

REGULAMENTAÇÃO DAS REDES SOCIAIS VERSUS CRIMES
CIBERNÉTICOS^aThiago Bessa Pontes

RESUMO

Objetivo: Investigar o papel da regulamentação das redes sociais no enfrentamento dos crimes cibernéticos, analisando o impacto das políticas existentes e explorando as lacunas que ainda precisam ser preenchidas. A pesquisa busca compreender como as regulamentações podem evoluir para garantir um equilíbrio entre segurança, liberdade de expressão e inovação tecnológica, contribuindo para um ambiente digital mais seguro e responsável.

Referencial Teórico: Baseia-se em uma revisão bibliográfica que inclui artigos científicos, legislações e relatórios técnicos. A análise aborda temas como moderação de conteúdo, responsabilidade dos intermediários, cidadania digital, e cooperação internacional. Destacam-se documentos fundamentais, como o trabalho de Gillespie (2018) sobre moderação de conteúdo e o estudo de Kowalski *et al.* (2014) sobre cyberbullying.

Método: O método adotado é qualitativo, combinando revisão bibliográfica, análise documental e estudos de caso. A revisão bibliográfica foi realizada com base em artigos científicos publicados a partir de 2003, utilizando a base de dados Scopus. A análise documental incluiu legislações como o Digital Services Act (DSA) da União Europeia e o Network Enforcement Act (NetzDG) da Alemanha. Os estudos de caso focaram na aplicação dessas legislações e nos esforços de plataformas para cumprir requisitos de moderação de conteúdo.

Resultados e Discussão: Os resultados indicam que a regulamentação das redes sociais influencia significativamente a prevenção de crimes cibernéticos e a governança digital. A moderação de conteúdo, a responsabilidade dos intermediários e a educação para a cidadania digital são aspectos-chave. No entanto, há desafios, como a falta de alinhamento global nas regulamentações e a dependência de algoritmos para a moderação de conteúdo, que podem levar a inconsistências e preocupações éticas.

Implicações da Pesquisa: A pesquisa destaca a necessidade de uma abordagem equilibrada entre a segurança digital e a liberdade de expressão, sugerindo que a regulamentação deve evoluir para incluir medidas preventivas, como a educação digital e o desenvolvimento de tecnologias de defesa.

Originalidade/Valor: Este estudo contribui para a literatura ao oferecer uma análise integrada das regulamentações existentes e suas implicações práticas no combate aos crimes cibernéticos. A pesquisa propõe soluções inovadoras, como a integração de tecnologias avançadas e a promoção da cidadania digital, que podem servir como base para futuras políticas e regulamentações. Além disso, o estudo destaca a importância de uma abordagem global e colaborativa para a governança digital.

Palavras-chave: regulamentação de redes sociais, crimes cibernéticos, moderação de conteúdo, governança digital, liberdade de expressão.

^a PhD in Education, Instituto Universitário de Lisboa (ISCTE-IUL), Lisboa, Portugal. E-mail: tbpsa@iscte-iul.pt



Received: 11/1/2024

Accepted: 1/3/2025

DOI: <https://doi.org/10.55908/sdgs.v13i2.4302>

SOCIAL MEDIA REGULATION VERSUS CYBERCRIME

ABSTRACT

Objective: To investigate the role of social media regulation in addressing cybercrime, analysing the impact of existing policies and exploring the gaps that still need to be filled. The research seeks to understand how regulations can evolve to ensure a balance between security, freedom of expression, and technological innovation, contributing to a safer and more responsible digital environment.

Theoretical Framework: This study is based on a bibliographic review, which includes scientific articles, legislation, and technical reports. The analysis addresses topics such as content moderation, intermediary responsibility, digital citizenship, and international cooperation. Key documents include Gillespie's (2018) work on content moderation and Kowalski *et al.* (2014) on cyberbullying.

Method: The adopted method is qualitative, combining bibliographic review, documentary analysis, and case studies. The bibliographic review was conducted using scientific articles published since 2003, with Scopus as the data source. The documentary analysis included legislation such as the European Union's Digital Services Act (DSA) and Germany's Network Enforcement Act (NetzDG). The case studies focused on the application of these regulations and platform efforts to comply with content moderation requirements.

Results and Discussion: The results indicate that social media regulation significantly influences cybercrime prevention and digital governance. Content moderation, intermediary responsibility, and digital citizenship education are key aspects. However, challenges remain, such as the lack of global alignment in regulations and the reliance on algorithms for content moderation, which can lead to inconsistencies and ethical concerns.

Research Implications: The research highlights the need for a balanced approach between digital security and freedom of expression, suggesting that regulation should evolve to include preventive measures such as digital education and the development of defence technologies. **Originality/Value:** This study contributes to the literature by offering an integrated analysis of existing regulations and their practical implications in combating cybercrime. The research proposes innovative solutions, such as the integration of advanced technologies and the promotion of digital citizenship, which could serve as a foundation for future policies and regulations. Furthermore, the study underscores the importance of a global and collaborative approach to digital governance.

Keywords: social media regulation, cybercrime, content moderation, digital governance, freedom of expression.

REGULACIÓN DE LAS REDES SOCIALES FRENTE A LOS DELITOS INFORMÁTICOS

RESUMEN

Objetivo: Investigar el papel de la regulación de las redes sociales en la lucha contra los ciberdelitos, analizando el impacto de las políticas existentes y explorando las lagunas que aún deben ser abordadas. La investigación busca comprender cómo las regulaciones pueden evolucionar para garantizar un equilibrio entre seguridad, libertad de expresión e innovación



tecnológica, contribuindo a un entorno digital más seguro y responsable.

