CRIMES CIBERNÉTICOS: suas principais vítimas[1]

CYBER CRIMES: its main victims

Andrielle Horaine Rodrigues Pires[2]
Thais dos Santos Ferreira[3]

Mestre Fernando Emídio dos Santos[4]

RESUMO

O presente artigo discute acerca do crime cibernético e os seus vultosos números de cometimento, bem como os meios utilizados pelos criminosos para a realização desse tipo de delito. Por meio de minuciosas pesquisas concluiu -se que as redes sociais se tornaram a principal ferramenta para a prática de diferentes categorias de crimes, sendo, portanto, importante estabelecer um cronograma que aponte o surgimento dos crimes virtuais e das mudanças ocorridas até o momento. O cibercrime se utiliza, principalmente, de dispositivos eletrônicos, que são sem dúvida o meio mais comum de cometer ilegalidades virtuais, facilitando a prática dessas. Este texto também aborda a facilidade e a liberdade que os dispositivos eletrônicos trazem. Em contrapartida, a tecnologia trouxe algumas inovações e superou muitas outras dificuldades, pois também facilitou, na medida em que proporcionou um ecossistema completamente novo para a implementação de crimes virtuais.

Palavras-chave: punições; vulnerabilidade; internet.

ABSTRACT

In this article, we discuss cybercrime and its significant prevalence, as well as the methods employed in its commission. Through research has led us to the conclusion that social networks have become the primary tool for various categories of cybercrimes, making it imperative to establish a timeline based on our experiences and the changes that have transpired thus far. Cybercrime predominantly involves electronic devices, which are undoubtedly the most common means for carrying out virtual crimes, thereby facilitating their perpetration. We also delve into the convenience and freedom that electronic devices offer. Nevertheless, this same perspective has brought about innovations, surmounted numerous challenges, and opened the door to a completely new ecosystem for the execution of virtual crimes.

Keywords: punishments; vulnerability; internet.

---

[1] Trabalho de Conclusão de Curso apresentado à Faculdade de Inhumas FacMais, como requisito parcial para a obtenção do título de Bacharel em Direito, no segundo semestre de 2023

[2] Acadêmico(a) do 10º Período do curso de Direito pela Faculdade de Inhumas. E-mail:andriellepires@aluno.facmais.edu.br

[3] Acadêmico(a) do 10º Período do curso de Direito pela Faculdade de Inhumas. E-mail: thaisferreira@aluno.facmais.edu.br

[4] Professor(a)-Orientador(a). Fernando Emídio dos Santos. Docente da Faculdade de Inhumas. E-mail: fernadoe@facmais.edu.br

1 INTRODUÇÃO

Este trabalho se propõe a explorar o complexo universo dos crimes cibernéticos. O foco do estudo se dá, especialmente, nas suas principais vítimas. À medida que a sociedade se torna cada vez mais dependente da conectividade digital, compreender as nuances dessas transgressões é essencial para mitigar os seus impactos e fortalecer as defesas contra ameaças virtuais.

Na elaboração deste trabalho, foram adotadas metodologias fundamentais para que pudéssemos chegar a um resultado satisfatório e transparente para os leitores. Desse modo, o estudo aqui fez uso de artigos científicos e revisão da legislação vigente, o que inclui a Lei Seca e o Código Penal comentado. Além disso, foram essenciais para o tema abordado buscar fontes com credibilidade científica, como websites de notícias reconhecidos, com o objetivo de enriquecer a perspectiva desenvolvida nesta pesquisa.

A obra Manual de Metodologia Científica, dos autores e organizadores, Neves e Domingos, retrata brevemente a importância da metodologia em uma pesquisa, a qual seria:

> O mais importante é conhecer o assunto com uma certa profundidade. Para tal, ler os livros, os manuais e as pesquisas já existentes permitirá formar o conhecimento necessário à abordagem do tema. Como proposta, vá às bibliotecas, aos arquivos de OM, leia periódicos específicos e consulte a internet regularmente, formando um hábito que facilitará o trabalho de pesquisa (Neves; Domingues, 2007, p. 29).

Nessa perspectiva, a metodologia se torna essencial para a pesquisa, pois é ela quem desenha o caminho para conduzir as análises que serão feitas. Mais ainda, ela também ajuda a garantir a validade e a fornecer confiabilidade aos resultados. Por fim, é válido dizer que a metodologia instrumentalizada permite que novos pesquisadores avaliem e construam novos trabalhos fazendo uso desse já elaborado.

O crime cibernético pode ser conceituado como atividades criminosas que envolvem o uso de computadores, aparelhos móveis e outros dispositivos eletrônicos para a prática de ações criminosas. Na maioria das vezes os objetivos da ilicitude são para prejudicar sistemas, aplicar golpes, o que, na grande maioria dos casos, causa prejuízo às vítimas.

