SOCIAL MEDIA ALGORITHMS AND FREE SPEECH: BALANCING RIGHTS UNDER THE DSA AND GDPR

Adebukola Omobolanle Oso[1] adebukolaoso2024@gmail.com Lead City University +2347044044344
Esther-Mary Olufunke Umeano[2] funkeumeano@gmail.com +2347061901131
Wilson Sakpere[3] sakpere.wilson@lcuedu.ng +2348159582869

Abstract

This article examines the intricate relationship between social media algorithms, free speech, and data protection within the European Union's Digital Services Act (DSA) and General Data Protection Regulation (GDPR). Focusing on pertinent provisions of Articles 12, 26, 27, 34, and 40 of the DSA, and Articles 5, 15, 17, 22, and 35 of the GDPR, the analysis delves into the challenges of algorithmic transparency, content moderation, and automated decision-making. The DSA mandates platforms to disclose content moderation policies and algorithmic processes, aiming to enhance accountability. However, this requirement raises concerns about revealing proprietary information and the potential for over-censorship, thereby impacting free expression. Conversely, the GDPR's restrictions on automated decision-making and data processing present obstacles for platforms that rely on personalization algorithms, potentially affecting user experience and innovation. The GDPR and DSA set global standards for digital governance, influencing how global tech companies (like Meta, X/Twitter, YouTube, and Tik-Tok) manage user data and content. This is because these companies operate in Nigeria, their policies shaped by the DSA and GDPR affect Nigerian users — from how content is moderated to how personal data is handled. This study employs a doctrinal legal research methodology, reviewing legal texts, policy papers, case law, and scholarly articles to propose a balanced approach. Recommendations include adopting context-specific regulations, enhancing transparency without compromising trade secrets, and empowering users through informed consent and control over personal data. Such measures are essential to harmonize the protection of free speech and privacy in the evolving digital landscape.

Keywords: Social Media Algorithms, Free Speech, Digital Services Act (DSA), General Data Protection Regulation (GDPR), Algorithmic Transparency, Content Moderation, User Data Protection.

[1] LLB (Hons), PGDip SP&C, LLM, PhD Candidate, Lead City University, Ibadan. Email: adebukolaoso2024@gmail.com
[2] BA , LLB, LLM, MPHIL ,PGD, PhD Candidate Lead City University Ibadan.
[3] PhD, Lecturer and Head of Computer Science Lead City University Ibadan. Email: sakpere.wilson@lcuedu.ng

1.0 Introduction

The proliferation of social media platforms has significantly reshaped global communication, with artificial intelligence (AI) technologies playing an instrumental role in curating content and shaping public discourse. As AI continues to drive algorithmic decision-making in content regulation, its implications for fundamental rights, particularly the right to privacy and freedom of expression, have garnered increasing attention from scholars, policymakers, and legal practitioners[4]. Social media platforms, relying heavily on algorithms for user interaction and content personalization, face complex challenges in balancing these rights within the rapidly evolving digital landscape[5].

In response to these challenges, the European Union has introduced the Digital Services Act (DSA)[6] and the General Data Protection Regulation (GDPR)[7], two legislative frameworks designed to regulate platform operations and safeguard individual rights. While both pieces of legislation aim to promote transparency and enhance user protection, they also present distinct challenges in regulating algorithmic processes. The tension between safeguarding personal data and ensuring freedom of expression remains a fundamental concern for platforms, regulators, and users alike. This introduction critically examines the intersection of the GDPR and DSA, highlighting their role in regulating algorithmic content moderation and identifying the key legal challenges of balancing privacy, free speech, and innovation in the digital age.

1.1. The GDPR: Navigating Data Protection Challenges

The General Data Protection Regulation (GDPR) 8 primarily focuses on enhancing data protection and user privacy, empowering individuals with greater control over their personal data. Provisions of the GDPR such as Articles 22, 5, 15, 17, and 35 impose stringent

[4] Council of Europe, Regulating Content Moderation on Social Media to Safeguard Freedom of Expression (Committee on Culture, Science, Education and Media, 2023) https://rm.coe.int/as-cult-regulating-content-moderation-on-social-media-to-safeguard-fre/1680b2b162 accessed 22 January 2025.

[5] Reviglio, U., & Agosti, C. (2020). Thinking Outside the Black-Box: The Case for "Algorithmic Sovereignty" in Social Media. Social Media + Society, 6. https://doi.org/10.1177/2056305120915613.

[6] Frosio, G. & Geiger, C. (2023). Taking fundamental rights seriously in the Digital Services Act's platform liability regime. European Law Journal, 31-77. First published 21 November 2023. Retrieved from https://onlinelibrary.wiley.com/doi/10.1111/eulj.12475 Accessed 28 December 2024.

[7] Hoofnagle, C., Van Der Sloot, B., & Borgesius, F. (2019). The European Union general data protection regulation: what it is and what it means*. Information & Communications Technology Law, 28, 65 - 98. https://doi.org/10.1080/13600834.2019.1573501.

requirements on consent, data security, and transparency, reflecting the regulation's commitment to privacy rights. [8]However, the GDPR also creates challenges for platforms that rely on complex algorithms for content curation and user engagement. Article 22 introduces ambiguity around automated decision-making, leaving platforms to navigate the delicate balance between algorithmic efficiency and compliance with data protection requirements. Meanwhile, the right of access (Article 15) and right to erasure (Article 17) further complicate algorithmic processes, as platforms must manage users' requests for data access and deletion without undermining the functionalities of personalized content. In essence, the GDPR seeks to protect privacy while imposing constraints on algorithmic processes, creating a tension between operational flexibility and regulatory compliance[9].