Marco Teórico: Este estudio se basa en una revisión bibliográfica que incluye artículos científicos, legislaciones e informes técnicos. El análisis aborda temas como la moderación de contenidos, la responsabilidad de los intermediarios, la ciudadanía digital y la cooperación internacional. Se destacan documentos clave, como el trabajo de Gillespie (2018) sobre moderación de contenidos y el estudio de Kowalski *et al.* (2014) sobre ciberacoso.

Método: El método adoptado es cualitativo, combinando revisión bibliográfica, análisis documental y estudios de caso. La revisión bibliográfica se realizó utilizando artículos científicos publicados desde 2003, con la base de datos Scopus. El análisis documental incluyó legislaciones como el Digital Services Act (DSA) de la Unión Europea y el Network Enforcement Act (NetzDG) de Alemania. Los estudios de caso se centraron en la aplicación de estas regulaciones y en los esfuerzos de las plataformas para cumplir con los requisitos de moderación de contenido.

Resultados y Discusión: Los resultados indican que la regulación de las redes sociales influye significativamente en la prevención de ciberdelitos y en la gobernanza digital. La moderación de contenidos, la responsabilidad de los intermediarios y la educación para la ciudadanía digital son aspectos clave. Sin embargo, existen desafíos, como la falta de alineación global en las regulaciones y la dependencia de los algoritmos para la moderación de contenidos, lo que puede generar inconsistencias y preocupaciones éticas.

Implicaciones de la Investigación: La investigación resalta la necesidad de un enfoque equilibrado entre la seguridad digital y la libertad de expresión, sugiriendo que la regulación debe evolucionar para incluir medidas preventivas, como la educación digital y el desarrollo de tecnologías de defensa.

Originalidad/Valor: Este estudio contribuye a la literatura al ofrecer un análisis integrado de las regulaciones existentes y sus implicaciones prácticas en la lucha contra los ciberdelitos. La investigación propone soluciones innovadoras, como la integración de tecnologías avanzadas y la promoción de la ciudadanía digital, que podrían servir de base para futuras políticas y regulaciones. Además, el estudio destaca la importancia de un enfoque global y colaborativo para la gobernanza digital.

Palabras clave: Regulación de redes sociales, Ciberdelitos, Moderación de contenidos, Gobernanza digital, Libertad de expresión.

1 INTRODUÇÃO

Na era digital, as redes sociais revolucionaram a comunicação global, criando possibilidades de interação e compartilhamento de informações. No entanto, ao mesmo tempo em que conectam bilhões de pessoas ao redor do mundo, essas plataformas tornaram-se terreno fértil para a proliferação de crimes cibernéticos, que incluem phishing, roubo de identidade, disseminação de desinformação e assédio online. A crescente sofisticação dos crimes cibernéticos e a dificuldade de aplicação de leis transnacionais complicam ainda mais a governança digital. Estudos mostram que o impacto das redes sociais não é uniforme; plataformas são usadas tanto para a disseminação de informações positivas quanto para perpetuar práticas prejudiciais (Kaur



et al., 2024).

O impacto dos crimes cibernéticos nas redes sociais é evidente em várias esferas, incluindo segurança individual, proteção de dados e confiança nas instituições digitais. O relatório do Fórum Econômico Mundial aponta que 2023 foi um ano marcante no aumento da sofisticação e frequência desses crimes, destacando a urgência de regulamentações eficazes para mitigar tais riscos. O estudo também enfatiza que as lacunas na legislação global de segurança cibernética tornam usuários e organizações vulneráveis a ataques cada vez mais complexos (World Economic Forum, 2023).

Ao mesmo tempo, as redes sociais enfrentam desafios em equilibrar a liberdade de expressão e os direitos fundamentais com a necessidade de moderação de conteúdo e combate ao uso indevido das plataformas. Jurisdições como Alemanha e União Europeia adotaram legislações para responsabilizar plataformas, como o Network Enforcement Act, que exige respostas rápidas a conteúdos ilícitos. Por outro lado, os Estados Unidos mantêm uma abordagem mais protetiva em relação à liberdade de expressão, respaldada pelo Artigo 230 da Lei de Decência nas Comunicações (Paulos & Çelik, 2021), mesmo sendo o país com maior percentual de ataques de cibercrime do mundo (Ahmed, 2021). Essas abordagens variadas destacam a complexidade de criar uma estrutura universal de regulamentação.

No contexto das redes sociais, crimes como o cyberbullying, a manipulação eleitoral e o terrorismo online exemplificam os riscos associados à falta de regulamentação robusta e estratégias de segurança cibernética integradas. Um estudo recente revela que 80% dos crimes cibernéticos nas redes sociais exploram vulnerabilidades em configurações de privacidade ou falta de conscientização dos usuários, destacando a importância de regulamentações que incentivem a educação digital e o desenvolvimento de tecnologias de defesa, como criptografia avançada e autenticação multifator (Damaraju, A., 2020).

Este artigo busca investigar o papel da regulamentação das redes sociais no enfrentamento dos crimes cibernéticos, analisando o impacto das políticas existentes e explorando lacunas que ainda precisam ser preenchidas. Além disso, propõe discutir como essas regulamentações podem evoluir para garantir um equilíbrio entre segurança, liberdade de expressão e inovação tecnológica.



