Revista Multidisciplinar do Nordeste Mineiro, v.04,2024

ISSN 2178-6925

HATERS NAS SOMBRAS: CRIMES CIBERNÉTICOS E A LEGISLAÇÃO BRASILEIRA

HATERS IN THE SHADOWS: CYBER CRIMES AND BRAZILIAN LEGISLATION

Taís Porto Silva

Graduanda do 10º Período do Curso de Direito da Faculdade AlfaUnipac - Teófilo Otoni - MG, Brasil. E-mail: portotais1@gmail.com

Igor do Vale Oliveira

Pós-Graduado em Direito e Processo do Trabalho pela Damásio Educacional, Graduado em Direito pela Faculdade Presidente Antônio Carlos de Teófilo Otoni - MG, Advogado e Docente no Curso de Direito na Faculdade AlfaUnipac de Teófilo Otoni - MG, Brasil

E-mail: igorvale.adv@gmail.com

Resumo

O estudo tem como objetivo versar sobre o crime cibernético, abordando especificamente as pessoas conhecidas como *"haters".* Tendo e vista que a falta de compreensão por parte de muitos do que pode ser considerado sério é agravada pela sensação de impunidade. Ademais, o fato de esse tipo de "*hater*" ser capaz de disseminar ódio rapidamente pela internet, torna-o ainda mais perigoso. Portanto, deve-se enfatizar a prioridade em construir uma fronteira entre discurso de *"true hate"* e liberdade de expressão válida. Nesse sentido, a pesquisa destacou a urgência em aprimorar a legislação vigente e fortalecer as ferramentas de investigação e punição relativas aos criminosos cibernéticos, sobretudo aos *"haters".* Ainda, ressaltou-se sobre a importância da conscientização acerca dos aspectos legais e prejudicais da fala de ódio no espaço virtual. Sendo possível concluir que não é garantida a segurança no ambiente virtual devido à falta de legislação específica do Brasil.

Palavras-chave: Crimes Cibernéticos; *Haters;* Discurso de Ódio; legislação; segurança virtual.

Abstract

The study aims to deal with cybercrime, specifically addressing people known as "haters". Given that the lack of understanding on the part of many of what can be considered serious is worsened by the feeling of impunity. Furthermore, the fact that this type of "hater" is capable of spreading hatred quickly across the internet makes it even more dangerous. Therefore, the priority of building a boundary between "true hate" speech and valid freedom of expression must be emphasized. In this sense, the research highlighted the urgency of improving current legislation and strengthening investigation and punishment tools relating to cyber criminals, especially "haters". Furthermore, the importance of raising awareness about the legal and harmful aspects of hate speech in the virtual space was highlighted. It is possible to conclude that security in the virtual environment is not guaranteed due to the lack of specific legislation in Brazil.

Keywords: Cyber Crimes; Haters; Hate Speech; legislation; virtual security.

ISSN 2178-6925

1. Introdução

O estudo versa sobre os crimes cibernéticos que, infelizmente, tem encontrado no vasto mundo virtual da internet. A sensação de impunidade muitas vezes serve como incentivo para a prática desses delitos, o que leva a refletir sobre os conflitos enfrentados nas investigações e a importância das legislações que buscam abster essas condutas maliciosas, sem, contudo, restringir a liberdade de expressão legítima de pessoa de boa índole.

O objetivo principal da presente pesquisa é analisar a dinâmica dos crimes cibernéticos em um ambiente ainda em construção na sociedade brasileira, o espaço virtual e compreender como se dá o processo de responsabilização dos indivíduos que propagam discursos de ódio, conhecidos como *"haters".*

Para isso, adota-se a metodologia da pesquisa bibliográfica, que conduziu por uma jornada pelas mais diversas fontes, desde doutrinas e jurisprudências até artigos científicos e reportagens, todas essenciais para a nossa investigação.