1.2 The DSA: Transparency and Content Moderation

In contrast, the DSA focuses on platform accountability, transparency in content moderation, and user protection. Articles 12, 26, 27, 34, and 40 mandate that platforms disclose their algorithmic processes and act promptly to remove illegal content. These provisions aim to increase accountability, protect users from harmful content, and ensure transparency in algorithmic decision-making. [10]However, the DSA raises concerns about over-censorship, with platforms potentially suppressing legitimate content to avoid penalties. The pressure to conform to regulatory requirements might lead platforms to over-censor, stifling free speech and innovation. Additionally, the obligation to disclose proprietary algorithms presents challenges for platforms in safeguarding their commercial interests, as revealing algorithmic models could undermine competitive advantages and technological development[11].

1.3. Ethical Considerations and the Future of Algorithmic Regulation

Despite the ambitions of both the GDPR and DSA, their regulatory frameworks face limitations, particularly in addressing biases within AI models and ensuring that algorithmic decisions respect the diverse needs of users across cultural, social, and economic contexts. Algorithms

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1.
[9] Kaminski, M., & Malgieri, G. (2019). Algorithmic Impact Assessments under the GDPR: Producing Multi-layered Explanations. Cybersecurity. https://doi.org/10.2139/ssrn.3456224.
[10] https://digital-strategy.ec.europa.eu/en/policies/dsa-impact-platforms
[11] European Commission. (2022). Artificial Intelligence Act: Proposal for a Regulation.

have often been criticized for perpetuating bias, reinforcing stereotypes, and unfairly treating marginalized groups. Scholars such as Bryson (2019)[12] and Singhal (2023)[13] argue that AI governance should incorporate ethical frameworks that emphasize fairness, accountability, and transparency. These ethical considerations are vital as platforms deploy AI-driven systems and regulators grapple with the broader societal impacts of these technologies. Thus, a comprehensive understanding of the legal frameworks that govern algorithmic decision-making is necessary, with an emphasis on fairness and equity in their application. Balancing privacy rights, free speech, and innovation requires an ongoing examination of existing legal structures and their ability to evolve with emerging challenges in digital governance.

This article critically analyzes the interplay between the DSA and GDPR in the context of social media algorithms, free speech, and data protection. By exploring the legal tensions, challenges, and ethical dimensions, it aims to offer insights into how these frameworks can more effectively balance user rights and platform responsibilities while fostering innovation in a rapidly advancing digital landscape.

2.0. Challenges

Social media platforms, powered by complex algorithms, have become essential tools for communication, entertainment, and political discourse. However, the algorithms designed to curate and recommend content can have significant implications for free speech, privacy, and individual rights[14]. With the rise of social media giants like Facebook, Twitter (now X), and Instagram, the European Union (EU) has sought to regulate the digital space with legal frameworks such as the Digital Services Act (DSA) and General Data Protection Regulation (GDPR). These regulations aim to balance the need for consumer protection, the safeguarding of

[12] Joanna J. Bryson (2019). "The Artificial Intelligence of the Ethics of Artificial Intelligence: An Introductory Overview for Law and Regulation."
[13] Singhal, M., et al., Transparency and Accountability in AI Systems: Safeguarding Wellbeing, Frontiers in Human Dynamics (2023), https://www.frontiersin.org/journals/human-dynamics/articles/10.3389/fhumd.2024.1421273/full, accessed 22 January 2025.

[14] Segado-Boj, F., & Díaz-Campo, J. (2020). Social media and its intersections with free speech, freedom of information and privacy. An analysis. Revista ICONO14 Revista científica de Comunicación y Tecnologías emergentes. https://doi.org/10.7195/ri14.v18i1.1379.

free speech, and the management of personal data within a rapidly evolving digital ecosystem.

2.1 Legal Foundations: The DSA and GDPR

The DSA, which came into force in November 2022, establishes a legal framework to regulate online platforms in Europe. It seeks to tackle illegal content, disinformation, and other harmful activities by requiring greater transparency in algorithmic decision-making and content moderation[15]. The DSA provides mechanisms to challenge content removals and algorithmic decisions, fostering greater accountability of platforms[16]. However, it also raises concerns regarding the overreach of regulatory powers and the potential stifling of free speech, especially when algorithms are used to detect and remove content deemed harmful or illegal.

The GDPR, which governs data protection and privacy, imposes strict requirements on how platforms collect, process, and share user data. It grants users the right to be forgotten, demands explicit consent for data usage, and mandates transparency in the use of personal data for profiling and targeting[17]. This regulation has a direct influence on social media algorithms, which often rely on user data for personalization, targeting, and recommendation systems. Balancing the rights to privacy and data protection with the functionality of algorithmic systems is a core challenge that intersects with freedom of speech.

2.2 Challenges in Balancing Rights: Algorithmic Transparency and Free Speech

One of the primary challenges in balancing free speech with the need for regulation lies in the transparency of algorithms. Social media algorithms are often treated as proprietary secrets by platform providers, which makes it difficult for regulators, users, and advocacy groups to assess their fairness and impact on content dissemination[18]. This lack of transparency raises concerns over the censorship of legitimate expression and algorithmic bias, which can disproportionately

---

[15] European Commission, The Digital Services Act: Ensuring a Safe and Accountable Online Environment, (2022) https://ec.europa.eu/digital-strategy/digital-services-act-ensuring-safe-and-accountable-online-environment_en, accessed 12 January 2025.