A internet tem sido uma ferramenta de grande porte para o cometimento de crimes de diversas categorias, e é importante relacionar uma linha do tempo em relação às experiências e às modificações vividas até os dias atuais.

O desenvolvimento tecnológico dos crimes cibernéticos tem acompanhado o avanço da tecnologia. Os criminosos fazem uso de técnicas cada vez mais sofisticadas, como phishing, ransomware e ataques da engenharia social para obter informações confidenciais, causar danos e obter benefícios financeiros ilícitos. De igual maneira, a segurança cibernética também tem evoluído para combater essas ameaças, algumas ações são as criptografias, a autenticação de dois fatores e a análise de comportamento.

> No artigo na qual trata-se das principais nuances dos crimes cibernético diz: Acredita-se que os crimes cibernéticos vêm sendo praticados no mundo por mais de cinco décadas, desde as primeiras referências até os dias atuais, propagando e se desenvolvendo conforme a globalização dessa nova era

> digital. Segundo Jesus: “Para a doutrina internacional, os crimes virtuais tiveram início na década de 1960, quando foram identificadas as primeiras referências sobre o tema, cuja maior parte foi de delitos de alteração, cópia e sabotagem de sistemas computacionais. ” (Vieira; Fernandes, 2017, p.2).

De acordo com dados da autora Denise Pereira Otsu, a década de 1970 foi o ano que surgiu um dos primeiros casos de crimes cibernéticos, com destaque para práticas como o hacking e a fraude de cartões de crédito. Esse foi o momento no qual se iniciou a caracterização do crime. Já a década de 1980 foi o ano que começou a se popularizar o uso de computadores pessoais e de redes, ampliando, concomitantemente, os crimes cibernéticos, com invasões a sistemas e, também, com a disseminação de vírus que, inclusive até os dias de hoje é bastante comum.

Na década de 1990 houve um crescimento exponencial da internet, emergindo também o comércio eletrônico, tal contexto possibilitou aumento dos crimes cibernéticos como o roubo de identidade, as fraudes on-line e ataques a websites. O ano de 2010 é marcado pela expansão dos crimes cibernéticos, o que inclui ransomware, ataques a engenharia social em larga escala para violar dados em grande escala, com o objetivo de afetar empresas e indivíduos em todo o mundo.

O ano de 2020 segue com a continuação do crescimento dos crimes cibernéticos, com ênfase na exploração de vulnerabilidades dos dispositivos, com aumento do uso de criptomoedas para atividades ilegais, dando espaço para novas práticas criminosas, como a deepfakes, que é uma tecnologia usada para a criação de vídeos fakes, porém reais, simulando situações fake e ataques baseados em inteligência artificial. (Otsu,2023, pg. 15,)

Até o momento atual as redes sociais têm tomado grande proporção em relação à prática desses crimes, o fim é sempre para obter vantagens ilícitas ou até mesmo para prejudicar a imagem e proferir ofensas a terceiros. Ao mesmo tempo que a internet proporciona um universo de informações, facilidades e até mesmo serve como meio de sustento de pessoas pelo mundo todo, ela também tem ultrapassado limites, o que culmina na abertura de espaço para criminosos.

Os crimes cibernéticos trazem vários problemas, como plágio, invasão a dispositivos informáticos, exposição, delitos contra a hora, apologia ao crime, estelionato, entre outros. Assim, existe uma crescente disponibilização de dados pessoais dos usuários na internet e, também, hackers à disposição. Dessa forma existem crimes próprios e crimes impróprios.

A doutrina brasileira classifica os crimes cibernéticos como “delito de natureza formal, posto que se consumam no momento da prática da conduta delitiva, independente da ocorrência do resultado naturalístico”. É possível pensar na necessidade de uma melhoria na lei específica para os crimes cibernéticos.

Assim, ao transitar por toda a evolução dos crimes cibernéticos, desde a década de 1970, torna-se evidente a evolução constante dessas ameaças ao longo dos anos. Desde os primórdios da computação, até os dias atuais, testemunhamos uma sofisticação crescente nas táticas empregadas pelos criminosos digitais. Esta evolução destaca a necessidade urgente de abordagens adaptativas e colaborativas na segurança cibernética juntamente com a educação digital.

2 ESPÉCIES E DENOMINAÇÕES DO CRIME VIRTUAL

Quando se trata de crimes na internet existem vários termos para que se referiram a eles, a título de exemplo: são os “crimes digitais”, os “crimes cibernéticos”, os “crimes eletrônicos”, os “crimes informáticos” dentre outras nomenclaturas. O assunto de crime na internet ainda deixa em aberto lacunas a serem preenchidas e esclarecidas, pois há criminosos anônimos que encorajam os outros ainda mais. Assim, alguns dos órgãos da Segurança Pública que são responsáveis pela investigação criminal desse tipo de delito são a Polícia Civil e a Polícia Federal.