Ademais, deve-se destacar que o trabalho se divide em três seções. Na primeira, aborda-se sobre a evolução da tecnologia da internet no Brasil, desde seus primórdios até os dias atuais, bem como descreve-se os crimes cibernéticos e revela suas formas mais comuns de ocorrência.

Já na segunda seção, analisa-se sobre o delicado tema do discurso de ódio na internet, examinando as legislações pertinentes em vigor. Por fim, na terceira e última seção, reflete-se sobre os limites da liberdade de expressão no ambiente virtual e discute estratégias para coibir essas práticas criminosas, visando, assim, concluir com êxito este estudo tão relevante.

2. Crimes Cibernéticos

2.1 Breve histórico dos crimes cibernéticos

Primeiramente, faz-se mister ressaltar que a história dos crimes cibernéticos remonta aos primórdios da internet e da computação moderna. Inicialmente, as redes de computadores eram utilizadas principalmente para fins acadêmicos e militares. Com o decorrer do tempo, a internet se expandiu, tornando-se acessível ao público

ISSN 2178-6925

em geral e possibilitando novas oportunidades para que muitos indivíduos começassem a praticar atividades criminosas.

Em meados dos anos 1970 e 1980, os primeiros casos de crimes cibernéticos envolvendo *hackers* explorando vulnerabilidades e falhas em sistemas de computador surgiram. Um exemplo notável é o caso Morris Worm, um dos primeiros grandes ataques em escala global, ocorrido em 1988, criado por um estudante da Universidade de Cornell, ficou conhecido por afetar aproximadamente 10% dos computadores conectados à Internet na época. Ao longo das décadas seguintes, os crimes cibernéticos evoluíram, surgindo novas formas de crime, como *phishing,* roubo de identidade, *malware* e ataques DDoS.

Já no Brasil, os crimes cibernéticos representam uma preocupação crescente, levando à promulgação de leis específicas, como a Lei Carolina Dieckmann, que visa proteger a privacidade e informações pessoais dos cidadãos no mundo digital. E o Marco Civil da Internet, que estabelece princípios, direitos, deveres, e também garantia para o uso da internet no Brasil.

A tecnologia passou, então, a representar progresso, riqueza, lazer e desenvolvimento. Contudo, o desafio da segurança digital persiste, exigindo constante atualização das leis, estratégias e mecanismos de combate. Portanto, é de extrema importância a constante evolução para lidar com ameaças diante da contínua mudança no âmbito virtual e também no cenário real do mundo.

Falando em cenário, no atual, a comunicação e a transferência de dados são intermediadas pela internet e suas redes conectadas. Destarte, é essencial considerar o impacto da internet nas relações interpessoais e na sociedade como um todo.

De acordo com Wigerfelt, Wigerfelt e Dahlstrand (2015), o avanço da internet é um fenômeno que caracterizou e influenciou vários aspectos da vida social. Por exemplo, ela oferece novas oportunidades para grupos minoritários participarem de debates e ocuparem espaços na esfera pública.

Contudo, o aumento do acesso à internet também tem sido acompanhado pelo crescimento das atividades que propagam discursos de ódio, como mencionado anteriormente. Esses discursos de ódio traz a sensação de perder todos aqueles direitos que são assegurados por lei, já que muitos estão escondidos atrás de perfis *fakes*, titulam a internet uma terra sem restrições e leis eficientes.

No entanto, é importante notar que o Poder Judiciário enfrenta grandes desafios ao investigar e julgar casos de crimes cibernéticos. Esses desafios surgem

mediante ao aumento gigantesco desses crimes, que ocorrem em conjunto com o avanço da tecnologia.

A complexidade desses crimes, que muitas vezes envolvem diferentes países, e a rápida evolução das tecnologias tornam a investigação e o processo judicial uma tarefa difícil para as autoridades judiciais. Além disso, a falta de conhecimento especializado dos profissionais jurídicos em questões relacionadas à tecnologia e à internet também contribui para essa dificuldade.