[16] Schneider, P., & Rizoiu, M. (2023). The effectiveness of moderating harmful online content. Proceedings of the National Academy of Sciences of the United States of America, 120. https://doi.org/10.1073/pnas.2307360120.

[17] Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). Springer.

[18] Sun, Haochen, The Right to Know Social Media Algorithms, 18(1) Harvard Law & Policy Review (2024) https://journals.law.harvard.edu/lpr/wp-content/uploads/sites/89/2024/08/18.1-Right-to-Know-Social-Media-Algorithms.pdf, accessed 16 January 2025.

affect marginalized groups or specific political views[19].

For example; the controversy surrounding Facebook's handling of political advertisements and misinformation during the 2016 U.S. Presidential Election and the 2019 European Parliament elections highlighted the unintended consequences of algorithmic amplification and content moderation[20]. Facebook's algorithm was accused of amplifying misleading content, while simultaneously removing legitimate political discourse under the guise of combatting disinformation, thus exacerbating the tension between regulation and free speech.

Additionally, the issue of moderation of harmful content creates friction between the DSA's regulatory goals and the right to free expression. The DSA requires platforms to remove illegal content promptly, but this might conflict with the fundamental right to share and access information. Content moderation can lead to the over-removal of content that is not necessarily harmful but may be flagged due to algorithmic misclassification[21]. For instance, platforms like YouTube have been criticized for over-removing videos that do not violate policies but are flagged by algorithms as potentially harmful[22].

2.3. Privacy Concerns: The Role of the GDPR in Algorithmic Regulation

The GDPR plays a significant role in regulating the ways in which social media algorithms operate by restricting how personal data can be used to influence user experiences. The regulation mandates that platforms disclose the purposes of data collection, the types of data being collected, and the methods used for profiling and targeting users[23]. However, this transparency requirement may conflict with the need for algorithms to operate efficiently and without undue interference.

---

[19] Eubanks, V. (2018). Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. St. Martin's Press.
[20] Bontridder N, Poullet Y. The role of artificial intelligence in disinformation. Data & Policy. 2021;3:e32. doi:10.1017/dap.2021.20
[21] Gillespie, T. (2018). Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media. Yale University Press.
[22] Brock, George, The Right to Be Forgotten, Reuters Institute for the Study of Journalism (University of Oxford, 2023) https://reutersinstitute.politics.ox.ac.uk/sites/default/files/research/files/The%2520Right%2520to%2520be%2520Forgotten%2520Extract.pdf, accessed 22 January 2025.
[23] Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). Springer.

For example, the recent enforcement of the GDPR against companies like Google and Facebook has led to fines and restructuring of data collection practices[24]. These changes aim to increase user consent but also impose significant operational challenges for platforms that rely on data-driven algorithms. In some cases, these regulatory frameworks might limit the platforms' ability to effectively curate content, which could inadvertently affect user experience and engagement.

2.4 Ethical Considerations and Potential Solutions

To navigate between freedom of speech, privacy, and algorithmic regulation, a multi-stakeholder approach involving regulators, tech companies, civil society, and users is necessary[25]. One potential solution lies in increasing the algorithmic accountability of platforms. By mandating that social media companies disclose the logic behind their algorithmic decisions in a transparent and understandable manner, users would be better equipped to understand how their data is being used and how content is filtered. This could help mitigate the risks of algorithmic bias and undue censorship while also fostering trust in digital platforms[26].

Furthermore, a contextual approach to content moderation could balance the need for safe online spaces without infringing on free speech. This would involve distinguishing between harmful and merely controversial content and providing clearer guidelines for moderation that account for cultural and political contexts[27].

Case Study: Facebook's Algorithmic Modifications

A key example of the evolving challenges in this space is Facebook's algorithmic changes, which have sparked debates over free speech, misinformation, and data privacy. In the aftermath of the 2016 U.S. election, Facebook adjusted its algorithm to reduce the spread of misleading

[24] European Data Protection Board, Meta Platforms Fined €1.2 Billion for GDPR Violations, (2023) https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en, accessed 22 January 2025.
[25] Floridi, L. (2020). The Ethics of Artificial Intelligence: A European Perspective. Springer.
[26] Gorwa, R., Binns, R., & Katzenbach, C., Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance, Big Data & Society, 7(1) (2020), https://doi.org/10.1177/2053951720943234, accessed 22 January 2025.
[27] Gillespie, T. (2018). Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media. Yale University Press.

information and fake news. However, this led to a significant backlash from users and political groups who felt that the moderation was politically biased and stifled free expression[28]. In response to criticisms, Facebook has promised increased transparency and accountability by publishing transparency reports, yet concerns remain about how algorithmic transparency can be achieved without compromising business interests[29].

In, summary regulatory frameworks introduced by the DSA and GDPR represent critical steps toward establishing a more transparent and accountable digital ecosystem. However, the challenge remains in ensuring that these regulations do not inadvertently undermine free speech or create barriers to innovation. As the digital landscape evolves, a nuanced approach to regulation that prioritizes both individual rights and platform accountability will be necessary. Policymakers must continuously assess and adapt these legal frameworks to keep pace with rapid technological advancements and the complex interplay between algorithms, privacy, and free expression.