2 MÉTODO

Este estudo adota uma abordagem metodológica qualitativa, combinando revisão bibliográfica, análise documental e estudos de caso para investigar o impacto da regulamentação de redes sociais no combate aos crimes cibernéticos. A seguir, descrevem-se as etapas e os critérios utilizados.

2.1 REVISÃO BIBLIOGRÁFICA

A revisão bibliográfica fundamenta-se em artigos científicos publicados a partir de 2003, encontrados na base de dados da Scopus com o auxílio da Scopus AI. O prompt inserido foi: "Como é que a regulamentação das redes sociais influencia a prevenção do cibercrime e a governação digital no enfrentamento do discurso de ódio online?" Este levantamento permitiu mapear os principais desafios associados à regulamentação de redes sociais e identificar legislações relevantes, como o Digital Services Act e o Network Enforcement Act (Kaur *et al.*, 2024; O'Regan, 2023).

2.2 ANÁLISE DOCUMENTAL

Foram analisados textos legais e relatórios técnicos relacionados à governança digital e à regulação de crimes cibernéticos em redes sociais. Entre os documentos analisados, incluem-se o Digital Services Act da União Europeia e legislações específicas como o Communications Decency Act dos Estados Unidos. Relatórios de organizações como o Fórum Econômico Mundial (2023) também foram considerados. A análise concentrou-se em identificar lacunas regulatórias e avaliar a eficácia das medidas implementadas.

2.3 ESTUDOS DE CASO

Para compreender os efeitos práticos das regulamentações, foram escolhidos dois estudos de caso: (1) a aplicação do Network Enforcement Act na Alemanha e (2) os esforços de plataformas como Facebook e Twitter para cumprir requisitos de moderação. Os critérios de seleção incluíram relevância atual, impacto na mitigação de crimes



cibernéticos e disponibilidade de dados em fontes acadêmicas confiáveis (Dawson & Thomson, 2021).

2.4 CRITÉRIOS DE VALIDAÇÃO

A validade do estudo é garantida pelo uso de múltiplas fontes científicas e pela triangulação dos dados obtidos na revisão bibliográfica, análise documental e estudos de caso. Métodos como a análise temática foram aplicados para categorizar as evidências coletadas, permitindo uma interpretação robusta e integrada (Braun & Clarke, 2006).

3 DESENVOLVIMENTO

3.1 REVISÃO BIBLIOGRÁFICA

A revisão bibliográfica obtida a partir da mineração dos dados realizada pela Scopus AI ao utilizar o prompt: “How does social media regulation influence cybercrime prevention and digital governance in addressing online hate speech?”, que pode ser traduzido livremente por “Como é que a regulamentação das redes sociais influencia a prevenção do cibercrime e a governação digital no enfrentamento do discurso de ódio online?” apresentou um total de 8 documentos relevantes para uma análise qualitativa dos aspectos e influências para a regulamentação das redes sociais (Tabela 2). Estes documentos apresentam em comum a referência básica de 5 documentos fundamentais, ou seja, os 5 artigos mais influentes e frequentemente citados dentro deste determinado tópico de pesquisa (Tabela 1). Os documentos fundamentais são citados por duas ou mais referências utilizadas para criar o seu resumo. A Tabela 1 apresenta os documentos fundamentais

**Tabela 1***Documentos fundamentais usados pela SCOPUS AI.*

Author full names	Title	Year	Source title	Volume	Cited by
Siegel, Alexandra A.; Badaan, Vivienne	Sectarianism: Experimental Approaches to Reducing Sectarian Hate Speech Online	2020	American Political Science Review	114	55
Massanari, Adrienne	Gamergate and The Fapping: How Reddit's algorithm, governance, and culture support toxic technocultures	2017	New Media and Society	19	762
Gillespie, Tarleton	Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media	2018	Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media		1279
Kowalski, Robin M.; Giumetti, Gary W.; Schroeder, Amber N.; Lattanner, Micah R.	Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth	2014	Psychological Bulletin	140	1970
Matamoros- Fernández, Ariadna	Platformed racism: the mediation and circulation of an Australian race- based controversy on Twitter, Facebook and YouTube	2017	Information Communication and Society	20	262

A partir dos 5 documentos fundamentais, foram sumarizados 9 aspectos/domínios e suas influências como propostas para a regulamentação das redes sociais. Estes domínios são fortemente influenciados pelos trabalhos científicos de 8 autores que usam em suas pesquisas os 5 documentos fundamentais usados pela SCOPUS AI.

Estes artigos podem ser encontrados na Tabela 2 que classifica de modo qualitativo o aspecto principal da abordagem de cada artigo, apresenta as principais influências da regulamentação estudada, e apresenta os dados de identificação dos documentos (Nome dos autores, Título do artigo, ano de publicação e a revista em que foi publicado)

**Tabela 2**

Quadro resumo bibliográfico dos aspectos e influências para regulamentação das redes sociais.