Como resultado, existe uma lacuna entre a demanda crescente por justiça em casos de crimes cibernéticos e a capacidade do sistema judiciário de lidar efetivamente com esses desafios.

Imagine que você está navegando em um oceano de crimes cibernéticos, onde os *hackers* estão sempre um passo à frente. O Poder Judiciário, responsável por investigar e julgar esses crimes, enfrenta uma batalha difícil. Os crimes cibernéticos são complicados e muitas vezes envolvem pessoas de diferentes países, o que dificulta ainda mais o trabalho dos juízes.

Além disso, a tecnologia está sempre se desenvolvendo rapidamente, o que torna difícil para os profissionais jurídicos acompanharem todas as novidades. Eles podem não entender completamente como funcionam os ataques cibernéticos ou como coletar evidências digitais. Isso cria um problema, pois há cada vez mais pessoas buscando justiça por crimes cibernéticos, mas o sistema judiciário não consegue lidar com essa demanda.

2.2 Conceito de crimes cibernéticos

Outro aspecto imprescindível para o presente estudo é a compreensão quanto ao aspecto conceitual de crimes cibernéticos, também conhecidos como crimes digitais ou crimes da era da informação, os quais são atividades ilegais que acontecem no âmbito virtual, usando computadores, *smartphones* e *tablets*. Esses crimes têm como objetivo principal comprometer a segurança de informações, causar danos a sistemas, roubar dados pessoais, financeiros ou corporativos, ou realizar atividades fraudulentas.

Além da classificação comum de crimes cibernéticos, que abrange uma ampla gama de atividades ilegais realizadas através de meios eletrônicos, também é possível dividir esses crimes em duas categorias adicionais: próprios e impróprios.

ISSN 2178-6925

Os crimes cibernéticos próprios são aqueles em que o alvo direto é um sistema informático ou seus dados. O objetivo desses crimes é violar a confiabilidade, integridade e disponibilidade desses sistemas. Pense em ataques diretos a computadores, redes ou dados armazenados, por exemplo, quando *hackers* invadem um sistema para roubar informações confidenciais ou distribuir *malware.*

Já os crimes cibernéticos impróprios são condutas ilegais que poderiam ter sido cometidas de outras formas, mas são facilitadas ou aprimoradas pelo uso da tecnologia digital. Um exemplo disso é a fraude *online,* em que os criminosos utilizam a internet e dispositivos eletrônicos para cometer fraudes. Embora a fraude em si não seja exclusiva do ambiente digital, a tecnologia torna mais fácil para os criminosos enganarem as pessoas e realizarem suas atividades ilegais.

Essa distinção entre crimes próprios e impróprios é útil para entender a complexidade dos crimes cibernéticos e como diferentes tipos de atividades ilegais podem ser realizadas no ambiente digital. Ao compreender essas categorias, pode-se ter uma visão mais clara dos desafios que se enfrenta na luta contra os crimes cibernéticos e desenvolver estratégias eficazes para combatê-los.

2.3 Espécies de crimes cibernéticos

Ultrapassada a análise conceitual, faz-se indispensável analisar as espécies de crimes cibernéticos. A primeira espécie pode ser compreendida com um caso hipotético corriqueiro, qual seja, imagine que você está navegando na internet e recebe um e-mail que parece ser de um banco conhecido, pedindo para você fornecer seus dados pessoais, como senha e número de cartão de crédito. Esse e-mail é um exemplo de *phishing,* uma forma de crime cibernético em que os criminosos tentam enganar as pessoas para obter informações confidenciais.

Outro exemplo comum é o *hacking,* em que os criminosos invadem sistemas de computadores para acessar, alterar ou roubar informações. Isso pode acontecer quando alguém invade o computador de uma empresa e rouba dados importantes.