3.0. **Understanding the GDPR and DSA in Balancing Rights in Social Media Algorithms and Free Speech**

3.1. Brief Introduction to the Objectives of the DSA and GDPR.

The General Data Protection Regulation (GDPR) and the Digital Services Act (DSA) are cornerstone EU legislative frameworks aimed at regulating the digital landscape. Adopted in May 2018, the GDPR focuses on harmonizing data protection laws across the EU, ensuring the privacy and security of personal data, and granting individuals greater control over their information[30]. Meanwhile, the DSA, effective from November 2022, introduces a comprehensive

[28] Allcott, H., & Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election. Journal of Economic Perspectives, 31(2), 211–236.
[29] Chadwick, A., Vaccari, C., & Kaiser, J., The Amplification of Exaggerated and False News on Social Media: The Roles of Platform Use, Motivations, Affect, and Ideology, American Behavioral Scientist (2022),https://journals.sagepub.com/doi/pdf/10.1177/00027642221118264, accessed 22 January 2025.
[30] Regulation (EU) 2016/679 (General Data Protection Regulation), Recitals 1-7

regulatory regime for online intermediaries and platforms, with the dual objectives of safeguarding fundamental rights and fostering transparency and accountability in the digital sphere[31]. Together, these frameworks address critical issues of data protection, online safety, and user rights in an increasingly algorithm-driven world.

3.2. Understanding the GDPR in Balancing Rights in Social Media Algorithms and Free Speech

The GDPR, as the EU's comprehensive framework for regulating personal data processing, is highly relevant to the functioning of social media platforms that depend on data-driven algorithms. Articles 5, 15, 17, 22, and 35 of the GDPR establish critical principles and rights that directly influence the design and operation of these algorithms. These provisions require platforms to balance their pursuit of algorithmic innovation with the fundamental rights to data protection and free expression[32].

Article 5 GDPR outlines the foundational principles for processing personal data, including lawfulness, fairness, transparency, purpose limitation, data minimization, and accountability. These principles are particularly significant in the context of social media platforms that utilize algorithms for content moderation and targeted advertising[33].

The principle of transparency requires platforms to clearly communicate how user data is processed, a necessity underscored by Case *C-136/17 GC and Others v CNIL (2020)*[34], where the Court of Justice of the European Union (CJEU) emphasized the importance of transparent data practices in online environments.

---

[31] Regulation (EU) 2022/2065 (Digital Services Act), Articles 1-2.

[32] Regulation (EU) 2016/679 (General Data Protection Regulation) Articles 5, 15, 17, 22, and 35. The official text of the GDPR can be found on the EU's website:
European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L119/1. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[33] Taddeo, M., & Floridi, L. (2018). How GDPR Compares to the Protection of Personal Data in Social Media: Ethical and Legal Implications. Philosophy & Technology, 31(4), 369–388. DOI: 10.1007/s13347-018-0335-0

[34] Court of Justice of the European Union (2020). Case C-136/17 GC and Others v CNIL. Available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=217645&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1. Accessed January 1, 2025.

The principles of transparency establish the norms for processing, which are enforced through mechanisms like Data Protection Impact Assessments (Article 35). These principles are integral to the GDPR framework, influencing detailed provisions throughout the regulation. To comply with accountability for transparency in their conduct, social media companies must conduct Data Protection Impact Assessments (DPIAs), as reinforced in the European Data Protection Board's (EDPB) guidelines. For example; Facebook's deployment of emotion-sensing algorithms drew scrutiny over inadequate assessments of privacy risks, further illustrating the critical role of DPIAs[35].

Moreover, Article 5 aligns with broader legislative instruments, such as the European Union Charter of Fundamental Rights, particularly Article 8, which guarantees the protection of personal data. This alignment ensures that data processing activities adhere to fundamental rights and freedoms, reinforcing the ethical and legal standards set forth in the GDPR[36].

Article 15 grants individuals the right to access their personal data, including insights into automated decision-making processes including content personalization, targeted advertising, browsing behavior, and inferred interests. This provision is vital for enhancing transparency in algorithmic operations, especially regarding content recommendation systems. In Schrems II (C-311/18)[37], the case originated from a complaint filed by Austrian privacy advocate Maximillian Schrems against Facebook Ireland. Schrems claimed that Facebook's transfer of his personal data to the United States violated EU data protection laws, citing concerns over U.S. government surveillance practices. The Court of Justice of European Union (CJEU) reiterated the importance of enabling users to understand and control how their data is used, fostering trust in digital services.

Article 15 of the GDPR aligns with provisions in the European Convention on Human Rights (ECHR), particularly Article 8, which guarantees the protection of personal? data, and Article 10, which safeguards freedom of expression. These connections emphasize the requirement for

[35] Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. International Data Privacy Law, 7(2), 76–99.DOI: 10.1093/idpl/ipx005.
[36] GDPR HUB, European Union Charter of Fundamental Rights and GDPR Alignment, (2025) https://gdprhub.eu, accessed 2January 2025.
[37] Court of Justice of the European Union (2020). Schrems II (C-311/18). Available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=227537&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1. Accessed January 1, 2025.

social media platforms to consider the impact of their algorithms on free speech. The case of *C-73/16, Puškár v. Financné riaditel'stvo Slovenskej republiky*[38] highlights the principles of Article 15 of the GDPR and its alignment with the ECHR. Mr. Puškár challenged the inclusion of his name on a Slovak tax authority blacklist, arguing that the lack of transparency in processing his personal data violated his rights. Furthermore, Article 15 is supported by Recitals 63 and 64 of the GDPR, which highlight the importance of access rights in promoting transparency and enabling individuals to verify the fairness of data processing. These provisions also recognize the necessity of identity verification to ensure that access requests are genuine, thereby safeguarding data security.

