


DEVELOPMENTS IN THE FIELD

Emerging Regulations on Content Moderation and Misinformation Policies of Online Media Platforms: Accommodating the Duty of Care into Intermediary Liability Models

Caio C. V. Machado¹  and Thaís Helena Aguiar² 

¹Lawyer and social scientist; Director of Instituto Vero (Brazil) and DPhil Candidate at the University of Oxford (UK). Fellow at Harvard SEAS. Caio holds a master's of law from the Sorbonne (France) and a master's in social science from the University of Oxford (UK). He graduated in Law from the University of São Paulo (Brazil)

²Lawyer; Researcher at Instituto Vero (Brazil). Graduate degree in Data Protection Law from the University of Lisbon (Portugal). Thaís graduated in Law from the Federal University of Pernambuco (Brazil)

Corresponding author: Caio C. V. Machado; Email: caio@vero.org.br

Abstract

Disinformation, hate speech and political polarization are evident problems of the growing relevance of information and communication technologies (ICTs) in current societies. To address these issues, decision-makers and regulators worldwide discuss the role of digital platforms in content moderation and in curtailing harmful content produced by third parties. However, intermediary liability rules require a balance that avoids the risks arising from the circulation at scale of harmful content and the risks of censorship if excessive burdens force content providers to adopt a risk-averse posture in content moderation. This piece examines the trend of altering intermediary liability models to include 'duty of care' provisions, describing three models in Europe, North America and South America. We discuss how these models are being modified to include greater monitoring and takedown burdens on internet content providers. We conclude with a word of caution regarding this balance between censorship and freedom of expression.

Keywords: Content moderation; Disinformation; Duty of care; Hate speech; Intermediary liability

1. Introduction

In recent years, the issue of online misinformation has prompted many countries to consider content moderation as a means of curtailing harmful content on the internet. These debates mark a significant departure from the previous approach of minimizing interference in the content transmitted by intermediaries on the internet, which marked regulation in the early 2000s. Content regulation is crucial to human rights as it relates to how freedoms are exercised online, and how democratic debate can be preserved in an increasingly digitally connected and networked society.

This piece examines the shift from models of least interference in content creation and dissemination to an active 'duty of care' that requires intermediaries to monitor and take

action against harmful content on their platforms. Specifically, we explore three existing models of intermediary liability in large democracies in Europe, North America and South America, and describe their key characteristics. We also examine how these models are evolving under similar provisions, such as the European Union's Digital Services Act, the British Online Safety Bill, the German NetzDG, and the anticipated Brazilian Fake News Bill.

Intermediary liability refers to the legal responsibility of intermediaries such as internet service providers (ISPs), social media platforms, search engines, web hosting companies, and content delivery networks for the content transmitted or stored on their platforms.¹ If the content is found to be illegal or infringing on the rights of others, these intermediaries can be held liable.² In this piece, we focus on the responsibility of content providers like social media platforms and search engines.

Content moderation involves reviewing, monitoring and managing user-generated content on online platforms to identify and remove content that violates the platform's policies or community guidelines. This process uses automated tools and human moderators to eliminate hate speech, bullying, spam and illegal content.³

Regulating content removal is a critical issue that affects online freedoms and democratic debate. As the internet continues to evolve, it is essential to maintain a balance between protecting individuals' rights and minimizing harmful content. The intermediary liability and content moderation models are evolving, and policymakers must continue to consider their effectiveness and impact on human rights.

The 'fake news' debate exposes a deeper issue: the reorganization of existing business models of the communications ecosystem. In the past, media conglomerates produced and distributed information in society.⁴ However, data-driven advertising business models now dominate the digital ecosystem, pushing communications companies to produce attention-grabbing and identity-confirming content. This results in a highly segmented information spaces, with echo chambers that promote disparate spaces of information consumption, political views, and even understandings of reality.⁵

To respond to the fast-growing and far-reaching informational challenges, countries have decided to review their models of intermediary responsibility to encompass mandatory rules for content moderation. While the traditional understanding of human rights preconcized by Article 19 of the International Covenant on Civil and Political Rights (ICCPR)⁶ was one of non-interference and authorization of speech, new means of limiting and removing content are now necessary as a means of sustaining freedom of expression and balancing other rights. The rising understanding is that content providers should have

¹ Media Defense, 'Intermediary Liability', <https://www.mediadefence.org/ereader/publications/introductory-modules-on-digital-rights-and-freedom-of-expression-online/module-3-access-to-the-internet/intermediary-liability/#:~:text=Intermediary%20liability%20occurs%20where%20governments,copyright%20infringements%2C%20digital%20piracy%2C%20trademark> (accessed 30 March 2023).