Um tipo de crime cibernético que tem se tornado cada vez mais comum é o *ransomware.* Imagine que você está usando seu computador e, de repente, todos os seus arquivos são criptografados e você não consegue mais acessá-los. Os criminosos por trás do *ransomware* exigem um resgate em troca da chave de descriptografia.

ISSN 2178-6925

Existem também os crimes relacionados à pirataria de *software,* filmes, músicas e outras formas de distribuição de conteúdo protegido por *copyright*. E o crime de invasão de privacidade, que se trata da divulgação não autorizada de trocas de mensagens, dados pessoais e informações íntimas.

Além disso, existem crimes cibernéticos como a difamação *online*, em que as pessoas publicam informações falsas ou prejudiciais sobre alguém na internet, escondidas atrás de perfis *fakes* e até mesmo em seus perfis real nas redes sociais de comunicação. E o *ciberbullying*, em que as pessoas assediam, intimidam ou ameaçam outras pessoas online.

É importante mencionar também a pornografia infantil, um crime cibernético extremamente grave, em que pessoas distribuem, produzem ou possuem material pornográfico envolvendo crianças. Esses são apenas alguns exemplos de crimes cibernéticos, portanto, é essencial estar ciente dos riscos e tomar medidas para proteger-se no mundo digital.

Por derradeiro, ressalta-se que a internet compõe um mundo virtual onde as distâncias físicas não se sobressaem e as pessoas se aproximam, muitas vezes alimentadas pelo sentimento de proteção fornecido pelo anonimato que ela mantém a suas abordagens (Pannain; Pazzella, 2015, p. 28).

Entretanto, essa mesma proteção que facilita o contato e a interação afetiva no global ambiente, propicia as condições para o surgimento de crimes, tendo em vista que muitas pessoas tendem a culpar o sentimento de segurança, a liberdade de impunidade proporcionada pela rede.

3. Crimes cibernéticos no ordenamento jurídico

3.1 Discurso de ódio na internet

Uma preocupação no Brasil é o discurso de ódio na internet, que reflete as dinâmicas globais de intolerância e preconceito amplificadas pelas plataformas *online.* O mundo digital tem sido utilizado no Brasil e em outros lugares para propagar mensagens de ódio com base em raça, gênero, orientação sexual, religião e origem étnica.

O Senado Federal informou que a Central Nacional de Denúncias da SaferNet registrou um aumento de 67,5% nas denúncias de crimes de ódio na internet

ISSN 2178-6925

envolvendo racismo, LGBTfobia, xenofobia, neonazismo, misoginia, apologia a crimes contra a vida e intolerância religiosa no primeiro semestre de 2022 (Crimes..., 2022).

O racismo virtual na maioria das vezes se manifesta em forma de insultos, memes depreciativos, estereótipos e até mesmo ameaças de violência contra grupos raciais minoritários. Abdias Nascimento, um grande nome que conheceu estágios do racismo no Brasil, fez um discurso impactante no Senado Federal afirmando:

> Um dos efeitos mais cruéis desse tipo de ideologia é confundir e atomizar o grupo oprimido, impedindo-o de se organizar para defender seus interesses. Assim, por exemplo, se denuncia a discriminação racial de que é vítima, o negro se vê enquadrado nas categorias de "complexado", "ressentido" ou mesmo "perturbado mental". Algum tempo atrás, poderíamos acrescentar as de "subversivo" ou "agente do comunismo internacional", estigmas que as instituições repressoras de nosso país [na ditadura militar] tentaram imprimir em minha própria pele e que me obrigaram a viver no exterior por mais de uma década (Nascimento, 2013, p. 2).

Outrossim, destaca-se que a propagação da misoginia e do machismo também é um elemento importante do discurso de ódio na internet no Brasil. Ataques verbais e ameaças de violência de gênero são comuns entre mulheres que trabalham em espaços públicos *online,* como jornalistas, políticas e influenciadoras.