Os crimes virtuais não se baseiam apenas em rede mundial de computadores, mas também em atos e em omissões que giram em torno dessa massa de informações no qual tem uma vítima prejudicada, os prejuízos podem ser de ordem patrimonial ou não, trazendo à tona um problema que ainda não existe uma pena razoável e explícita.

De acordo com Túlio Lima Vianna, há classificações que desenvolvem o *Malwares*, “*Crackers* de sistemas- piratas que invadem computadores ligados”, “*Crackes* de programas- piratas que quebram proteções de *software* cedido a título de demonstração para usá-los por tempo indeterminados, como se fosse cópias legítimas”, “*Phreakers*- piratas especialistas em telefonia móvel ou fixa”, “Desenvolvedores de vírus, *worms* e *trojans*- programadores que criam pequenos softwares que causam algum dano ao usuário”, “Piratas de programas- indivíduos que clonam programas, fraudando direitos autorais”, “Distribuidores de *warez*- *webmasters* que disponibilizam em suas páginas software sem autorização dos detentores dos direitos autorais” (Viana, 2001, pg. 62).

Ao se observar as classificações subjetivas de Vianna podemos constatar os sujeitos e os motivos, 1-curiosos são pessoas curiosas que querem aprender novas técnicas, não causam danos materiais, fazem espionar e não compartilhar os dados apenas leem e não modificam, podem pertencer a um grupo específico ou ter seu próprio código de ética, 2- pichadores digitais têm como seu principal objetivo serem vistos e reconhecidos, querem se tornar famosos no universo *cyberpunk*, 3- revangistas são funcionários ou ex-funcionários que têm como principal objetivo sabotar a empresa por vingança, frequentemente trabalham na área de TI das empresas, 4- vândalos, suas ações são motivadas pelo simples fato de causar danos às suas vítimas, isso é feito travando o servidor e também deixando-o fora de alcance da internet, 5- espiões atuam de forma confidente para obter informações, 6- ciberterroristas são terroristas digitais, geralmente têm como motivação a política, conseguem informações confidenciais, 6- ladrões têm como objetivo financeiro, ataques a bancos nos quais realizam transferência de fundos bancários, 7- estelionatário se configura também com um objetivo financeiro, pois buscam adquirir números bancários de cartões de créditos que são cadastrados em grandes sites comerciais.

Portanto, cabe salientar que a lei foi criada para combater os crimes e vem enfrentando desafios conforme já descrito, sobre as formas de evolução dos ataques virtuais, e em relação à exigência por uma atualização contínua e mais firme. Isso porque as várias formas de se mover no ambiente digital demandam medidas mais eficientes, trazendo punições mais severas e proporcionando a proteção de dados no ambiente virtual, edificando a importância de setores públicos e privados para uma melhor visão de como enfrentar esses desafios da progressiva evolução tecnológica.

3 LEI 12.737 DE 30 DE NOVEMBRO DE 2012 (LEI CAROLINA DIECKMANN)

A Lei específica para os crimes cibernéticos, é conhecida como “Lei Carolina Dieckmann”, mas não trata do crime em espécie. A lei foi criada e desempenha o seu papel. Ela surgiu a partir de uma vítima, figura pública, que teve as suas imagens pessoais divulgadas, tencionando uma defesa própria, os restantes dos delitos se baseiam no efeito danoso. Mas a realidade é que, embora a lei esteja ativa, para essas infrações, há ainda falhas na competência para julgar e para encontrar o infringente, de acordo com as Leis Nº 12.735/12 e 12.737/12

> LEI Nº 12.735 - Art. 1 º Esta Lei altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.(...)Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.Art. 5 º O inciso II do § 3o do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:(...)II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio; (Brasil, 2012).

Como já colocado sobre a lei Carolina Dieckmann, ela se origina a partir de um fato que aconteceu com a atriz Carolina Dieckmann, após ter as suas fotos íntimas vazadas na web. Esse ato criminoso gerou ameaças e extorsões na vítima para que suas imagens não fossem divulgadas. Então a lei criminaliza vândalos que invadem dispositivos eletrônicos para a divulgação de dados pessoais não autorizados, a mesma norma está em vigor há 10 anos. Caso condenado, o infringente é sentenciado a uma pena de reclusão, de 6 meses a 2 anos, e multa.

> Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.Art. 2º O Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:“Invasão de dispositivo informático Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico. § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. § 4º Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. § 5 º

> Aumenta-se a pena de um terço à metade se o crime for praticado contra: I - Presidente da República, governadores e prefeitos; II - Presidente do Supremo Tribunal Federal; III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal." (Grifo nosso)"Ação penal Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos (Brasil, 1941).