Aspecto	Influência da Regulamentação	Author full names	Title	Year	Source title
Moderação de Conteúdo	Exige estratégias equilibradas entre direitos dos usuários e segurança.	Enarsson, Therese	Navigating hate speech and content moderation under the DSA: insights from ECtHR case law	2024	Information and Communications Technology Law
Responsabilidade dos Intermediários	Varia por região; a UE impõe obrigações, enquanto os EUA oferecem isenções.	Yu, Wenguang	Internet Intermediaries' Liability for Online Illegal Hate Speech	2018	Frontiers of Law in China
Cidadania Digital	Educação sobre comportamento responsável reduz riscos de crimes cibernéticos.	Althibyani, Hosam A.; Al-Zahrani, Abdulrahman M.	Investigating the Effect of Students' Knowledge, Beliefs, and Digital Citizenship Skills on the Prevention of Cybercrime	2023	Sustainability (Switzerland)
Marcos Regulatórios	Exemplos como o NetzDG demonstram eficácia e limitações.	Griffin, Rachel	New school speech regulation as a regulatory strategy against hate speech on social media: The case of Germany's NetzDG	2022	Telecommunications Policy
Interesse Público	Plataformas devem integrar o interesse público em sua governança.	Griffin, Rachel	New school speech regulation as a regulatory strategy against hate speech on social media: The case of Germany's NetzDG	2022	Telecommunications Policy
Cooperação Internacional	A interlegalidade auxilia na navegação por diferentes contextos jurídicos.	Bello, Barbara Giovanna	Tackling online hate speech from a European perspective: Potentials and	2023	Onati Socio-Legal Series



			challenges of inter-legality		
Intervenções Tecnológicas	Compreender determinantes digitais ajuda na prevenção eficaz.	Weber, Ina; Vandebosch, Heidi; Poels, Karolien; Pabian, Sara	Features for Hate? Using the Delphi Method to Explore Digital Determinants for Online Hate Perpetration and Possibilities for Intervention	2023	Cyberpsychology, Behavior, and Social Networking
Apoio Público	Influenciado por experiências pessoais e percepção de danos.	Park, Ahran ; Kim, Minjeong; Kim, Ee-Sun	SEM analysis of agreement with regulating online hate speech: influences of victimization, social harm assessment, and regulatory effectiveness assessment	2023	Frontiers in Psychology
Abordagem de Justiça Social	Destaca a proteção de grupos marginalizados.	Otero, Paloma Viejo	Platform governance and social justice: Governing hate speech on social media	2024	Platform Governance and Social Justice: Governing Hate Speech on Social Media

A partir dos resultados apresentados na tabela 2 temos que a regulamentação das redes sociais influencia significativamente a prevenção do cibercrime e a governação digital ao exigir moderação de conteúdos, moldar atitudes públicas e promover comportamentos online responsáveis.

Uma regulamentação eficaz exige um equilíbrio entre a proteção dos direitos dos utilizadores e a garantia da segurança, com foco em abordagens sistémicas e preventivas. Na seção Resultados e discussões deste trabalho apresentamos mais detalhes.

3.2 ANÁLISE DOCUMENTAL DAS LEGISLAÇÕES DE REGULAMENTAÇÃO DE REDES SOCIAIS

A análise das legislações de regulamentação de redes sociais revela um panorama



jurídico global sobre a governança digital e a proteção contra crimes cibernéticos. Diversos países adotaram abordagens únicas para regular o uso de plataformas digitais, focando principalmente na proteção dos usuários e no combate à desinformação. A seguir, são apresentadas cinco das legislações mais relevantes, com base nas fontes disponíveis.

Na União Europeia (UE) foi estabelecida A Lei de Serviços Digitais (DSA) com o objetivo de criar um ambiente online mais seguro, transparente e responsivo. A DSA visa a proteção dos usuários e a responsabilização das plataformas digitais, obrigando-as a gerenciar conteúdos prejudiciais, como discurso de ódio e desinformação. O foco da legislação está na transparência dos anúncios e na proteção de menores, além de exigir maior responsabilidade das plataformas para monitorar conteúdos e limitar o impacto de conteúdos prejudiciais (European Union, 2023).

Em contraste, a Lei de Execução de Rede (NetzDG) da Alemanha foca na rápida remoção de conteúdos ilegais, como discurso de ódio e outros conteúdos nocivos, por plataformas com mais de 2 milhões de usuários. Esta legislação tem se mostrado influente globalmente e serve como modelo para outros países que buscam implementar regulamentações mais rigorosas sobre as plataformas digitais (Federal Ministry of Justice, 2021).

A Lei de Privacidade Online das Crianças (COPPA) dos Estados Unidos, por sua vez, estabelece requisitos rígidos para a coleta de dados de crianças menores de 13 anos. As plataformas devem obter o consentimento dos pais antes de coletar informações pessoais de menores, com o objetivo de proteger sua privacidade. Essa legislação é fundamental para evitar o abuso de dados pessoais e para garantir que as plataformas respeitem os direitos das crianças (Federal Trade Commission, 2023).

No Brasil, o Marco Civil da Internet, sancionado em 2014 (Planalto, 2014), estabelece princípios fundamentais para a governança da internet, como a neutralidade da rede, a privacidade dos usuários e a proteção de dados pessoais. Estima-se que esse marco legal será complementado pelo Projeto de Lei das Fake News, que visa combater a disseminação de desinformação em plataformas digitais. O projeto de lei exige que as redes sociais adotem medidas de transparência em relação a anúncios políticos e rastreamento de conteúdos, buscando um equilíbrio entre a liberdade de expressão e a proteção contra abusos (Câmara dos Deputados, 2020).

Na Austrália foi sancionada em 2021 a Lei de Execução de Rede (Australian Government, 2021), que estabelece que menores de 16 anos precisam de autorização dos



país para acessar redes sociais. Essa regulamentação foi criada para proteger os jovens de riscos online, incluindo a exposição a conteúdos prejudiciais, bullying digital e exploração. As autoridades australianas enfatizam a necessidade de plataformas mais responsivas na proteção da privacidade e segurança dos menores (Australian Government, 2021).