O caso da jornalista Patrícia Campos Mello, vítima de ataques misóginos após uma reportagem investigativa, é um exemplo emblemático desse específico. A jornalista afirmou: "Depois que eles fizeram isso, basicamente a minha vida virou um inferno. Tem até hoje memes pornográficos com montagens de mulheres peladas com o meu rosto. Tem mensagens de gente falando que eu deveria ser estuprada" (Mello, 2022, p. 05).

Além disso, a homofobia e a transfobia são outras formas predominantes de discurso de ódio que ocorrem na internet brasileira. As pessoas LGBT+ são frequentemente insultadas, discriminadas e até mesmo ameaçadas de violência em plataformas de internet. O caso do ator Victor Meyniel, que foi vítima de homofobia, sendo brutalmente agredido, citado na reportagem de Eliel Guihen (2023, p. 01), diz que: "Existe o ato de injúria racial, homofóbica, gênero. Existe e tá na nossa cara. Existe, é crime e da prisão. Ontem foi meu aniversário e é um presente poder estar conversando aqui (...) não se omitam, é questão de uma ajuda".

À luz de todo o exposto, verifica-se que o discurso de ódio na internet no Brasil envolve políticas públicas, regulação governamental e responsabilidade das plataformas *online.* A lei brasileira não regulamenta o discurso de ódio *online*, apesar

ISSN 2178-6925

do Marco Civil da Internet estabelecer princípios importantes sobre a liberdade de expressão e a responsabilidade dos provedores de internet.

3.2 Legislação atual relativa aos crimes cibernéticos

A Lei Carolina Dieckmann foi criada como resposta a um caso muito comentado em que a atriz Carolina Dieckmann foi vítima de um *Hack* que revelou suas fotos íntimas e recebidas na internet sem sua autorização. Esta lei visa prevenir e punir uma variedade de crimes cibernéticos, como acesso não autorizado a sistemas computacionais, obtenção de dados pessoais sem consentimento e interrupção de serviços de computador, entre outros. Uma das principais mudanças que essa lei trouxe foi a criminalização do acesso não autorizado a dispositivos informáticos, conhecido como “hackeamento”.

A Lei Carolina Dieckmann e o Marco Civil da Internet (Lei nº 12.965/2014) são regulamentos importantes para a segurança cibernética no Brasil. Embora o Marco Civil não se concentre especificamente em crimes cibernéticos, ele estabelece princípios essenciais sobre a proteção da privacidade, a liberdade de expressão e a responsabilidade dos provedores de internet. Além disso, este marco legal estabelece diretrizes para manter registros de conexão e acesso a aplicações de internet, que podem ser úteis na investigação e proteção de crimes cibernéticos (Brasil, 2014).

Outrossim, tem-se também a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, é uma lei brasileira que regulamenta como organizações públicas e privadas tratam dados pessoais. A Lei Geral de Proteção de Dados (LGPD), baseada no Regulamento Geral de Proteção de Dados (GDPR) da UE, foi desenvolvida com o objetivo de aumentar o controle e a proteção dos dados pessoais dos cidadãos do Brasil. O GDPR estabelece padrões claros sobre como as informações devem ser coletadas, armazenadas, usadas e compartilhadas (Brasil, 2018).

A LGPD define dados pessoais como dados relacionados a uma pessoa identificável ou identificável, ou seja, dados que podem identificar uma pessoa direta ou indiretamente. Isso inclui informações como nome, endereço, número de telefone, endereço de e-mail, registros médicos, informações financeiras e até mesmo dados como endereço IP e cookies de navegação na internet (Brasil, 2018).

A violação da LGPD pode resultar em sanções administrativas, como advertências e multas de até 2% do exercício da organização (até R$ 50 milhões por

ISSN 2178-6925

infração), bloqueio ou eliminação de dados pessoais envolvidos na violação e suspensão parcial ou total de atividades relacionadas ao tratamento de dados (Brasil, 2018).