Article 17 GDPR, often referred to as the "*Right to be forgotten*," grants individuals the right to request the erasure of their personal data without undue delay under certain conditions like the absence of a lawful basis for processing[39]. This right is critical for users seeking to remove their digital footprint from algorithmic profiling, particularly on platforms like TikTok, which have faced scrutiny for retaining user data without proper consent[40].

Balancing this right with freedom of expression is a nuanced challenge, as evidenced in Google Spain v. AEPD and Mario Costeja González (C-131/12)[41], where Mario Costeja requested Google to remove links to a 1998 newspaper article about a debt auction concerning his social security debts, arguing that this outdated information harmed his privacy. This prompted the CJEU to weigh privacy rights against public access to information. In the context of social media algorithms, this balance underscores the dual responsibility of platforms to respect user rights while fostering open discourse.

Moreover, Article 17 (3) of the GDPR aligns with Article 10 ECHR, which guarantees the right to freedom of expression. Social media platforms often invoke this framework to justify retaining

[38] C-73/16, *Puškár v. Financné riaditel'stvo Slovenskej republiky* [2017] ECLI:EU:C:2017:725.
[39] Neethu, R. (2017). What the roll out of EU data legislation means for you. Nature Biotechnology, 35, 712-713. https://doi.org/10.1038/nbt.3928.
[40] Associated Press, TikTok Fined €345 Million for GDPR Privacy Violations, (2023) https://apnews.com/article/tiktok-data-privacy-europe-regulation-fine-8ebacba7646ef872fb8e85a1bcb93876, accessed 5 January 2025.
[41] Court of Justice of the European Union (2014). Google Spain v. AEPD and Mario Costeja González (C-131/12). Available at: https://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1. Accessed January 1, 2025.

user-generated content that aligns with public interest or democratic principles. Similarly, Article 17 complements Recital 65 GDPR which highlights the need to balance the right to erasure with other rights, particularly freedom of expression, ensuring that data deletion does not compromise societal values or legitimate interests.

Article 22 grants individuals the right not to be subject to decisions based solely on automated processing, including profiling, that produce legal effects or significantly affect them. Social media algorithms often rely on profiling to deliver personalized content, raising concerns about user autonomy and oversight[42]. For instance, Twitter faced criticism for its algorithmic content moderation, where automated systems disproportionately flagged certain content, sparking debates about bias and fairness[43]. However, exceptions to Article 22 exist if such processing is necessary for contractual obligations, authorized by law, or based on explicit consent. Article 22 ensures human oversight in automated decisions, mitigating risks of unjust outcomes

Article 35

Figure 1

establishes a legal obligation for data controllers to conduct Data Protection Impact Assessments (DPIAs) when processing activities, particularly those involving new technologies, and those likely to pose high risks to the rights and freedoms of natural persons. A notable case highlighting the importance of DPIAs in the context of social media algorithms is the complaint filed by the Austrian activist group NOYB against X (formerly Twitter) in August 2024. The complaint alleged that X used personal data from its users to train its artificial intelligence (AI) systems without obtaining proper consent[44]. This requirement is critical for assessing the privacy implications of social media algorithms. For example, TikTok's introduction of real-time user engagement metrics prompted regulatory inquiries into whether DPIAs were adequately conducted[45].

[42] Reviglio, U., & Agosti, C. (2020). Thinking Outside the Black-Box: The Case for "Algorithmic Sovereignty" in Social Media. Social Media + Society, 6. https://doi.org/10.1177/2056305120915613.
[43] Gorwa, R., Binns, R., & Katzenbach, C. (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. Big Data & Society, 7. https://doi.org/10.1177/2053951719897945.
[44] Reuters, 'X Hit with Austrian Data Use Complaint over AI Training' (12 August 2024) https://www.reuters.com/technology/x-hit-with-austrian-data-use-complaint-over-ai-training-2024-08-12/ accessed 18 January 2025.
[45] European Commission (2023). Algorithmic Transparency and Compliance in Digital Services. Available at: https://ec.europa.eu/info/law/law-topic/data-protection_en. Accessed January 1, 2025.

The DPIA process involves evaluating risks, such as discriminatory outcomes or the amplification of harmful content, and implementing measures to mitigate them. The role of DPIAs in maintaining transparency and trust is further emphasized in the EDPB's DPIA Guidelines (2018)[46].

These requirements complement the provisions of Article 10of the ECHR which underscores the importance of protecting freedom of expression while addressing risks posed by algorithmic systems. Similarly, the proposed Artificial Intelligence Act introduces additional safeguards for high-risk AI systems, such as those used in content moderation or algorithmic profiling[47]. Together, these frameworks form a robust legal foundation for assessing and mitigating risks in algorithmic decision-making.

Overall, the GDPR provides a robust framework for governing the use of personal data in social media algorithms, ensuring transparency, fairness, and accountability. Articles 5, 15, 17, 22, and 35 collectively address key challenges in balancing algorithmic innovation with data protection and user rights. These safeguards, when aligned with the DSA's requirements, foster a digital ecosystem that upholds individual freedoms while promoting responsible innovation.

3.2. Understanding the DSA in Balancing Rights in Social Media Algorithms and Free Speech

The DSA addresses the critical issue of algorithmic governance in social media platforms through a detailed framework, which includes Articles 12, 26, 27, 34, and 40. These articles focus on ensuring social media algorithms respect free speech, balance user protection, and comply with data privacy laws under the GDPR.