² Konstantinos Komaitis, 'Intermediary Liability: The Hidden Gem', *Internet Society* (11 March 2020), <https://www.internetsociety.org/blog/2020/03/intermediary-liability-the-hidden-gem/> (accessed 30 March 2023); Christoph Schmon and Haley Pedersen, 'Platform Liability Trends Around the Globe: Taxonomy and Tools of Intermediary Liability', *Electronic Frontier Foundation* (25 May 2022), <https://www.eff.org/pt-br/deeplinks/2022/05/platform-liability-trends-around-globe-taxonomy-and-tools-intermediary-liability> (accessed 30 March 2023).

³ Sarah T Roberts, 'Content Moderation', in Laurie A Schintler and Connie L McNeely (eds.), *Encyclopedia of Big Data* (Cham: Springer International Publishing, 2022).

⁴ Yochai Benkler, Robert Faris and Hal Roberts, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics* (New York: Oxford University Press, 2018).

⁵ Amy Ross Arguedas et al, 'Echo Chambers, Filter Bubbles, and Polarisation: A Literature Review', <https://reutersinstitute.politics.ox.ac.uk/echo-chambers-filter-bubbles-and-polarisation-literature-review> (accessed 30 March 2023)

⁶ International Covenant on Civil and Political Rights, United Nations General Assembly Resolution 2200A (XXI) (adopted 16 December 1966).

obligations to moderate content more actively, and even be held accountable when they fail to contain harmful content being disseminated over their services.⁷

In the next section, we will explore three existing models in large democracies in North America, Latin America and Europe. These models address the issues of intermediary responsibility and content moderation and provide different approaches to maintaining freedom of expression while limiting the circulation of harmful information.

II. Models of Limited Intermediary Liability

We will look at three models of intermediary liability. The American model provides immunity for third-party content and content moderation.⁸ The European model suggests immunity with a ‘notice and takedown’ approach.⁹ Meanwhile, the Brazilian model offers immunity for third-party content, but content providers may be liable for wrongfully removing content.¹⁰ These models, which we will explore in greater detail below, demonstrate that intermediary liability is centred on protecting content providers from the harm caused by third-party content. However, the methods of content removal differ across these models.

The American Model: Section 230 of the Communications Decency Act of 1996

In the US model, established in Section 230 of the Communications Decency Act of 1996 (CDA), ‘no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider’.¹¹ This provision assigns the responsibility of published content to its authors, as opposed to the content providers. It allows companies to build their digital products and services with less risk and was considered essential for the economic development of the internet economy.¹² This reflects a vision that content providers are also part of a ‘dumb pipe’ system, which favours Freedom of Expression because the protection granted to intermediaries is a protection that extends to the users of their services.¹³

This immunity, however, is not unlimited. Federal criminal laws, illegal or harmful content, and copyright violations¹⁴ are examples of norms [or rules] that assign duties to platforms.

⁷ Talita Dias, ‘Tackling Online Hate Speech through Content Moderation: The Legal Framework Under the International Covenant on Civil and Political Rights’, *Countering Online Hate and its Offline Consequences in Conflict-Fragile Settings* (forthcoming) (30 June 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4150909 (accessed 30 March 2023).

⁸ Communications Decency Act of 1996 (CDA), Pub. L. No. 104-104 (Tit. V), 110 Stat. 133 (8 February 1996), codified at 47 U.S.C. §§223, 230.

⁹ European Parliament, ‘Reform of the EU Liability Regime for Online Intermediaries’, May 2020, [https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRS_IDA\(2020\)649404_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRS_IDA(2020)649404_EN.pdf) (accessed 30 March 2023)

¹⁰ Flávio Rech Wagner and Diego Rafael Canabarro, ‘Study – An Assessment of Marco Civil’s Intermediary Liability Framework’, *Internet Society Brazil Chapter* (19 May 2021), <https://isoc.org.br/noticia/study-an-assessment-of-marco-civil-s-intermediary-liability-framework> (accessed 30 March 2023).