Acerca dessa legislação, cumpre colacionar posicionamento de Patrícia Peck Pinheiro:

> A LGPD surge com o intuito de proteger direitos fundamentais como privacidade, intimidade, honra direito de imagem e dignidade. Pode-se pontuar também que a necessidade de leis específicas para a proteção dos dados pessoais aumentou com o rápido desenvolvimento e expansão da tecnologia no mundo, como resultado dos desdobramentos da globalização, que trouxe como uma de suas consequências o aumento da importância da informação. Isso quer dizer que a informação passou a ser um ativo de alta relevância para governantes e empresários: quem tem acesso aos dados, tem acesso ao poder (Pinheiro, 2020, p. 70).

Além dessas leis específicas, o Código Penal Brasileiro também inclui artigos que podem ser aplicados a crimes cometidos online, como calúnia, difamação, ameaça, estelionato, entre outros (Brasil, 1940). À medida que a tecnologia e as práticas criminosas evoluem, a interpretação e a aplicação dessas leis no contexto da internet têm sido objeto de discussão e desenvolvimento jurisprudencial.

No entanto, apesar da existência dessas leis, a legislação sobre crimes cibernéticos enfrentados por desafios, como a rápida evolução das tecnologias digitais, a falta de cooperação internacional em casos transnacionais e a dificuldade de identificar e rastrear crimes *online.* Como resultado, é necessário um esforço contínuo para manter a legislação atualizada e fortalecida, bem como investir em capacitação e recursos para a investigação e aplicação da lei no combate aos crimes no mundo digital.

4. A complexidade da liberdade de expressão no contexto dos "*haters" online*

4.1 A delicada fronteira entre liberdade de expressão e discurso de ódio na esfera digital

Diversos âmbitos da sociedade discutem este tema complexo e atual do embate entre a liberdade de expressão e o discurso de ódio na esfera digital. Muitas constituições, incluindo a brasileira, garantem o direito fundamental à liberdade de

expressão. Mas esse direito não é absoluto. Tem limites quando entra em conflito com outros direitos, como o direito à não discriminação ou a dignidade humana.

O surgimento das redes sociais e plataformas digitais trouxe novos obstáculos para esse contexto. O anonimato que a internet oferece muitas vezes incentiva as pessoas a espalhar discursos de ódio, intolerância e violência. Essa disseminação de conteúdo nocivo pode causar danos significativos às vítimas, afetando sua saúde mental, emocional e até mesmo sua segurança física.

Encontrar um equilíbrio entre proteger a liberdade de expressão e evitar o discurso de ódio é um grande desafio. Como afirmou a Ministra Carmen Lúcia, do Supremo Tribunal Federal (STF) do Brasil, “quem não tem direito à liberdade de expressão não tem garantia de qualquer outro direito porque a palavra é a expressão da alma, do pensamento” (CNJ, 2018).

Mas a pergunta que fica é: Até onde essa expressão da alma é algo saudável? É nítido que o aumento do discurso de ódio na internet e seus efeitos estão causando preocupação em todo o mundo. No Brasil, vários casos têm sido julgados, incluindo ataques racistas e homofóbicos e ameaças de violência. Esses casos mostram o quão urgentemente precisa de políticas e medidas eficazes para combater o discurso de ódio na internet.

É necessário que os governos, empresas de tecnologia, organizações civis e usuários da internet colaborem para resolver esse problema. A promoção da educação digital, a implementação de políticas de moderação de conteúdo e a responsabilização dos perpetradores do discurso de ódio são medidas significativas que contribuem para esse objetivo.

Ao lidar com a delicada fronteira entre a liberdade de expressão e o discurso de ódio no mundo digital, é necessário adotar uma abordagem sensível e sensata. Embora seja essencial proteger a liberdade de expressão, não pode ser feita às custas da segurança e da dignidade dos indivíduos. É imperativo buscar soluções que permitam que todos vivam em um ambiente *online* mais justo, respeitoso e seguro, pois a toxidade da das redes sociais está adoecendo as pessoas.