Portanto, trata-se de uma Lei cujo fim é combater delitos virtuais, como a distribuição de informações pessoais e a violação de dispositivos eletrônicos. A lei tem como meta manter a segurança e a privacidade dos cidadãos na internet para que os seus dados não sejam compartilhados indiscriminadamente na web. Assim, é preciso lidar com pessoas na internet com tantas informações trazidas por elas mesma, a própria pessoa se colocando em risco por não saber sobre hackers, que, meticulosamente, podem até serem instalados em seus computadores com um simples link, ou, também, através de sites que as pessoas desconhecem a procedência, há vítimas mais vulneráveis como os jovens e os idosos.

A Lei se compara com a Teoria Tridimensional do Direito, trazida pelo jurista Miguel Reale, que gira em torno de 3 paradigmas: o valor, a norma propriamente dita e o fato jurídico.

> "O Direito não é apenas a norma ou a letra da lei, pois é muito mais do que a mera vontade do Estado ou do povo, é o reflexo de um ambiente cultural de determinado lugar e época, em que os três aspectos – fático, axiológico e normativo – se entrelaçam e se influenciam mutuamente numa relação dialética na estrutura histórica". (Reale, 2003, p. 85)

Ao comparar a lei, ela retrata a ocasião vivida, a ação que levou a criação de normas que visam a proteger ao se tratar da circunstância vivida em sociedade, simboliza o ocorrido, no qual o nome da atriz se tornou o nome em lei , por conta do direito e da influência em sociedade que a atriz tem.

3.1 Ineficácia da lei carolina dieckmann

Ao se referir a um crime sancionado no ano de 2012 no Brasil, no qual aborda sobre as invasões nos dispositivos digitais e a divulgação de dados pessoais sem o consentimento. Portanto, existem dificuldades para a eficácia da aplicação da lei, como por exemplo os obstáculos para punir e rastrear os invasores, que estão à espreita, assim também há a necessidade de atualização da legislação em decorrência do avanço tecnológico.

O que a norma visa é o aperfeiçoamento para proteger as vítimas por meio de uma punição eficaz para os infratores. Um exemplo de crime é o que consta no Art. 171 do CP, o qual trata do crime de espionagem, que tem como finalidade obter vontades sobre a vítima, através de chantagens.

Dessa forma, para uma melhor aplicabilidade do dispositivo legal, a legislação deve revisar as melhorias, por via de aprimoramento para garantir a todos segurança e uma lei eficaz. Há alguns problemas identificados, tendo em vista que a

celeridade com que a lei foi criada, para casos específicos, houve diversas lacunas e pontos a serem considerados em várias situações que não foram pensadas. Além disso, é preciso considerar a velocidade em como a tecnologia está avançando, fator que acaba gerando uma legislação obsoleta, porque novas formas de crimes surgem a cada evolução, o que também gera maior dificuldade para o rastreamento e identificação dos criminosos, impedindo a aplicabilidade da lei em si.

A tecnologia vem avançando a cada dia, e existem pessoas que são leigas para os dispositivos, como as redes sociais, ou não têm recursos ou até mesmo entendimento se realmente precisam ser suficientes para terem programas que protejam os seus dados, exemplo de antivírus ficando, ficando assim à mercê dos criminosos.

O professor Ferreira refere-se à Lei na sua ineficaz e ao mesmo tempo normalizam, tais ações:

> Por isso temos a sensação de impunidade, sendo um atrativo muito forte para o crescimento desse tipo de delito. As ameaças podem ser tanto por meio de monitoramentos não autorizados do sistema como a (DEEP WEB), como através de ataques mais sofisticados por hackers. (Ferreira, 2015, p.32).

> A ineficácia na normatização nos crimes virtuais, ainda não foi suprida para um combate efetivo contra esses delitos, por isso diante dessa dificuldade encontrada, ou até mesmo pela natureza taxativa do Código Penal, há uma grande impossibilidade da aplicação da analogia nos crimes virtuais. (Ferreira, 2015, p.44).

Assim, as punições para os crimes virtuais veem sendo desenvolvidas com acompanhamento, de acordo com o delito cometido, para uma punição adequada e justa. Ao tratar desse crime, que ainda está em evolução e que precisa de uma melhoria, pois escancara o que deve ser melhorado para tornar a eficácia mais justa, punindo quem o comete.

Segundo a autora Fernanda Barbosa Moura, o crime virtual trata de condutas típicas, ilícitas e culpáveis, entre pessoa física ou jurídica pelo mundo virtual, o que visa a um todo:

> Conclui-se, portanto, que crime virtual é a conduta típica, ilícita e culpável que preenche os pressupostos de crime ou de contravenção penal, ocorrida com dolo ou culpa, perpetrada por pessoa física ou jurídica por meio da informática, seja na Rede Mundial de Computadores ou não, e que vai de encontro à segurança do sistema informático, o qual deve observar a integridade, desimpedimento e a privacidade de indivíduos e entidades. (Moura, Fernanda Barbosa, 2019, p.8).