¹¹ 47 U.S.C. § 230(c)(1).

¹² Ashley Johnson and Daniel Castro, ‘Overview of Section 230: What It Is, Why It Was Created, and What It Has Achieved’, *Information Technology and Innovation Foundation* (ITIF) (22 February 2021), <https://itif.org/publications/2021/02/22/overview-section-230-what-it-why-it-was-created-and-what-it-has-achieved/> (accessed 03 April 2023).

¹³ Electronic Frontier Foundation (EFF), ‘Section 230’, <https://www.eff.org/issues/cda230> (accessed 30 March 2023).

¹⁴ US Congress, H.R.2281 – 105th Congress (1997–1998): Digital Millennium Copyright Act (28 October 1998), <https://www.congress.gov/bill/105th-congress/house-bill/2281> (accessed 30 March 2023); Copyright Alliance, ‘Copyright Law Explained: The DMCA Notice and Takedown Process’, <https://copyrightalliance.org/education/>

Moreover, the law also authorizes intermediaries to moderate content and protects the removal of content that has been done in good faith. It is the Good Samaritan principle set out in Section 230(c)(2): operators of interactive computer services are exempt from liability when, in good faith, they remove or moderate third-party material that they deem ‘obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected’.

The Previous EU Model: Articles 12 to 15 of the European Union’s 2000 E-Commerce Directive

The Directive on Electronic Commerce, also known as the E-commerce Directive,¹⁵ was adopted by the European Union in 2000. Its main purpose is to establish a legal framework for electronic commerce in the EU and facilitate cross-border online transactions. The directive applies to a wide range of online services, including e-commerce platforms, social media platforms and search engines. One of the key provisions of the directive is the safe harbour provision, which protects intermediaries from liability for the content that they transmit or store on their platforms.

Similar to the American model, this provision is intended to encourage innovation and free expression on the internet by limiting the legal liability of intermediaries. However, the directive also establishes conditions under which intermediaries can be held liable for illegal content transmitted or stored on their platforms. These include cases where the intermediary has actual knowledge of illegal activity or information on their platform or where they fail to promptly remove such content once they become aware of it. Additionally, the directive provides for a notice and takedown procedure, which allows individuals or organizations to request the removal of illegal content from intermediaries’ platforms.

The Brazilian Model: Article 19 of the ‘Internet Bill of Rights’

The Brazilian model of intermediary liability, as described in Article 19 of the Brazilian Civil Rights Framework for the Internet,¹⁶ also establishes that internet intermediaries are not responsible for the content generated by third parties. However, intermediaries can be required to remove content that is deemed illegal by court order, violate intellectual property rights, or contain unauthorized nudity.

The Brazilian model has obtained international relevance because it counts on a judicial revision to appreciate issues related to Freedom of Expression. Unlike the American model, which grants content providers immunity in the acts of content moderation, the Brazilian model understands that these practices can violate rights and are subject to legal liability. This is why articles 19 and 21 of Marco Civil clarify the standards to be met to balance moderation of harmful content and freedom of expression, a fundamental right reinforced several times in the law.

Interestingly, these mechanisms are now converging towards more stringent obligations of monitoring and removing content which we will see in the following section.

[copyright-law-explained/the-digital-millennium-copyright-act-dmca/dmca-notice-takedown-process/#:~:text=What%20is%20a%20DMCA%20Takedown,websites%20and%20other%20internet%20sites](https://copyright-law-explained.com/the-digital-millennium-copyright-act-dmca/dmca-notice-takedown-process/#:~:text=What%20is%20a%20DMCA%20Takedown,websites%20and%20other%20internet%20sites) (accessed 30 March 2023); US Copyright Office, ‘The Digital Millennium Copyright Act’, <https://www.copyright.gov/dmca/> (accessed 30 March 2023).

¹⁵ Directive 2000/31/EC, OJ L 178, 17.7.2000, pp 1–16.

¹⁶ Law no. 12965/2014 (*Marco Civil da Internet*) (Brazil), art 19.

