são responsabilizados no final. A polícia ainda enfrenta muitos desafios para lidar com crimes no metaverso, devido à novidade e complexidade desse ambiente, a rapidez das atividades criminosas e a necessidade de recursos especializados.

Um caso que ficou mundialmente conhecido e que pode servir de exemplo para entender a nova gama de direitos que podem ser violados com a inovação das tecnologias, mais especificamente dizendo, do metaverso, é o caso de Nina Jane Patel, uma psicoterapeuta inglesa de 43 anos, que revelou que seu avatar na plataforma de realidade virtual da empresa Meta (antiga Facebook) foi vítima de abuso sexual. Ao criar um avatar com características semelhantes às suas para fins de pesquisa no metaverso, ela foi rapidamente abordada e assediada por quatro avatares masculinos. O incidente foi relatado em uma entrevista ao "Universa", do UOL.

Apesar da psicoterapeuta não ter sido afetada fisicamente no mundo real, condutas como essa com certeza promovem consequências emocionais traumatizantes, já que universo é criado exatamente com o intuito de passar uma experiencia de sensações que vivemos fora do mundo físico.

Esses crimes são facilitados pelas interações virtuais, exigindo legislação específica e colaboração global para abordá-los de maneira eficaz e equilibrar a liberdade digital com a responsabilidade legal.

7. INEFICÁCIA DA LEGISLAÇÃO FRENTE AOS CRIMES CIBERNÉTICOS

Com o avanço da tecnologia e o crescimento da internet, surgiram novas formas de interação e oportunidades em diversas áreas, mas também trouxeram consigo uma série de desafios, especialmente no que diz respeito à segurança online. Os crimes cibernéticos tornaram-se uma ameaça cada vez mais preocupante, afetando indivíduos, empresas e até governos. No entanto, apesar do esforço para combatê-los, a legislação de crimes cibernéticos enfrenta inúmeros problemas que dificultam sua eficácia, já que existe uma

carência de normas ou tipos, sobrando muitas vezes para o Código Penal, enquadrar alguma conduta.

> Temos uma mistura explosiva no Brasil, que é a falta de educação, de formação para as crianças e jovens, com uma legislação que prevê penalidades brandas para os crimes de estelionato, tipo no qual é enquadrada a maioria dos ilícitos praticados no mundo digital (ANTONIOLI, 2023).

Um dos principais desafios é a velocidade com que as ameaças cibernéticas evoluem. Os criminosos cibernéticos estão sempre desenvolvendo novas técnicas e para burlar as medidas de segurança em sistemas e redes. A legislação, no entanto, geralmente é mais lenta para se adaptar às mudanças tecnológicas, o que resulta em lacunas que os criminosos podem explorar.

Alex Neder, advogado criminalista e consultor jurídico, afirma de forma impetuosa quanto a elaboração de Lei que não satisfazem por completo a necessidade jurídica nos tempos atuais:

> Enquanto se perdurar essa lamentável situação, teremos leis ineficazes e ineficientes como esta, que não protegem a sociedade e nem dão a segurança jurídica necessária, e estaremos sempre insatisfeitos, com o sentimento de impunidade e ausência de proteção, como se nossas instituições não funcionassem, e não funcionam mesmo, com instrumentos legislativos que nascem com sérias deficiências que comprometem quase por completo seu objetivo e eficácia (NEDER, 2013).

Em 2022, foi conduzida uma pesquisa pela empresa de soluções em segurança cibernética, Fortinet, realizada pelo laboratório de inteligência e ameaças, FortiGuard Labs, e a mesma constatou que no primeiro semestre de 2022, o Brasil testemunhou um alarmante aumento de 94% nas tentativas de ataques cibernéticos direcionados a empresas, totalizando 31,5 bilhões de registros. Em comparação ao mesmo período do ano anterior, que contabilizou 16,2 bilhões de tentativas (CNN BRASIL, 2022). Esse crescimento representa uma clara indicação da crescente sofisticação dos ataques virtuais com o passar do tempo.