4 TIPIFICAÇÃO NO ORDENAMENTO JURÍDICO

Há punições para os crimes praticados no meio virtual. As penalidades podem variar de acordo com a gravidade do crime e a legislação vigente do país em questão. Em geral, as punições podem incluir multas, prisões e restituições pelos

danos causados às vítimas. Além disso, muitos países têm leis específicas para combater o crime cibernético como também agências especializadas para investigações desses tipos de crimes.

O artigo 1º do Código penal diz o seguinte:

> " Art. 1º- Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal" (Brasil, 1940).

Tendo em vista que, alguns crimes que muitas vezes não são vistos pelas pessoas, impondo assim, medidas provisórias referentes a essas práticas de delinquência para que os seus autores possam ser punidos com pena e detenção. Essas ações tendem a fornecer uma proteção para pessoas mais vulneráveis, as mesmas que não percebem como os seus dados pessoais podem estar desprotegidos. Esse crime é abordado no ordenamento jurídico brasileiro, que traz medidas para lidar com esse tipo de ato no meio virtual.

O Princípio da Legalidade é fundamental no sistema jurídico, desse modo, é imprescindível que a lei seja clara e específica sobre a constituição de um crime antes de ser designada uma punição a alguém.

O assédio sexual, que é bastante comum nas redes sociais, tem sua punição especificada no artigo 216-A do Código Penal:

> Art. 216-A. Constranger alguém com o intuito de obter vantagem ou favorecimento sexual, prevalecendo-se o agente da sua condição de superior hierárquico ou ascendência inerentes ao exercício de emprego, cargo ou função. Pena detenção, de 1 (um) a 2 (dois) anos (Brasil, 1940).

Dessa maneira, o artigo realça a seriedade no modo como deve ser tratado criminalmente alguém que viole os dados pessoais de um outro. Os dispositivos penais têm como objetivos, prevenir a integridade e a credibilidade das redes sociais, colocado como primordial para a liberdade individual. Então é essencial que a legislação evolua de acordo com a tecnologia.

Alguns dos casos mais comuns de assédio sexual no meio virtual incluem o envio não solicitado de imagens explícitas, mensagens com teor sexual indesejadas, chantagem sexual (conhecida como "sextorsão";), criação de perfis falsos para assediar, compartilhamento não consensual de imagens íntimas (conhecido como "pornografia de vingança") e comentários ofensivos de natureza sexual.

Trata-se de um tipo criminal que uma parte superior age com interesse, com uma parte mais vulnerável para obter vantagens sexuais, sendo assim a injuriada dar queixa na polícia por difamação ou injúria.

A Lei n° 7.716/89, juntamente com o artigo 140 do CPB, no que refere aos crimes de cor e de raça, trazem a distinção que ocorre no mundo virtual, demonstrando que há que existe lei para que essa infração seja punida, de acordo com o artigo 20;

> Art. 20. Praticar, induzir ou incitar, pelos meios de comunicação social ou por publicação de qualquer natureza, a discriminação ou preconceito de raça, por religião, etnia ou procedência nacional. c/c Art. 140. Injuriar alguém, ofendendo-lhe a dignidade ou o decoro. (...) § 3º Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência Não existe uma lei especifica ao se tratar de Mercado Negro, vai se referir na distribuição de conteúdo ilícito, deixando claro normas estabelecidas em lei como consta no art.33; (Brasil, 1940).

> Art. 33. Importar, exportar, remeter, preparar, produzir, fabricar, adquirir, vender, expor à venda, oferecer, ter em depósito, transportar, trazer consigo, guardar, prescrever, ministrar, entregar a consumo ou fornecer drogas, ainda que gratuitamente, sem autorização ou em desacordo com determinação legal ou regulamentar. (Brasil, 1940)

Ao se tratar de Pornografia Infantil, a lei 8.069/90 no artigo 214-A, visa conter a produção, a destruição e a venda de conteúdo impróprio;

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente; Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa (Brasil, 1990).

A espionagem ganhou relevância no Brasil no ano 2013, ano qual um colaborador dos Estados Unidos conseguiu informações de vários países, incluindo o Brasil, tendo essas informações vazadas na web, fixadas na Lei. Nº 7.170 de 14 de dezembro de 1983;

> Art. 13 – Comunicar, entregar ou permitir a comunicação ou a entrega, a governo ou grupo estrangeiro, ou a organização ou grupo de existência ilegal, de dados, documentos ou cópias de documentos, planos, códigos, cifras ou assuntos que, no interesse do Estado brasileiro, são classificados como sigilosos. Pena: reclusão, de 3 a 15 anos.Parágrafo único – Incorre na mesma pena quem – Com o objetivo de realizar os atos previstos neste artigo, mantém serviço de espionagem ou dele participa; II –Com o mesmo objetivo, realiza atividade aerofotográfica ou de sensoriamento remoto, em qualquer parte do território nacional; III – oculta ou presta auxílio a espião, sabendo-o tal, para subtraí-lo à ação da autoridade pública; IV – obtém ou revela, para fim de espionagem, desenhos, projetos, fotografias, notícias ou informações a respeito de técnicas, de tecnologias, de componentes, de equipamentos, de instalações ou de sistemas de processamento automatizado de dados, em uso ou em desenvolvimento no País, que, reputados essenciais para a sua defesa, segurança ou economia, devem permanecer em segredo. (Brasil, 1983)