Article 12 obligates providers of intermediary services, such as social media platforms, to establish clear and accessible points of contact for their users. By obligating platforms to provide

[46] European Data Protection Board, Data Protection Impact Assessment (DPIA), (2018) https://www.edpb.europa.eu/our-work-tools/our-documents/topic/data-protection-impact-assessment-dpia_en, accessed 3 January 2025.
[47] Kalodanis, K., Rizomiliotis, P., & Anagnostopoulos, D. (2023). European Artificial Intelligence Act: an AI security approach. Inf. Comput. Secur., 32, 265-281. https://doi.org/10.1108/ics-10-2022-0165.

accessible contact points, Article 12facilitates effective communication between users and service providers. This transparency is essential for users to understand and challenge decisions made by algorithms that may impact their freedom of expression. As seen in the Delfi AS v. Estonia (2015) case, where the ECHR held the Estonian news portal Delfi liable for offensive comments posted by its users. The court emphasized that Delfi had failed to establish effective measures for users to report or contest such comments and had not provided accessible contact points for addressing grievances. By ensuring clear communication channels, this article helps mitigate algorithmic opacity and empowers users to effectively assert their rights[48].

Article 26 makes provision for the subject matter. It establishes rules to enhance transparency and accountability in online advertising practices on platforms. The provision requires online platforms to disclose key details about advertisements shown to users, ensuring that such content can be identified as advertising in a clear, concise, and unambiguous manner. This includes disclosing the source of the advertisement, the entity paying for it (if different from the source), and meaningful information about the targeting criteria used (Article 26(1))[49]. These measures aim to prevent deceptive practices, empower users, and foster trust in online services.

To further enhance clarity in commercial communications, Article 26 obligates platforms to provide functionality allowing users to declare whether their content contains commercial communications. When such declarations are made, platforms must ensure other users can identify the commercial nature of the content in real time, using clear and prominent markings (Article 26(2)). This ensures a standardized approach to transparency and reduces potential confusion among users.

A relevant example is the case of *Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. (Case C-673/17)*, where

[48] Latham & Watkins LLP, The Digital Services Act: Practical Implications for Online Services and Platforms, (2022) https://www.lw.com/admin/upload/SiteAttachments/Digital-Services-Act-Practical-Implications-for-Online-Services-and-Platforms.pdf, accessed 14 January 2025.
[49] Senftleben, M. (2022). Trademark Law, AI-Driven Behavioural Advertising and the Digital Services Act – Towards Source and Parameter Transparency for Consumers, Brand Owners and Competitors. In R. Abbott (Ed.), Research Handbook on Intellectual Property and Artificial Intelligence (pp. 309–324). Edward Elgar Publishing accessed 5 January 2025.

the Court of Justice of the European Union (CJEU) ruled that consent for cookies must be specific, informed, and freely given[50].

By requiring transparency in advertising practices and regulating profiling, Article 26 addresses critical challenges associated with algorithmic targeting, privacy violations, and the manipulation of online users[51]. These obligations ensure platforms uphold fairness and accountability while providing users with the tools and information needed to make informed decisions about the content they encounter online.

Article 27 specifically targets the lack of transparency in recommender systems, which are integral to how content is prioritized on platforms. This provision requires platforms to include in their terms and conditions a plain-language explanation of the main parameters driving their recommender systems, as well as any available options for users to modify or influence those parameters (Article 27(1))[52]. By requiring this level of detail, the DSA seeks to demystify the algorithms that curate and prioritize content, enabling users to understand why certain information is being recommended.

To further enhance user autonomy, platforms must offer a functionality that allows users to select and modify their preferred settings for recommender systems. This functionality must be directly accessible from the section of the platform where the information is prioritized (Article 27(3)). This ensures users can easily exercise control over their digital experience without navigating complex or hidden options[53].

The purpose of these requirements is to enhance transparency and accountability in content curation practices while safeguarding users' rights to freedom of expression and access to information. In practice, this provision obliges platforms to rethink how they communicate

[50] Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. Case C-673/17, EU:C:2019:801.
[51] Inside Privacy, 'Rules on Targeted Advertising: What do the Digital Markets Act and Digital Services Act Say?' (Inside Privacy, 2024) https://www.insideprivacy.com/advertising-marketing/rules-on-targeted-advertising-what-do-the-digital-markets-act-and-digital-services-act-say/ accessed 2 January 2025.
[52] Claire Pershan and Jesse McCrosky, 'No Perfect Solution to Platform Profiling Under Digital Services Act' (Tech Policy Press, 25 August 2023) https://www.techpolicy.press/no-perfect-solution-to-platform-profiling-under-digital-services-act/ accessed 23 January 2025.
[53]

algorithmic decision-making to users. By providing options to adjust recommender settings, platforms also reduce risks of perceived bias or manipulation, fostering trust in their services.

Article 34 applies to platforms designated as Very Large Online Platforms (VLOPs). Under Article 33, online platforms (including social media) with 45 million or more average monthly active users in the EU are VLOPs. This classification subject social media platforms with this capacity to enhanced obligations due to their significant societal impact[54].

Article 34 establishes annual risk assessment obligations for VLOPs. By mandating algorithmic transparency and accountability, Article 34 ensures that social media platforms continuously assess and adapt to risks, preventing harms like unlawful suppression of free speech; provide regulators with oversight mechanisms to evaluate compliance. This provision align with broader human rights frameworks, like the ECHR) particularly Article 10, which safeguards freedom of expression [55]. Also, Article 34foster public trust in digital platforms through documented mitigation efforts.