Por fim, vale pontuar que as vezes a pessoa diz coisas absurdas, passíveis inclusive de penalização legal, e acredita que dizer “ah, mas é minha opinião” valida aquilo que foi dito como algo aceitável. Isso é muito perigoso. O que se vê, muitas vezes, um excesso de relativização de coisas que não são relativizáveis. Racismo é racismo. Homofobia é homofobia. Quando se diz algo que coloca em risco a

ISSN 2178-6925

integridade física, o direito de ir e vir do outro, já não se trata mais de pura opinião (Melo, 2018).

4.2 Estratégias de enfrentamento ao discurso de ódio na esfera digital: exemplos e perspectivas

Congruente todo o exposto, verifica-se que o discurso de ódio na internet é um fenômeno alarmante que tem aumentado com o desenvolvimento das redes sociais e das plataformas digitais. Esse tipo de discurso pode ter um efeito devastador, causando conflitos, fomentando preconceito e até encorajando a violência contra grupos ou pessoas específicas.

A partir dessa situação, várias abordagens para combater o discurso de ódio na internet surgiram, mas também enfrentaram alguns desafios, tais como educação e conscientização, moderação de conteúdo, regulamentação e responsabilização e cooperação internacional.

Quanto a educação e a conscientização são fundamentais para combater o discurso de ódio na internet. As pessoas não precisam apenas aprender sobre o que constitui discurso de ódio; eles também precisam aprender a sentir, respeitar e entender diferentes perspectivas e identidades. As iniciativas da sociedade civil, campanhas de conscientização e programas educacionais nas escolas desempenham um papel importante nesse sentido.

Ademais, é imprescindível a moderação de conteúdo em suas plataformas, sendo responsabilidade primária das empresas de tecnologia. Isso inclui criar e implementar diretrizes claras de uso que proíbem o discurso de ódio e estabelecer mecanismos eficientes para detectar e remover conteúdo prejudicial. A moderação de conteúdo, por outro lado, enfrenta problemas importantes, como identificar com precisão o discurso de ódio e equilibrar a liberdade de expressão com a remoção de conteúdo perigoso.

Na sequência, faz-se necessário a regulamentação e responsabilização como uma forma de controle do discurso de ódio na internet, sendo componente crucial. Embora seja uma área complicada e controversa, regras claras podem ajudar a limitar o discurso de ódio e responsabilizar os culpados. No entanto, é fundamental garantir que essas regras não restrinjam de forma injusta a liberdade de expressão legítima.

ISSN 2178-6925

Por derradeiro, necessita-se da cooperação internacional, tendo em vista que a internet é transnacional, logo, a cooperação internacional é essencial para combater o discurso de ódio online. Isso envolve não apenas a cooperação entre as nações em termos de informações e melhores práticas, mas também, a criação de padrões e diretrizes comuns para lidar com o problema a nível mundial. Isso significa que a cooperação entre governos, empresas de tecnologia e organizações da sociedade civil é essencial.

5. Considerações finais

À luz de todo o exposto, denote-se que, em síntese, este estudo enfatiza as dificuldades enfrentadas na luta contra os crimes cibernéticos, particularmente no que diz respeito aos *"haters"* e ao discurso de ódio na internet. A rápida evolução tecnológica e a falta de legislação específica dificultam a investigação e punição desses crimes. Esses indivíduos são ainda mais perigosos devido à sensação de impunidade e à velocidade com que as mensagens de ódio se propagam na internet.

Entretanto, é importante enfatizar a importância da conscientização e da educação digital para evitar o discurso de ódio. Os usuários devem ser conscientes dos limites da liberdade de expressão e saber como suas palavras podem afetar as vítimas. As empresas de tecnologia também desempenham um papel importante na moderação de conteúdo e na adoção de medidas efetivas para combater o discurso de ódio em suas plataformas.