Portanto, sem leis específicas para crimes cibernéticos, podem haver lacunas na legislação que não abrangem adequadamente as atividades criminosas no ambiente digital. Isso pode permitir que criminosos se aproveitem de brechas legais e evitem ser responsabilizados.

A resposta para o problema se encontra na adaptação jurídica para tutelar os direitos dos usuários virtuais resultando na diminuição e consequentemente na abolição de penalidades por equiparação de crimes no mundo real, já que isso fere a proporcionalidade entre as condutas e as devidas punições.

> Ambas as modalidades são graves e demandam resposta estatal, todavia, para fins de segurança jurídica, proporcionalidade e até razoabilidade, melhor do que formalmente equipará-las seria a criação de tipo penal específico ao cenário virtual (FORZENIGO, 2022).

8. OUTROS DESAFIOS ENFRENTADOS NO COMBATE A CIBERCRIMINALIDADE

Os crimes cibernéticos se tornam ainda mais complexos devido ao fato de que os criminosos muitas vezes atuam em diferentes países, tornando difícil a cooperação entre as autoridades para investigá-los e responsabilizá-los. Isso pode impedir o avanço das investigações e dificultar a punição dos infratores.

No que se refere a territorialidade dos crimes virtuais, não temos no Brasil, legislação que tipifique o tema, portanto, a luz do art. 6° do Código Penal Brasileiro, adotamos a teoria da ubiquidade, ou seja, o local do crime pode ser definido onde ocorreu a ação ou omissão ou onde se produziu ou deveria produzir os atos de ataque ao servidor ou sistema informático, tendo que se considerar vários fatores para a definição da competência em casos de crimes fora do país.

Outro desafio é a dificuldade de atribuir responsabilidade aos criminosos. O anonimato proporcionado pela internet e o uso de tecnologias para ocultar a verdadeira identidade tornam difícil identificar os criminosos e produzir as provas necessárias. Isso pode levar à impunidade e à sensação de que não há consequências reais para os atos criminosos cometidos online.

> Nota-se, que a condenação do réu está condicionada à comprovação da autoria e da materialidade do crime, ou seja, quando se tem certeza que o indivíduo cometeu o crime. Dessa forma, caso não haja a obtenção desses dois requisitos, poderá o juiz absolver o réu por faltas de provas. Um dos primeiros desafios que Ministério Público encara ao começar uma investigação, se dá principalmente na obtenção dessas provas (REIS, 2021).

Além disso, a falta de conscientização pública sobre os crimes cibernéticos e medidas preventivas também contribui para a vulnerabilidade da sociedade. A educação e o treinamento em segurança cibernética são essenciais para aumentar a conscientização e proteger os indivíduos contra ataques.

Vejamos o que fala Patrícia Peck Pinheiro:

> De maneira geral, podemos dizer que é essencial a conscientização das pessoas com relação ao uso da rede e das ferramentas tecnológicas para mitigar riscos. Isso porque a maioria dos usuários nasceu em uma era analógica e não está familiarizada com os riscos que o uso inadequado dessas ferramentas pode causar, como, por exemplo, deixar o computador do trabalho desbloqueado, com a senha de e-mail gravada, e alguém mandar um e-mail como se fosse você. Por isso acreditamos que educar é essencial (PINHEIRO. 2021, p. 229).

Uma questão adicional é a crescente sofisticação das ferramentas e tecnologias usadas pelos criminosos. Ataques como o ransomware e phishing se tornaram cada vez mais comuns e de alto impacto. As autoridades precisam enfrentar essas ameaças com recursos adequados e pessoal treinado, mas nem sempre isso é viável.

9. CONCLUSÃO

O avanço da era digital trouxe uma infinidade de comodidades e progressos tecnológicos que transformaram totalmente nossa forma de viver. Entretanto, em meio as vantagens, surgiram alguns desafios, e os crimes cibernéticos aparecem como um dos problemas mais preocupantes e complexos que a sociedade enfrenta. Apesar dos esforços para implementar legislações que lidem com essas ameaças virtuais, ainda nos deparamos com a ineficácia da Lei em proteger efetivamente os cidadãos dos perigos do universo digital.