O crime de estelionato, que também é frequentemente cometido através do meio virtual, tem como conceito a caracterização de ações fraudulentas com a intenção de obter vantagens ilícitas em prejuízo alheio, é uma ação que atenta contra a boa-fé. É por essas razões que há punição adequada no ordenamento jurídico para a prática do crime de estelionato.

O estelionato está previsto no Código Penal Brasileiro em seu artigo 171. Este artigo expõe os elementos e as condições nas quais se configura o crime de estelionato.

> Art. 171 – Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena – reclusão, de um a cinco anos, e multa. (Brasil, 1940).

E quando nos referimos ao da identidade, podemos dizer que são informações retiradas do sistema por malwares, com a probabilidade de aplicação de golpe como extração de dinheiro em contas bancárias e em dados pessoais

roubados, utilizando o próprio CPF da pessoa para fazer compras em sites. Pode acontecer também com as Pessoas Jurídicas, que usufruem de dados da empresa para celebrar negócios, o roubo de identidade consta no artigo 307 do Código Penal;

> Art. 307 - Atribuir-se ou atribuir a terceira falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem: Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave. Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave. (Brasil, 1940).

Portanto, a legislação de crime cibernético desempenha um papel crucial na proteção da sociedade digital, estabelecendo parâmetros legais para lidar com ameaças virtuais. Ao regulamentar atividades ilícitas on-line, as leis visam dissuadir potenciais infratores e fornecer meios eficazes para responsabilizá-los. Contudo, o desafio persiste na adaptação constante dessas leis à evolução rápida da tecnologia, garantindo uma abordagem equilibrada entre a segurança cibernética e a proteção dos direitos individuais. – Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena – reclusão, de um a cinco anos, e multa.

5 A VULNERABILIDADE NO MEIO DIGITAL

A internet é uma grande invenção da humanidade, pois ela tem se reinventado cada vez mais por meio das suas inovações tecnológicas, conhecido como a Era Digital. Os meios de comunicação nos tempos atuais encontram-se cada vez mais no meio digital. Dificilmente se encontra pessoas que não têm acesso a internet. De acordo com os dados do IBGE, 87% dos domicílios localizados no Brasil, estão conectados à internet. Isso demonstra o quanto a população está vulnerável a esse tipo de crime.

A classe idosa é o alvo atrativo no meio digital, infelizmente esse grupo vem se destacando em relação à vulnerabilidade de golpes e de fraudes praticadas no meio intelectual. As pessoas da terceira idade tem buscado se habituar cada vez mais às mais recentes tecnologias. Tal inserção se dá por conta da necessidade em encontrar as pessoas, hoje apenas nos dispositivos e redes sociais.

De acordo com os dados do IBGE, o percentual de idosos (60 anos ou mais) que fazem uso da internet, subiu de 24,7% em 2016 para 62,1 % em 2022. O que se pode extrair desses dados é que essas pessoas menos envolvidas com as tecnologias procuram a internet, através das redes sociais, como um meio de distração e até como uma forma de refúgio.

Os idosos podem ser os mais vulneráveis a crimes cibernéticos devido à falta de familiaridade com a tecnologia, que é o elemento responsável por desenvolver essa habilidade de proteção e conhecimento sobre os perigos. Os criminosos tendem a se passar por parentes próximos ou até mesmo “fingir” ser funcionários ou colaboradores de bancos. Há uma estratégia bem elaborada que os estelionatários acessam dados que possam vitimar pessoas, coagindo-as a depositarem dinheiro ou a facilitar o saque do mesmo.

De acordo com o autor Marcos Antônio Frota Cardoso, a vulnerabilidade dos idosos está relacionada à falta de paciência a qual as pessoas já desenvolveram, o preconceito no qual as pessoas já têm pelo fato de saberem, naturalmente os idosos

possuem uma maior dificuldade para compreender e utilizar os meios tecnológicos. (Cardoso, 2023, p. 9,).

Uma proposta interessante seria oferecer uma educação digital em conjunto com um suporte para ajudar essa classe a se familiarizar com a tecnologia e as suas funções. No presente momento ainda não existem políticas públicas voltadas para auxiliar os idosos com o objetivo de oferecer esse tipo de educação e ensinamento. Além disso, poderiam fornecer auxílio com programas de conscientização, workshops educacionais e campanhas que as auxiliem sobre os riscos on-line, mostrando qual a melhor forma de se proteger.