Essas legislações revelam o esforço global em regulamentar redes sociais, equilibrando a proteção contra crimes cibernéticos e a preservação de direitos fundamentais como a privacidade e a liberdade de expressão. A regulamentação digital continua a ser um campo dinâmico, com novos desafios emergindo conforme as tecnologias evoluem.

4 RESULTADOS E DISCUSSÕES

A análise documental sobre a regulamentação digital e os crimes cibernéticos em redes sociais destaca importantes tendências e desafios globais.

A União Europeia implementou a legislação DSA para estruturar a moderação de conteúdos, abrangendo desde desinformação até discurso de ódio, com um foco em direitos fundamentais e intervenções sistêmicas em design de plataformas, entretanto ainda há fragmentação na abordagem entre as diversas regiões do mundo. Essa falta de alinhamento global ameaça os benefícios de uma internet aberta, levando a uma “soberania digital” fragmentada. Essa disparidade na aplicação de regulamentações, especialmente em contextos linguísticos e geográficos, torna a moderação de conteúdo inconsistente.

A dependência de algoritmos e automação para gerir conteúdo suscita preocupações de censura e discriminação. Relatórios sugerem a implementação de códigos de conduta mais robustos e medidas de design que desincentivem comportamentos abusivos online. Além disso, há um apelo por uma colaboração multilateral para criar um sistema mais coeso e baseado nos direitos humanos para regulamentação digital.

Esse panorama reforça a relevância de aprofundar ainda mais a análise documental para compreender as intersecções entre leis nacionais e desafios tecnológicos, com vistas a propor soluções mais equitativas e eficazes para a regulação de crimes cibernéticos em redes sociais.



Após a criação do prompt: "Como é que a regulamentação das redes sociais influencia a prevenção do cibercrime e a governação digital no enfrentamento do discurso de ódio online?", de forma a atender aos objetivos deste estudo que investiga o papel da regulamentação das redes sociais no enfrentamento dos crimes cibernéticos, analisando o impacto das políticas existentes e explorando lacunas que ainda precisam ser preenchidas foi possível categorizar em 3 principais áreas pelas quais a regulamentação deve ser apoiada, são as áreas: Prevenção de cibercrimes, Governação Digital e Abordar o discurso de ódio online.

A **Prevenção de Cibercrimes** exige moderação eficaz de conteúdos, responsabilidade dos intermediários e educação para a cidadania digital. Regulamentos como a DSA na Europa impõe regras às plataformas para equilibrar segurança e direitos digitais. Enquanto a UE amplia a responsabilidade dos intermediários, os EUA adotam uma abordagem mais flexível. Promover a cidadania digital através da educação fortalece a proteção contra crimes cibernéticos. Na sequência apresentam-se como resultados três sugestões sumarizadas de como prevenir os cibercrimes:

- **Moderação de conteúdos:** Regulamentos como a Lei dos Serviços Digitais (DSA) na Europa determinam que as plataformas equilibrem os interesses comerciais com os direitos e a segurança dos utilizadores, exigindo estratégias de moderação diferenciadas para combater o discurso de ódio (Enarsson, 2024). Tanto a moderação automatizada como a humana enfrentam desafios, mas as estruturas regulamentares fornecem orientações essenciais para uma moderação eficaz;
- **Responsabilidade do intermediário:** Os diferentes países adotam abordagens variadas à responsabilidade do intermediário. Por exemplo, a UE tende a expandir a responsabilidade dos intermediários, impondo obrigações às plataformas para combater o discurso de ódio ilegal, o que pode ajudar a prevenir o cibercrime relacionado com o discurso de ódio (Yu, 2019). Esta abordagem contrasta com o modelo dos EUA, que oferece aos intermediários amplas isenções de responsabilidade (Yu, 2019);
- **Cidadania digital:** promover a cidadania digital através da educação pode ter um impacto significativo na prevenção do cibercrime. Educar os utilizadores sobre o comportamento online responsável e as leis digitais ajuda a mitigar riscos associados ao discurso de ódio e outros crimes cibernéticos (Althibyani & Al-Zahrani, 2023).



A segunda categoria de **Governança Digital** eficaz exige regulamentações robustas, consideração do interesse público e cooperação internacional. Leis como a NetzDG na Alemanha obrigam plataformas a remover conteúdos ilegais, mas têm limitações ao depender de denúncias. Além disso, integrar o interesse público na conceção das plataformas pode prevenir proativamente o discurso de ódio. Diante da falta de uma definição universal, a colaboração entre regulamentações nacionais e internacionais é essencial para superar desafios na regulação digital. Na sequência apresentam-se como resultados, três sugestões sumarizadas de governança digital:

- Estruturas regulamentares: países como a Alemanha implementaram leis como a NetzDG, que exigem que as plataformas operem procedimentos de reclamações para garantir a remoção rápida de conteúdos ilegais. No entanto, esta abordagem tem limitações, pois muitas vezes depende das queixas dos utilizadores e não aborda todos os factores que promovem o discurso de ódio (Griffin R., 2022);
- Considerações de interesse público: uma governança digital eficaz exige que as plataformas considerem o interesse público nos seus processos de conceção e governação. Esta abordagem sistémica visa moldar os ambientes de plataforma para desencorajar o discurso de ódio de forma proactiva, em vez de simplesmente o excluir após o facto (Griffin R., 2022);
- Regulamentações internacionais e nacionais: A falta de uma definição universal de discurso de ódio e de regulamentações nacionais variadas complicam a governação. No entanto, a interlegalidade, que envolve a cooperação entre as estruturas jurídicas internacionais e nacionais, pode ajudar a enfrentar estes desafios. (Bello B.G., 2023)