Article 34's enforcement is pivotal to addressing concerns about opaque algorithmic practices and ensuring a balanced coexistence of free speech and content regulation. Its emphasis on systemic risk assessments positions it as a cornerstone for legal scholarship on algorithmic governance and rights protection in the digital age[56].

Article 40 of the DSA provides for data access and scrutiny. Article 40 (1) establishes that

[54] Husovec, M. (2024). The Digital Service Act's Red Line: What the Commission Can and Cannot Do About Disinformation. SSRN.accessed 23December 2024.
[55] European Commission, 'Digital Services Act: Empowering Users to Control Recommender Systems' (2020) https://ec.europa.eu/digital-services-act-recommender-systems accessed 1December 2024.
[56] Tommasi, S. (2023). Risk-Based Approach in the Digital Services Act and in the Artificial Intelligence Act. The Risk of Discrimination in the Digital Market, 73–83.accessed 1December 2024.

VLOPs must provide the Digital Services Coordinator (DSC) of their country of establishment or the European Commission with access to data necessary to monitor and assess compliance with the DSA, upon a reasoned request within a specified timeframe[57].

Also, that the DSC and the EC may use the accessed data solely to monitor compliance, ensuring the protection of personal data, trade secrets, confidential information, and the security of the platform Article 40 (1). Furthermore, VLOPs must also explain the algorithmic design, logic, functionality, and testing of their algorithmic systems, including recommender systems, when requested by the DSC or the EC.

Besides, Article 40 (4) mandates VLOPs to provide vetted researchers with access to data upon a reasoned request from the Digital Services Coordinator (DSC). This paragraph underscores the regulatory framework allowing independent research on the systemic risks posed by VLOPs, fostering accountability while mitigating potential harms[58].

Other core provisions are provided by Article 40 (5) and (6). Together these paragraphs introduce safeguards for VLOPs, ensuring their legitimate concerns over data security and confidentiality are considered, while maintaining oversight through the DSC's decision-making process. For example, these paragraphs intend that VLOPs can request amendments to data access requests if they lack the data or if granting access would compromise security or confidentiality (like trade secrets)[59]. The DSC thus, can reviews these requests and provides a decision within 15 days, ensuring a balance between researchers' needs and the platforms' operational security. This aligns with the GDPR's emphasis on protecting sensitive information.

Noteworthy is Article 40 (8)which outlines the requirements for researchers to obtain "vetted" status. Researchers must be affiliated with recognized organizations, independent of commercial interests, transparent about funding, and capable of protecting personal data and confidential

[57]Halil, D., Kollnig, K., & Tamò-Larrieux, A. (2024). Regulating pressing systemic risks – but not too soon? Comparative Analysis of the Implementation of Data Access Requests to Platform Data under Article 40(4) of the EU Digital Services Act. SSRN. Accessed 4 December 2024.
[58] Kuczerawy, A. (2024). The Legal Significance of Independent Research based on Article 40 DSA for the Management of Systemic Risks in the Digital Services Act. European Journal of Risk Regulation, 1–13. Accessed 16 December 2024.
[59] Dergacheva, D., Katzenbach, C., Schwemer, S. F., & Quintais, J. P. (2023). Improving Data Access for Researchers in the Digital Services Act. SSRN accessed 5 January 2025.

information. Additionally, they must demonstrate that their research will contribute to understanding systemic risks and that results will be publicly accessible. This paragraph establishes a rigorous vetting process.

Article 40 (8, 10, 12 and 13) together address transparency, accountability, and data-sharing requirements in relation to systemic risks and free speech considerations as they address transparency, accountability, and data-sharing requirements in relation to systemic risks and free speech considerations. Article 40 (10) empowers the Digital Services Coordinator (DSC) to terminate a vetted researcher's data access if they no longer meet the conditions outlined in paragraph 8. Nonetheless, it ensures that researchers accessing platform data remain compliant with the outlined conditions, balancing the need for transparency with the protection of the platform's data integrity and confidentiality.

Recent developments have underscored the real-world impact of the DSA. For instance, in January 2025, the EC launched an investigation into Elon Musk's platform, X (formerly Twitter), over potential violations of EU content moderation rules. The investigation, which sought internal documentation regarding X's recommender system, highlighted the enforcement of DSA's transparency and accountability provisions[60]. Similarly, major platforms such as Meta's Facebook, X, and Google's YouTube have committed to enhancing their efforts to tackle online hate speech as part of an updated code of conduct integrated into the DSA. This cooperation with organizations aims to address hate speech notices promptly and effectively[61].

DSA represents a robust regulatory framework that addresses key concerns surrounding algorithmic governance. Through Articles 12, 26, 27, 34, and 40, it balances the imperative of free speech with the need for greater transparency, accountability, and privacy protections. By complementing the GDPR and aligning with ECHR principles, the DSA provides a foundation for fostering a fairer, more democratic digital ecosystem. This regulatory synergy is critical for

[60] Latham & Watkins LLP, The Digital Services Act: Practical Implications for Online Services and Platforms, (2022) https://www.lw.com/admin/upload/SiteAttachments/Digital-Services-Act-Practical-Implications-for-Online-Services-and-Platforms.pdf, accessed 22 January 2025.
[61] European Commission, 'Digital Services Act: Empowering Users to Control Recommender Systems' (2020) https://ec.europa.eu/digital-services-act-recommender-systems accessed 23 January 2025.

mitigating risks associated with algorithmic decision-making while upholding fundamental rights in the digital age.