A privacidade e a segurança dos usuários on-line exigem, não apenas medidas repressivas, mas também uma abordagem preventiva. O que se deveria propor é a conscientização pública sobre práticas seguras na internet e a promoção da cibereducação são peças-chave para construir uma sociedade digital mais resiliente.

Portanto, essa vulnerabilidade das pessoas de terceira idade na internet é um grande desafio e reflete a urgente necessidade de políticas públicas, e também a buscar iniciativas para promover a conscientização e a educação digital como também medidas de proteção. Essas políticas públicas poderiam capacitar os idosos para o enfrentamento dos desafios digitais, promover a inclusão digital, contribuir para uma participação mais ativa e informada na era digital. Essas ações serviriam para garantir que essa parcela da população não fique à margem desses crimes, até serviriam para minar o número alto de vítimas, que tem sido tão frequente.

5.1 Dos desafios na jornada dos influenciadores digitais

O mundo digital atual está vivenciando a era de criadores de conteúdo, conhecidos como “influencers digitais”, e notavelmente isso se expandiu fazendo com que inúmeras pessoas pelo mundo buscassem isso como forma de trabalho e sustento. De modo que esse grupo, diariamente, se torne vítima dos crimes virtuais e, principalmente, crimes contra a honra, por suas exposições excessivas no meio digital. Os crimes mais comuns são a injúria e a difamação, nos quais, na maioria dos casos, as vítimas sofrem com comentários maldosos de crime de racismo, ofensas sobre os seus corpos, algo que atinge também a dignidade e o decoro da vítima. Ambos os crimes estão previstos no rol do código penal:

> Art. 139- Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena -detenção, de três meses a um ano, e multa.
> Art. 140- Injuriar alguém, ofendendo-lhe a dignidade ou o decoro: Pena - detenção, de um a seis meses, ou multa.
> Art. 141 - As penas cominadas neste Capítulo aumentam-se de um terço, qualquer dos crimes é cometido:
> § 2º Se o crime é cometido ou divulgado em quaisquer modalidades das redes sociais da rede mundial de computadores, aplica-se em triplo a pena. (Brasil, 1940).

Os influenciadores digitais tendem a interagir com frequência com os seus seguidores nas suas redes sociais, por razões óbvias, como fortalecer os vínculos, para construir uma comunidade engajada com os esses seguidores, e naturalmente, construir público para apresentar às suas publicidades, campanhas e trabalhos do dia a dia.

Como na grande maioria das vezes, esses influenciadores têm consigo nas redes sociais grandes números de seguidores, pessoas diferentes, opiniões

diferentes umas das outras, acaba que as pessoas pegam muito pesado diversas vezes, e, assim, praticando um crime no meio virtual.

Diante o exposto, o autor Samuel Silva Basilio Soares descreveu em seu artigo sobre o assunto tratado:

> A internet deve ser vista como um ambiente democrático, coexistindo as mais diversas formas de pensamento. Dessa maneira, é um local para o debate das diversas formas e pontos de vistas relacionados a diversos ou determinados assuntos, contudo, cada indivíduo que faz uso da internet deve se responsabilizar por suas opiniões. (Soares, 2016, p. 8).

Lua, de 7 meses de idade. Na matéria apresentada pelo G1 notícias, a influenciadora, juntamente com seu esposo, explicou como esses ataques aconteceram através de seu instagram. Viih Tube conta que a filha sofreu uma onda de xingamentos, e já vem sofrendo desde quando tinha apenas 3 meses de idade, nos comentários as pessoas sofrem xingamentos.

O casal compartilhou na matéria um dos vários comentários ofensivos desferidos contra a sua filha, lido por eles:

> “Do que adianta nascer rica, mas ser obesa?’. ‘Tinha tudo pra ser linda, mas é obesa. Tadinha’. ‘Ela vai explodir (risos)’. Esses comentários estão na foto de um bebê de sete meses”, diz Eliéser, esposo de Viih Tube e pai da Lua.” (G1, 2023)

Desse modo, as pessoas que fizeram esses comentários, ofendendo, xingando e praticando ataques contra a criança, praticaram o crime contra a honra, que tem previsão nos artigos 138, 139 e 140 do Código Penal. Portanto, essas pessoas devem responder pelo crime cometido. É importante mencionar, que o cometimento de crimes contra a honra no meio virtual tem a sua pena aplicada o triplo da pena inicial.

Assim, no panorama atual, os idosos e os influenciadores digitais enfrentam desafios únicos no cenário do crime cibernético. Os idosos, muitas vezes menos familiarizados com tecnologia são alvos frequentes de golpes on-line, exigindo estratégias educacionais e de conscientização específicas para protegê-los.