A terceira e última categoria que trata de **Abordar o Discurso de Ódio Online** exige intervenções tecnológicas, apoio público e uma abordagem de justiça social. As plataformas podem tanto facilitar quanto prevenir a propagação desse conteúdo, tornando essencial a implementação de soluções tecnológicas eficazes. O apoio à regulamentação depende da perceção da sua eficácia na mitigação dos danos. Além disso, uma abordagem centrada na justiça social pode proteger grupos vulneráveis, equilibrando segurança e liberdade de expressão. Na sequência apresentam-se como resultados, três sugestões sumarizadas de governança digital:

- Intervenções tecnológicas: os estudos sugerem que os recursos tecnológicos das plataformas de redes sociais podem facilitar e prevenir a propagação do discurso



de ódio. As intervenções eficazes exigem a compreensão destes determinantes digitais e a implementação de soluções baseadas na tecnologia (Weber I. et.al., 2023);

- Atitudes e apoio público: o apoio público à regulamentação é influenciado por experiências pessoais com o discurso de ódio e percepções dos seus danos sociais. As medidas regulamentares têm maior probabilidade de obter apoio se forem percebidas como eficazes na mitigação dos danos (Park A.; Kim M.; Kim E.-S., 2023);
- Abordagem de justiça social: uma abordagem de justiça social à governação da plataforma pode reduzir a circulação de conteúdos prejudiciais dirigidos a grupos marginalizados. Esta abordagem enfatiza a necessidade de políticas que protejam as comunidades vulneráveis e, ao mesmo tempo, equilibrem a liberdade de expressão (Otero P.V. ,2024).

Com base no resultado da consulta, a influência da regulamentação das redes sociais na prevenção do cibercrime e no enfrentamento do discurso de ódio online, bem como os desafios associados à eficácia em diferentes países, as considerações éticas e as inovações tecnológicas, possuem desafios significativos.

As diferenças nas definições de discurso de ódio e na responsabilização das plataformas variam conforme os contextos sociais, éticos, legais e políticos de cada país (Enarsson T., 2024). Na União Europeia, a tendência é ampliar a responsabilidade dos intermediários, como demonstrado pela Lei NetzDG da Alemanha, que inspirou outras legislações, apesar das suas limitações operacionais. (Yu W., 2018)

A implementação dessas regulamentações também levanta questões éticas, especialmente no equilíbrio entre a liberdade de expressão e a segurança digital, conforme discutido na Convenção Europeia dos Direitos Humanos (Griffin R., 2023; Bello B.G., 2023).

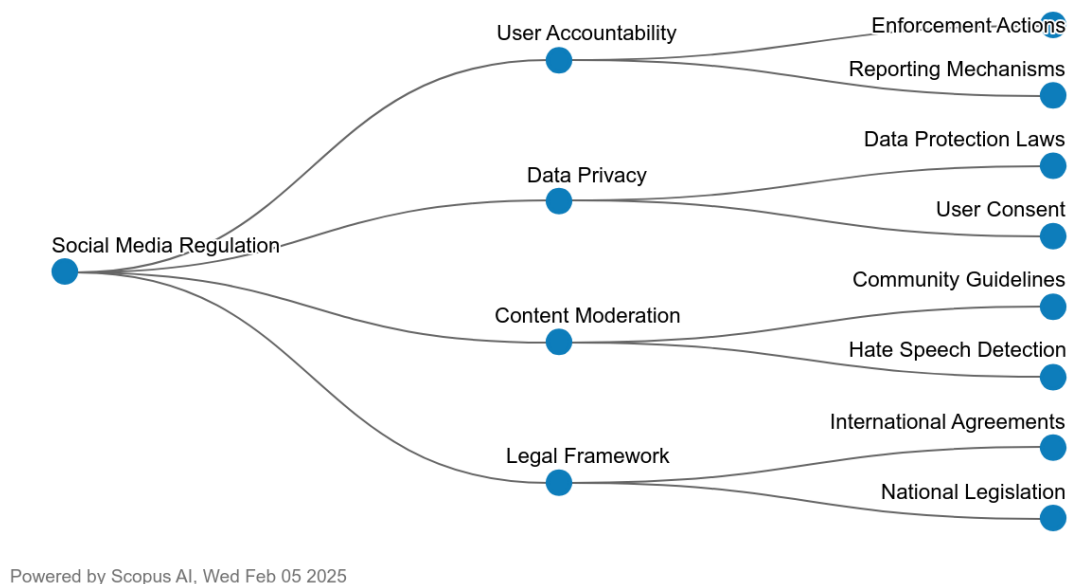
A evolução tecnológica surge como um complemento essencial à regulamentação, com pesquisas propondo novas abordagens para a detecção e classificação de discurso de ódio, como o uso de BiLSTM e reconhecimento de fala (Park A.; Kim M.; Kim E.-S., 2023). Contudo, a eficácia dessas soluções ainda exige avaliação aprofundada e adaptação a diferentes sistemas jurídicos. Assim, uma análise mais abrangente requer estudos adicionais para compreender melhor a efetividade das regulamentações em escala global.