III. The Rise of a Duty of Care

Intermediary liability solutions have aimed to mitigate the liability of content providers for third-party content they host. However, the methods for content removal were highly localized, where each jurisdiction built their own approach to striking down harmful content based on their national view of balancing Freedom of Expression. The emergence of issues like misinformation and hate speech online, which pose threats to democracy, physical and mental safety, and public health, has prompted countries to reconsider their stance. These developments, along with debates about the role of internet content providers in distributing online content, have led to new regulatory arrangements that place greater responsibilities on content providers for removing harmful content. However, this model places the burden on content providers to make legal judgements about the content circulating online. This raises concerns about their lack of legitimacy to validate political speech and the challenge of handling the volume of online communications with the aid of automated tools, which can suppress speech at large scale if left unchecked.

The German NetzDG of 2017

In Europe, for instance, Germany passed in 2017 the Network Enforcement Act (Netzwerkdurchsetzungsgesetz, or simply 'NetzDG'), a regulation that explicitly 'aims to fight hate crime, criminally punishable fake news and other unlawful content on social networks more effectively'¹⁷ and increases the rigor in holding intermediaries accountable. Generally, the law creates a list of situations that oblige platforms to carry out the summary removal of content.

Among its innovations, the new rules require more transparency from content providers and expedited response to users' complaints. According to the rules of effective complaints management, which establish a standard with more transparency and efficiency, operators of social networks 'must offer users an easily recognizable, directly accessible and permanently available procedure for reporting criminally punishable content', as well as 'immediately take notice of content reported to them by users and examine whether that content might violate criminal law'.

From a practical perspective, NetzDG's added rigor to pre-existing legal obligations did not necessarily lead to the desired changes. In fact, in the same year it entered into force, a study has shown that the law did not result in widespread calls for takedowns, nor has it compelled intermediaries to adopt a 'take down, ask later approach'. However, uncertainty as to whether it would effectively prevent hate speech remained in the air.¹⁸

The stringent law has been immediately criticized for posing threats to online free speech since its content moderation strict rules, applied to social media companies, could incentivize intermediaries to over-police speech.¹⁹ For these reasons, Germany passed the

¹⁷ German Bundestag, Network Enforcement Act (Netzwerkdurchsetzungsgesetz, NetzDG); Bundesministerium des Justiz, 'Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act, NetzDG) – Basic Information (2017)', https://www.bmj.de/DE/Themen/FokusThemen/NetzDG/NetzDG_EN_node.html (accessed 30 March 2023).

¹⁸ Counter Extremism Project, 'ICYMI: New Report on Germany's NetzDG Online Hate Speech Law Shows No Threat of Over-Blocking' (27 November 2018), <https://www.counterextremism.com/press/icymi-new-report-germany%E2%80%99s-netzdg-online-hate-speech-law-shows-no-threat-over-blocking> (accessed 30 March 2023).

¹⁹ Diana Lee, 'Germany's NetzDG and the Threat to Online Free Speech,' *Yale Law School Media Freedom & Information Access Clinic* (10 October 2017), <https://law.yale.edu/mfia/case-disclosed/germanys-netzdg-and-threat-online-free-speech> (accessed 30 March 2023).

Act to Amend the Network Enforcement Act, which entered into force on 28 June 2021,²⁰ with notable changes to the user-friendliness of complaint procedures,²¹ appeals procedure and arbitration, transparency reports, and expansion of powers of the Federal Office of Justice.²²

The European Union's Digital Services Act (DSA) of 2022

Recently, the European Union approved a digital strategy consisting of two norms: the Digital Services Act²³ and the Digital Markets Act.²⁴ Together, the laws form a normative framework that seeks to establish a safe digital environment that can both meet competition aspects and protect users' fundamental rights.

The DSA, updating European regulation, sought to bring more incisive rules to digital services in general, which 'include a large category of online services, from simple websites to internet infrastructure services and online platforms'.²⁵ In this way, the digital strategy reaches a variety of providers, even if it recognizes that it has a primary focus on intermediaries and digital platforms – online marketplaces, social networks, content-sharing platforms, and others.