Os delitos cibernéticos englobam várias atividades ilícitas, desde o roubo de dados e ataques a sistemas de informação, até fraudes eletrônicas e disseminação de conteúdo malicioso, causando danos incalculáveis a outros indivíduos, afetando tanto suas finanças quanto suas vidas pessoais e profissionais.

Uma das principais razões para a ineficácia da lei no combate aos crimes cibernéticos é a rapidez com que os criminosos se adaptam e melhoram suas táticas. A evolução veloz da tecnologia coloca os cibercriminosos constantemente à frente, explorando novas fraquezas e métodos para escapar do alcance da justiça.

A legislação muitas vezes se esforça para acompanhar essas mudanças constantes, deixando brechas que os infratores exploram.

Ademais, a pena frequentemente não corresponde à gravidade dos crimes cibernéticos. As punições podem ser leves, ocasionando no encorajamento dos infratores. A aplicação da lei também pode ser complexa e demorada, o que desestimula denúncias e dificulta a responsabilização dos criminosos.

Para enfrentar os perigos dos crimes cibernéticos, é necessária a colaboração entre todos. Uma legislação mais ampla e atualizada, investimentos na tecnologia de segurança, educação pública sobre o tema e cooperação internacional são fundamentais para fortalecer a proteção contra essas ameaças digitais em constante crescimento. Somente assim poderemos enfrentar de forma efetiva os perigos dos crimes cibernéticos e garantir a segurança de nossa sociedade digital em constante evolução.

REFERÊNCIAS

ANTONIOLI, Philip. **Os Desafios do Enfrentamento aos Crimes Cibernéticos no Brasil.** Disponível em: https://camposeantonioli.com.br/crimes-ciberneticos-no-brasil/. Acesso em: 15 jul. 2023.

BRAMBILLA, Guilherme de Souza. **Crimes Virtuais**. ETIC – Encontro de Iniciação Cientifica; Toledo Prudente Centro Universitário, 2015.

BRASIL ESCOLA, Equipe Brasil. **Internet**. Disponível em: https://brasilescola.uol.com.br/informatica/internet.htm. Acesso em: 11 fev. 2023.

BRASIL, CNN. **Levantamento mostra que ataques cibernéticos no Brasil cresceram 94%.** 19 ago. 2022. Disponível em: https://www.cnnbrasil.com.br/tecnologia/levantamento-mostra-que-ataques-ciberneticos-no-brasil-cresceram-94/. Acesso em: 15 jul. 2023.

BRASIL. Gov. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: https://www.gov.br/mds/pt-br/acesso-a-informacao/lgpd. Acesso em: 2 ago. 2023.

CAPITAL, Carta. **Estupro, assédio, aliciamento: Sem leis claras, metaverso é terreno fértil para crimes virtuais. 19 abr. 2022.** Disponível em: https://www.cartacapital.com.br/carta-capital/estupro-assedio-aliciamento-sem-leis-claras-metaverso-e-terreno-fertil-para-crimes-virtuais/. Acesso em: 10 ago. 2023.

COMPLIANCIE, Tech. **Crimes digitais no Metaverso, segurança e seus desdobramentos legais**. 9 nov. 2022. Disponível em: https://techcompliance.org/crimes-digitais-no-metaverso/. Acesso em: 06 ago. 2023.

CRESPO, Marcelo Xavier de F. **Crimes Digitais**. Disponível em: Minha Biblioteca, Editora Saraiva, 2011.

GARCIA, GABRIELLE. **O que é metaverso? Veja significado e como entrar no universo virtual.** TECHTUDO. 6 mar. 2023. Disponível em: https://www.techtudo.com.br/listas/2023/03/o-que-e-metaverso-veja-significado-e-como-entrar-no-universo-virtual-edsoftwares.ghtml. Acesso em: 5 ago. 2023.