No caso dos influenciadores digitais, cuja presença na internet é marcante, a ameaça se manifesta de maneiras diversas, desde ataques diretos às suas contas bancárias, até às formas mais sutis, como apropriação indevida de identidade.

6 CONSIDERAÇÕES FINAIS

É importante destacar a urgente necessidade de políticas públicas para a proteção de todos, de modo mais exclusivo para a classe mais vulnerável, como já adiantado, frente à crescente ameaça e exposição a riscos de se tornarem vítimas desses crimes praticados no meio virtual.

Assim, é crucial não apenas reprimir atividades criminosas, mas também investir em educação digital para os idosos, promover conscientização entre os influenciadores e desenvolver regulamentações que abordem as lacunas existentes na proteção cibernética desses grupos específicos. Dessa forma, podemos construir uma sociedade digital mais resiliente e equitativa.

Este artigo demonstra uma compreensão clara das complexidades e dos desafios do combate ao cibercrime, com foco nas suas principais vítimas: os idosos e os influenciadores digitais. Ao longo do estudo, foi destacada a vulnerabilidade desses grupos às ameaças digitais, exigindo abordagens concretas e políticas públicas direcionadas.

Uma análise da Lei Carolina Dickman, que representa um modo repressor legal para os crimes cibernéticos no Brasil, revela avanços, mas também aponta para a necessidade de uma adaptação constante diante da evolução das tecnologias e das estratégias criminosas. Embora a legislação seja crucial, não pode ser estática face a um ambiente digital dinâmico.

Foi enfatizada a importância de ações preventivas, tais como programas educativos dirigidos às pessoas idosas e a influenciadores, destinados a aumentar a sensibilização e as capacidades de proteção desses grupos. Além disso, estabelecer e melhorar mecanismos de inspeção e de resposta rápida é fundamental para mitigar o impacto do cibercrime.

A Lei Carolina Dieckmann representa um passo importante no sentido da criminalização da atividade ilícita nas redes, mas a sua eficácia está intrinsecamente ligada à capacidade de adaptação às mudanças tecnológicas. A investigação destaca a necessidade de revisão regular para garantir que a legislação permaneça relevante e eficaz num contexto de crescente sofisticação do crime cibernético.

No geral, o exposto destaca a importância de uma abordagem multidisciplinar que reúna diferentes esforços, de setores diversos, para combater o cibercrime. Ao aumentar a sensibilização, implementar medidas preventivas e reforçar a legislação existente, podemos aspirar a um ambiente digital mais seguro, mais inclusivo e resiliente para todos os cidadãos, independentemente da idade ou do estatuto on-line.

Conclui-se portanto, enfatizando a necessidade urgente de uma abordagem abrangente que envolva departamentos governamentais, empresas de tecnologia, sociedade civil e a própria comunidade digital. Somente através deste tipo de cooperação poderemos construir um ambiente digital mais seguro, mais justo e mais resiliente para todos. Este trabalho contribui para uma compreensão mais ampla desse fenômeno em evolução, explorando as lacunas e desafios atuais presentes.

REFERÊNCIAS

ALMEIDA, Jessica de Jesus. **Crimes cibernéticos**. 2015. 2 v. Curso de Direito, Universidade Tiradentes, Aracaju, 2015.

BRASIL. LEI 14.155/2021: promove alterações nos crimes de violação de dispositivo informático, furto e estelionato. Dizerodireito.com.br.

BUENO, James Nogueira. **Crimes na internet** , 2023. p.02.

CRUZ, DIEGO; RODRIGUES, JULIANA. Crimes cibernéticos e a falsa sensação de impunidade. **Crimes cibernéticos,** Garça - SP, ano 2 018, n. 13, p. 1-18, 8 jan.

MAIA, Fernanda Barbosa. **Desafios do direito na era da Internet**: UMA BREVE ANÁLISE SOBRE OS CRIMES CIBERNÉTICOS. 2019. 7 f. Curso de Direito, Universidade Cândido Mendes, Barreiras, 2019. Cap. 4.

MASSON, Cleber. **Código Penal comentado**. 5ª ed. São Paulo: Método, 2017.

NEVES, Eduardo Borba; DOMINGUES, Clayton Amaral. **Manual de metodologia da pesquisa científica**. **Rio de Janeiro: EB/CEP**, p. 204, 2007.

NUCCI, Guilherme de Souza. **Código Penal Comentado**. 14ª ed. Rio de Janeiro: Forense, 2014.

POMPEU, Ana Luiza Brandão Calil et al. **Crimes Cibernéticos**: A Ineficácia da Lei Carolina Dieckmann. 2022.

REALE, Miguel. **Teoria Tridimensional do Direito**, p. 85. 5ª ed., Editora Saraiva, São Paulo, 2003.

SOARES, Samuel Silva Basílio. **Os crimes contra honra na perspectiva do ambiente virtual**. Âmbito jurídico, v. 1, 2016.