O Mapa conceitual (Figura 1) gerado a partir da revisão dos documentos da base da Scopus apresenta que a regulação das redes sociais abrange diversos aspectos fundamentais para garantir um ambiente digital seguro e responsável.

A responsabilização do usuário é um dos pilares dessa regulação, envolvendo mecanismos como ações de aplicação, que punem violações das normas, e sistemas de denúncia, permitindo que os próprios usuários relatem conteúdos inadequados. Além disso, a privacidade de dados é um tema central, com leis específicas como o GDPR e a LGPD estabelecendo diretrizes sobre o uso de informações pessoais. O consentimento do usuário também se torna essencial para assegurar maior transparência na coleta e tratamento de dados dentro das plataformas.

Figura 1

Mapa conceitual relacionado a revisão de literatura.



Outro ponto crucial na regulação é a moderação de conteúdo, que busca equilibrar a liberdade de expressão com a necessidade de combater discursos de ódio e desinformação. As diretrizes da comunidade estabelecem normas internas para definir o que pode ou não ser publicado, enquanto tecnologias avançadas são utilizadas na detecção e remoção de conteúdos prejudiciais. Esse esforço visa criar um espaço digital mais inclusivo e respeitoso, evitando a proliferação de informações falsas ou ofensivas que possam impactar negativamente os usuários e a sociedade como um todo.

Por fim, a estrutura legal desempenha um papel essencial nesse processo,



contando com legislações nacionais e acordos internacionais que estabelecem padrões regulatórios para as redes sociais. A colaboração entre diferentes países e organizações permite a criação de normas mais eficazes e padronizadas, garantindo que as empresas de tecnologia cumpram suas obrigações legais. Dessa forma, a regulação das redes sociais exige um esforço conjunto entre governos, plataformas e usuários para promover um ambiente digital ético, equilibrando inovação e proteção dos direitos individuais.

5 CONCLUSÕES

A legislação global sobre cibercrime e o desenvolvimento de políticas têm ganhado cada vez mais relevância, refletindo o crescente reconhecimento da necessidade de um sistema legal robusto para combater as ameaças cibernéticas em escala global. A evolução das leis de cibersegurança é impulsionada pela crescente sofisticação das ciberameaças, que exigem respostas legais rápidas e adaptáveis. Em um mundo onde as atividades criminosas na internet atravessam fronteiras, a cooperação internacional torna-se essencial para a criação de um quadro legal eficaz.

As políticas de segurança cibernética devem ser constantemente revistas e aprimoradas para refletir os novos desafios apresentados pela inovação tecnológica, como os ataques de ransomware e os crimes digitais que exploram vulnerabilidades em sistemas interconectados.

A colaboração entre países, por meio de acordos e iniciativas multilaterais, têm o potencial de aumentar a eficácia na prevenção e mitigação das ciberameaças. A implementação de medidas legais mais harmonizadas e a criação de órgãos de governança transnacional podem melhorar a capacidade de resposta a incidentes cibernéticos. No entanto, a complexidade das jurisdições legais e as diferentes abordagens nacionais tornam a coordenação internacional um desafio. O desenvolvimento de legislações globais mais coesas pode também facilitar a detecção e a punição de criminosos cibernéticos, assegurando que as vítimas possam ser apoiadas, independentemente de onde os crimes ocorram.

A regulamentação e a governança das redes sociais emergem como um dos temas mais debatidos no contexto digital contemporâneo. As plataformas sociais têm um impacto profundo na sociedade, mas também são alvos frequentes de abuso, desinformação e violação da privacidade dos usuários.



O equilíbrio entre a liberdade de expressão e a necessidade de regulamentação eficaz tem sido um ponto central, com o desafio de implementar políticas que protejam os usuários sem comprometer os direitos fundamentais de comunicação. À medida que os regulamentos para a moderação de conteúdos e proteção de dados pessoais se tornam mais rigorosos, observa-se um aumento na pressão sobre as plataformas para aderirem a essas regras, resultando em um panorama dinâmico de governança digital.

A eficácia das regulamentações depende não apenas da aplicação interna, mas também da cooperação internacional para garantir a uniformidade das políticas. Ações regulatórias que envolvem várias nações têm o potencial de criar um ambiente mais seguro para os usuários, permitindo uma maior proteção contra conteúdos nocivos e práticas invasivas de dados. Contudo, a uniformização das políticas exige um compromisso internacional que equilibre as particularidades culturais e legais de cada país, ao mesmo tempo que promove um padrão global de segurança.

Assim, a regulação das redes sociais não se limita apenas ao aumento da privacidade do usuário, mas também à criação de um espaço digital mais saudável e responsável.