GOTO, MATTHEUS. **O que é metaverso? Entenda a origem do termo e saiba como entrar nesse universo virtual.** EPOCA NEGÓCIOS. 27 abr. 2022. Disponível em: https://epocanegocios.globo.com/Tudo-sobre/noticia/2022/04/o-que-e-metaverso-entenda-origem-do-termo-e-saiba-como-entrar-nesse-universo-virtual.html. Acesso em: 5 ago. 2023.

INFOMONEY. **METAVERSO: tudo sobre o mundo virtual que está chamando a atenção dos investidores.** 8 nov. 2022. Disponível em: https://www.infomoney.com.br/guias/metaverso/. Acesso em: 5 ago. 2023.

JOBIM, Caio. **Crimes virtuais: Justiça brasileira cumpre mandado no metaverso e plataforma VR da Meta tem denúncia de abuso sexual.** 29 jun. 2022. Disponível em: https://br.cointelegraph.com/news/virtual-crimes-brazilian-justice-fulfills-arrest-warrant-in-the-metaverse-and-british-reports-rape-on-metas-vr-platform. Acesso em: 10 ago. 2023.

KASPERSKY. **O que são crimes cibernéticos? Como se proteger dos crimes cibernéticos.** Disponível em: https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime. Acesso em: 15 abril 2023.

LINS, Bernardo Felipe Estellita. **A evolução da Internet: uma perspectiva histórica**. Cadernos ASLEGIS, 2013.

METRO. **Psicoterapeuta britânica conta que foi vítima de estupro no metaverso: 'O que aconteceu foi real'**. 3 jun. 2022. Disponível em: https://www.metroworldnews.com.br/social/2022/06/03/psicoterapeuta-britanica-conta-que-foi-vitima-de-estupro-no-metaverso-o-que-aconteceu-foi-real/. Acesso em: 06 ago. 2023.

NEDER, Alex. **Crimes na internet, legislação ineficaz**. 8 jan. 2013. Disponível em: https://www.oabgo.org.br/oab/noticias/artigo/08-01-2013-crimes-na-internet-legislacao-ineficaz-por-alex-neder/. Acesso em: 20 jul. 2023.

PINHEIRO, Patrícia P. **Direito Digital**. Disponível em: Minha Biblioteca, (7th edição). Editora Saraiva, 2021, p. 229.

REIS, CAIO. JUSBRASIL. **Crimes virtuais: Uma análise acerca da (in) eficácia da legislação e os desafios de sua persecução penal.** 31 maio 2021. Disponível em: https://www.jusbrasil.com.br/artigos/crimes-virtuais-uma-analise-acerca-da-in-eficacia-da-legislacao-e-os-desafios-de-sua-persecucao-penal/1220973039. Acesso em: 15 jul. 2023.

ROCK CONTENT. **Conheça a história da Internet, sua finalidade e qual o cenário atual.** Disponível em: <https://rockcontent.com/br/blog/historia-da-internet/>. Acesso em: 11 fev. 2023.

SEREC, Fernando E. **Metaverso: Aspectos Jurídicos.** Grupo Almedina (Portugal), 2022. E-book. ISBN 9786556276335. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786556276335/. Acesso em: 09 ago. 2023.

SILVA JUNIOR, Reginald Vieira da. GENOVA, Edivaldo Waldemar. **Os Desafios do Direito Penal Frente aos Crimes Cibernéticos.** Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano. 06, Ed. 12, Vol. 03. Disponível em: https://www.nucleodoconhecimento.com.br/lei/crimes-ciberneticos. Acesso em: 01 jul. 2023.

SOUZA, Thiago. **História da Internet: quem criou e quando surgiu**. Toda Matéria, [s.d.]. Disponível em: https://www.todamateria.com.br/historia-da-internet/. Acesso em: 18 fev. 2023.

WIKIPÉDIA, a enciclopédia livre. **TCP/IP**. Flórida: Wikimedia Foundation, 2023. Disponível em: https://pt.wikipedia.org/w/index.php?title=TCP/IP&oldid=65098324. Acesso em: 14 fev. 2023.