Two critical provisions in the new European regulation are the due diligence obligations and systemic risk monitoring. The due diligence obligations, which can be interpreted as a duty of care, impose new legal obligations on digital services by establishing a list of measures considered reasonable to avoid damage to users, under penalty of having negligence recognized and, therefore, subjecting these platforms to liability. Meanwhile, systemic risk monitoring is an obligation directed at very large online platforms (VLOPs) that impose the monitoring and surveillance of harmful trends such as disinformation and hate speech.²⁶ Along the same lines, VLOPs will be subject to annual independent audits, as well as being obliged to offer users at least one recommendation system option that is not based on user activity on the network (profiling).

So far, all that can be said is that the changes in European regulation have made the rules governing accountability for digital services more rigid and aim to create a more secure and competitive digital environment, which will benefit both the economy and individual freedoms. Whether these goals will be achieved or how well they will be achieved, as well as possible new problems are still questions in the open air, as the new rules have not yet come into force.

²⁰ Library of Congress, 'Germany: Network Enforcement Act Amended to Better Fight Online Hate Speech', <https://www.loc.gov/item/global-legal-monitor/2021-07-06/germany-network-enforcement-act-amended-to-better-fight-online-hate-speech/> (accessed 30 March 2023).

²¹ NetzDG § 3, para 1 and explanatory memorandum, 17.

²² Deutscher Bundestag, Entwurf eines Gesetzes zur Änderung des Netzwerkdurchsetzungsgesetzes, Drucksache 19/18792 27.04.2020, <https://dserver.bundestag.de/btd/19/187/1918792.pdf> (accessed 30 March 2023).

²³ European Parliament and Council of Europe, Regulation (EU) 2022/2065, OJ L 277, 27.10.2022, pp 1–102; European Commission, 'The Digital Services Act: Ensuring a Safe and Accountable Online Environment', https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en (accessed 30 March 2023).

²⁴ European Parliament and Council of Europe, Regulation (EU) 2022/1925, OJ L 265, 12.10.2022, pp 1–66; European Commission, 'The Digital Markets Act: Ensuring Fair and Open Digital Markets', https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en (accessed 30 March 2023).

²⁵ European Commission, 'The Digital Services Act Package', <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> (accessed 30 March 2023).

²⁶ Eliska Pirkova, 'The Digital Services Act: Your Guide to the EU's New Content Moderation Rules', *Access Now* (6 July 2022), <https://www.accessnow.org/digital-services-act-eu-content-moderation-rules-guide/> (accessed 30 March 2023).

Duty of Care in Other Countries: USA, UK and Brazil

In the US, Section 230 rules have been challenged across the political spectrum. Republicans oppose content moderation because they understand that there is significant damage to freedom of expression, despite the intention to manage harmful content. On the other hand, Democrats understand that the immunity granted to platforms does not meet the objective of making the digital environment safer precisely because it promotes inertia in the face of materials that cause greater damage and circulate freely on networks. Still, despite political divergences, a survey showed that most US citizens favour eradicating harmful misinformation over protecting free speech.²⁷

Several civil society organizations argue that internet freedom of expression could not be the same without Section 230.²⁸ On the other hand, the provisions are not free from controversy either: today, many claim that Section 230 is a tool that grants undue immunities to platforms and disregards social media's ability to stop the spread of false information and hate speech. Section 230 has already been the object of more than 25 legislative measures that attempt to abolish or alter it due to the demand on platforms to have greater accountability.²⁹ In Brazil, Bill no. 2630/2020 (nicknamed *PL das Fake News*)³⁰ offered a proposal to combat online disinformation. Over the last three years, the Bill has undergone developments, particularly after the invasions of the three powers in Brasilia in 2023.

Proposed during the pandemic, PL2630 emerged in a context of informational disorder and had as its initial focus the fight against disinformation. Over time, the engagement of social sectors in the legislative discussion made the project take on a proposal quite different from the initial one and, today, PL2630 has taken on the outlines of a platform regulation proposal. The core of the project remains centred on user rights and transparency in content moderation, which can be understood on three fronts: broad transparency, as in general reports and statistics made available by platforms; systemic transparency and analysis of the risks posed by digital services to fundamental freedoms, which relates to issues of algorithmic transparency; and individual transparency, with clarifications to the user about decision-making in content moderation and its fundamentals. However, the project still contains controversial parts and is a hot and disputed agenda in the National Congress. The Bill had its urgency approved in April³¹ and is still awaiting a vote,³² amid a contentious debate that includes intense publicity and the public positioning of digital platforms regarding PL2630.³³

²⁷ Anastasia Kozyreva et al, 'Resolving Content Moderation Dilemmas Between Free Speech and Harmful Misinformation' (2023) 120:7 *Proceedings of the National Academy of Sciences* e2210666120.