REFERÊNCIAS

- Ahmed, Arooj. (2021). Over 304 million ransomware threats surfaced in the first half of 2021. Retrieved from: <https://www.digitalinformationworld.com/2021/08/over-304-million-ransomware-threats.html>
- Althibyani, H. A., & Al-Zahrani, A. M. (2023). Investigating the Effect of Students' Knowledge, Beliefs, and Digital Citizenship Skills on the Prevention of Cybercrime. Sustainability, 15(15), 11512. <https://doi.org/10.3390/su151511512>
- Australian Government. (2021). Online Safety Act 2021. eSafety Commissioner. Retrieved from <https://www.esafety.gov.au/about-us/legislation/online-safety-act-2021>
- Bello, B. G. (2023). Tackling online hate speech from a European perspective: Potentials and challenges of inter-legality. Onati Socio-Legal Series, 13(4), 1376-1411. <https://doi.org/10.35295/OSLS.IISL/0000-0000-0000-1392>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101. <https://doi.org/10.1191/1478088706qp063oa>
- Câmara dos Deputados. (2020). Projeto de Lei 2630/2020 - Fake News. Retrieved from <https://www.camara.leg.br/propostas-legislativas/2252580>
- Damaraju, A. (2020). Social Media as a Cyber Threat Vector: Trends and Preventive Measures. Revista Espanola de Documentacion Cientifica, 14(1), 95-112.
- Dawson, M., & Thomson, R. (2021). The role of social media in the mitigation of cybercrimes. Journal of Cybersecurity, 7(3), 45-61. <https://doi.org/10.1093/cyber/cta123>
- Enarsson, T. (2024). Navigating hate speech and content moderation under the DSA: Insights from ECtHR case law. Information and Communications Technology Law. <https://doi.org/10.1080/13600834.2024.2395579>
- European Union. (2023). Digital Services Act. Publications Office of the European Union. Retrieved from <https://op.europa.eu/en/publication-detail/-/publication/4a5ee5d0-d91f-11ed-a05c-01aa75ed71a1/language-en>
- Federal Ministry of Justice. (2021). NetzDG - Netzwerkdurchsetzungsgesetz. Retrieved from <https://www.gesetze-im-internet.de/netzdg/>
- Federal Trade Commission. (2023). Children's Online Privacy Protection Rule (COPPA). Retrieved from <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>
- Gillespie, T. (2018). Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85051469782&partnerID=40&md5=8d850b5298b7e5dc1a1fcf4c427fe3da>
- Griffin, R. (2022). New school speech regulation as a regulatory strategy against hate



- speech on social media: The case of Germany's NetzDG. Telecommunications Policy, 46(9), 102411. <https://doi.org/10.1016/j.telpol.2022.102411>
- Kaur, G., Bonde, U., Pise, K. L., Yewale, S., Agrawal, P., Shobhane, P., Maheshwari, S., Pinjarkar, L., & Gangarde, R. (2024). Social Media in the Digital Age: A Comprehensive Review of Impacts, Challenges and Cybercrime. Engineering Proceedings, 62(1), 6. <https://doi.org/10.3390/engproc2024062006>
- Khiralla, F. A. M. (2020). Statistics of cybercrime from 2016 to the first half of 2020. International Journal of Computer Science and Network, 9(5), 252-261. Retrieve from: <https://ijcsn.org/articles/0905/Statistics-of-Cybercrime-from-2016-to-the-First-Half-of-2020.html> 10.13140/RG.2.2.30131.66088
- Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. Psychological Bulletin, 140(4), 1073-1137. <https://doi.org/10.1037/a0035618>
- Massanari, A. (2017). #Gamergate and The Fappening: How Reddit's algorithm, governance, and culture support toxic technocultures. New Media and Society, 19(3), 329-346. <https://doi.org/10.1177/1461444815608807>
- Matamoros-Fernández, A. (2017). Platformed racism: The mediation and circulation of an Australian race-based controversy on Twitter, Facebook and YouTube. Information, Communication & Society, 20(6), 930-946. <https://doi.org/10.1080/1369118X.2017.1293130>
- Otero, P. V. (2024). Platform governance and social justice: Governing hate speech on social media. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85210793364&partnerID=40&md5=4f96e8148ce0720751d29cd669e54dce>
- Park, A., Kim, M., & Kim, E.-S. (2023). SEM analysis of agreement with regulating online hate speech: Influences of victimization, social harm assessment, and regulatory effectiveness assessment. Frontiers in Psychology, 14, 1276568. <https://doi.org/10.3389/fpsyg.2023.1276568>
- Paulos, B., & Çelik, S. (2021). THE CHALLENGES OF REGULATING HATE SPEECH ON SOCIAL MEDIA IN LIGHT OF THE THEORY OF FREEDOM OF EXPRESSION. Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi, 11(1), 97-134. <https://doi.org/10.52273/sduhfd..922588>
- Planalto. (2014). Lei nº 12.965, de 23 de abril de 2014 - Marco Civil da Internet. Retrieved from http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/12965.htm
- Siegel, A. A., & Badaan, V. (2020). #No2Sectarianism: Experimental Approaches to Reducing Sectarian Hate Speech Online. American Political Science Review, 114(3), 837-855. <https://doi.org/10.1017/S0003055420000283>
- Tourkochorit, I. (2023). Balancing Freedom of Speech and Privacy in the Digital Services Act. European Law Journal. Recuperado de <https://chicagounbound.uchicago.edu/cjil/vol24/iss1/7/>



- Weber, I., Vandebosch, H., Poels, K., & Pabian, S. (2023). Features for Hate? Using the Delphi Method to Explore Digital Determinants for Online Hate Perpetration and Possibilities for Intervention. *Cyberpsychology, Behavior, and Social Networking*, 26(7), 479-488. <https://doi.org/10.1089/cyber.2022.0195>
- World Economic Forum. (2023). 2023 was a big year for cybercrime – here’s how we can make our systems safer. Recuperado de <https://www.weforum.org/meetings/annual-meeting-on-cybersecurity-2023/>
- Yu, W. (2018). Internet Intermediaries' Liability for Online Illegal Hate Speech. *Frontiers of Law in China*, 13(3), 342-356. <https://doi.org/10.3868/s050-007-018-0026-5>