Além disso, devido à natureza transnacional da internet, o enfrentamento dessa questão requer colaboração internacional. Para garantir um ambiente virtual mais seguro, justo e respeitoso para todos, é necessário um esforço conjunto de governos, empresas, organizações da sociedade civil e usuários individuais.

Assim, denote-se que a complexidade do desafio e quanto é importante usar uma abordagem multifacetada e colaborativa para superar o emblema discutido no presente estudo acadêmico, não sendo possível, portanto, esgotar a pesquisa neste trabalho. Razão pela qual, segure-se novas pesquisas futuras quanto o avanço da legislação brasileira no que tange aos crimes cibernéticos.

ISSN 2178-6925

Referências

BRASIL. **Decreto-lei nº 2.848, de 7 de dezembro de 1940.** Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm >. Acesso em: 30 mar. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: < L12965 (planalto.gov.br) >. Acesso em: 20 fev. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: < L13709 (planalto.gov.br) >. Acesso em: 20 fev. 2024.

CNJ. **Liberdade de expressão garante a democracia, diz Cármen Lúcia.** Brasília, DF: CNJ, 2018. Disponível em: < Liberdade de expressão garante a democracia, diz Cármen Lúcia - Portal CNJ >. Acesso em: 3 abr. 2024.

CRIMES de ódio têm crescimento de até 650% no primeiro semestre de 2022. [*S.L.*]: SaferNet**,** 2022. Disponível em: < Crimes de ódio têm crescimento de até 650% no primeiro semestre de 2022 | SaferNet Brasil >. Acesso em: 20 fev. 2024.

GUIHEN, Eliel. **Ator Victor Meyniel faz alerta sobre casos de homofobia após sofrer agressão:** 'Não se omitam'. [*S.L.*]: Cosmoliko**,** 2023. p. 1. Disponível em: < Ator Victor Meyniel faz alerta sobre casos de homofobia após sofrer agressão: 'Não se omitam' (cosmoliko.com) >. Acesso em: 22 mar. 2024.

NASCIMENTO, Abdias. **13 de maio uma mentira cívica**. Brasília, DF: Portal Geledés, 2013. p. 2. Disponível em: < Abdias Nascimento: 13 de maio uma mentira cívica (geledes.org.br) >. Acesso em: 20 fev. 2024.

MELLO, Patrícia Campos. **Atingidas pela desinformação**. São Paulo, SP: Desinformante, 2022. p. 5. Disponível em: < Atingidas pela desinformação: Patrícia Campos Mello (desinformante.com.br)>. Acesso em: 21 fev. 2024.

MELO, Tatiane de. **Discurso de ódio na internet é tema do Psicologia em foco no rádio.** Belo Horizonte, MG: CRP-MG, 2018. Disponível em: < Discurso de ódio na internet é tema do Psicologia em Foco no rádio | CRP-MG (crp04.org.br) >. Acesso em: 06 abr. 2024.

PANNAIN, Camila Nunes; PEZZELLA, Maria Cristina**. Liberdade de Expressão e Hate Speech na Sociedade da Informação.** Revista Direitos Emergentes da Sociedade Global, Santa Maria, 2015. p. 28.
PINHEIRO, Patrícia Peck. **Proteção de dados pessoais:** comentários à Lei n. 13.709/2018 (LGPED). 2. Ed. São Paulo: Saraiva Educação, 2020. p. 70.

WIGERFELT, Anders S.; WIGERFELT, Berit. DAHLSTRAND, Karl Johan. Online **Hate Crime – Social Norms And The Legal System.** Revista Quaestio Iuris. v. 8, n. 3, Rio de Janeiro, p. 1859-1878, 2015. Disponível em: < Vista do Online hate crime – social norms and the legal system / Crime de ódio virtual - normas sociais e o sistema jurídico (uerj.br) >. Acesso em: 06 abr. 2024.