²⁸ Electronic Frontier Foundation (EFF), 'Section 230', <https://www.eff.org/issues/cda230> (accessed 30 March 2023).

²⁹ Jeff Kosseff, 'A User's Guide to Section 230, and a Legislator's Guide to Amending It (or Not)' (2022) 37:2 *Berkeley Technology Law Journal*; United States Department of Justice Archives, 'Department of Justice's Review of Section 230 of the Communications Decency Act of 1996', <https://www.justice.gov/archives/ag/department-justice-s-review-section-230-communications-decency-act-1996> (accessed 30 March 2023).

³⁰ Senado Federal, Projeto de Lei no. 2630, de 2020 (Lei das Fake News), <https://www25.senado.leg.br/web/atividade/materias/-/materia/141944> (accessed 30 March 2023).

³¹ Câmara dos Deputados, 'Projeto das fake news tem urgência aprovada e irá a voto na próxima terça' (25 April 2023), <https://www.camara.leg.br/noticias/955642-projeto-das-fake-news-tem-urgencia-aprovada-e-ira-a-voto-na-proxima-terca-acompanhe/> (accessed 30 April 2023).

³² Heloisa Cristaldo, 'Arthur Lira retira de pauta votação do PL das Fake News' (2 May 2023), <https://agenciabrasil.ebc.com.br/politica/noticia/2023-05/arthur-lira-retira-de-pauta-votacao-do-pl-das-fake-news> (accessed 03 May 2023).

³³ Supremo Tribunal Federal, 'STF determina remoção de anúncios com ataques ao PL das Fake News' (2 May 2023), <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=506578&ori=1> (accessed 3 May 2023);

In the United Kingdom, the Online Safety Bill places a duty of care on internet service providers to keep users safe. In doing so, it also notes that companies should have regard for privacy and freedom of expression concerns.³⁴ Although framed in broad terms, the duty of care consists of three distinct duties, defined from sections 9 to 11 of the Bill: protection of users from illegal content (section 9); additional measures to protect children's online safety (section 10); and protection of all users from harmful content, although not illegal, for services with broader reach and magnitude (section 11). Like other regulations, the Online Safety Bill has faced criticism for imposing duties that can burden providers and potentially facilitate censorship.³⁵

IV. Conclusion

Intermediary liability is undergoing significant changes that will force internet content providers to take on greater responsibility for the risks associated with their activities. This includes the dissemination of harmful content like misinformation and hate speech. However, there are concerns that this will decrease the relative immunity that these providers have for hosting third-party content, impacting both economic incentives and human rights. The economic capacity of developing automated tools and sustaining teams that are capable of operating content moderation in such expedited time frames is also a concern.

While combating harmful content is a valid goal, the challenge lies in identifying illegal forms of speech and creating mechanisms to remove them without over-moderating content. Economic incentives to suppress speech more actively arising from stricter rules may make it harder for people to communicate online, potentially chilling speech on these platforms.

Financial support. No funding was received for preparation of this article.

Competing interest. Authors Caio C. V. Machado and Thaís Helena Aguiar declare none.

Folha, 'Telegram distorce PL das Fake News e fala em censura e fim da liberdade de expressão' (9 May 2023), <https://www1.folha.uol.com.br/poder/2023/05/telegram-distorce-pl-das-fake-news-e-fala-em-censura-e-fim-da-liberdade-de-expressao.shtml> (accessed 9 May 2023).

³⁴ Online Safety Bill, HL Bill 87 (Rev) 58/3 (UK), <https://bills.parliament.uk/bills/3137> (accessed 30 March 2023).

³⁵ Markus Trengove et al, 'A Digital Duty of Care: A Critical Review of the Online Safety Bill' (13 April 2022), <http://doi.org/10.2139/ssrn.4072593> (accessed 30 March 2023).