4.0 **Balancing Rights: Synergies and Overlaps Between the DSA and GDPR on Social Media Algorithms and Free Speech**

The proliferation of social media platforms has amplified the role of algorithms in shaping public discourse, raising critical challenges in balancing free speech, data protection, and platform accountability. The EU's DSA and GDPR aim to address these concerns through complementary yet distinct approaches. Articles 12, 26, 27, 34, and 40 of the DSA and Articles 5, 15, 17, 22, and 35 of the GDPR provide regulatory frameworks that converge on key principles: transparency, accountability, and safeguarding fundamental rights.

4. 1. Synergies and Overlaps between the DSA and GDPR

4. 1. 1. Algorithmic Accountability and Transparency (DSA Articles 26 and 27, GDPR *Articles 5 and 22)*

The DSA emphasizes algorithmic transparency under Articles 26 and 27, requiring platforms to disclose how content is ranked and recommended. This regulatory obligation dovetails with the GDPR's Articles 5 and 22, which regulate automated decision-making by mandating fairness, accountability, and the right to challenge decisions. These provisions collectively aim to mitigate algorithmic bias while ensuring user autonomy over data and content exposure.

David Kaye, former United Nation (UN) Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, underscores the critical role of transparency in addressing algorithmic opacity. In his 2019 report to the UN, Kaye advocated for regulatory frameworks that prioritize user autonomy while safeguarding against algorithmic discrimination[62]. The DSA and GDPR exemplify such an approach by requiring risk assessments

[62] David Kaye, Summary of Experts' Consultation to A/HRC/41/35 Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (UN Human Rights Council, 2019) A/HRC/41/35/Add.4 https://www.ohchr.org/en/documents/thematic-reports/ahrc4135add4-summary-experts-consultation-ahrc4135-report-special accessed 14 January 2025.

and empowering individuals to contest algorithmic decisions.

For instance, in *Case C-40/17, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV.*[63], the Court of Justice of the EU (CJEU) affirmed that data controllers must ensure compliance with GDPR Article 22 when algorithms significantly affect users' rights. The DSA complements this ruling by imposing explicit obligations on platforms to assess the societal risks of algorithmic amplification under Article 27.

However, as legal scholar Margot E. Kaminski warns, excessive transparency mandates may inadvertently expose proprietary algorithmic models, leading to risks such as intellectual property theft or malicious exploitation. Kaminski suggests a tiered disclosure model to strike a balance between transparency and innovation[64].

4. 1. 2. Free Speech and Content Moderation (DSA Articles 12 and 40, GDPR Articles 15 and 17)

The DSA's Article 12 introduces mechanisms for users to contest content moderation decisions, reinforcing free speech protections. Article 40 further encourages the adoption of codes of conduct to ensure fair and proportionate content moderation practices. Similarly, GDPR Articles 15 and 17 establish the right to access and erase personal data, providing additional safeguards against misinformation and defamatory content.

Irene Khan, current UN Special Rapporteur on the promotion and protection of freedom of opinion and expression, emphasizes that content moderation must be proportionate, transparent, and grounded in international human rights law[65]. These principles resonate with the Digital Services Act (DSA), which incorporates user-centric safeguards aimed at preventing arbitrary censorship and promoting accountability.

[63] Case C-40/17 Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV [2019] ECLI:EU:C:2019:629, Judgment of the Court (Second Chamber), delivered on 29 July 2019.

[64] Kaminski ME, 'Understanding Transparency in Algorithmic Accountability' in Barfield W (ed), The Cambridge Handbook of the Law of Algorithms (Cambridge University Press 2020) pp. 121–138 https://www.cambridge.org/core/books/cambridge-handbook-of-the-law-of-algorithms/understanding-transparency-in-algorithmic-accountability/D355F8D31BF1778431D92D2E79917093 accessed 23 January 2025.

[65] Khan I, 'Statement of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (UN Human Rights Council, 2 July 2021) https://www.ohchr.org/en/press-briefing-notes/2021/07/statement-irene-khan-special-rapporteur-promotion-and-protection accessed 3 January 2025.

The seminal *Google Spain SL v. Agencia Española de Protección de Datos (C-131/12*) case illustrates the balancing act between data protection and free speech. The CJEU ruled that the "right to be forgotten" must be weighed against the public's right to information, a principle echoed in the DSA's safeguards against arbitrary content removal [66]. These frameworks collectively promote proportionality in addressing online harms while preventing undue suppression of legitimate speech.

4. 2. 1. Legal Challenges in Balancing Competing Rights

Judicial interpretations underscore the complexities of balancing free speech with data protection and platform accountability. In *Netlog NV v. SABAM (C-360/10),* the CJEU cautioned against imposing blanket monitoring obligations on platforms, highlighting the risk of overreach into users' freedom of expression[67].

Human rights organizations such as Article 19 advocate for a cautious approach to content moderation, warning that overly restrictive measures can lead to self-censorship and stifling of dissent, undermining free speech. To address these concerns, Executive Director Quinn McKew emphasizes that the DSA's focus on transparency and due process provides a balanced framework. This approach seeks to tackle harmful content effectively while safeguarding individuals' rights to freedom of expression[68].

4. 2. 2. Perspectives from ICT and Innovation Studies

Experts in ICT and innovation argue that the GDPR's stringent data protection standards can pose compliance challenges that stifle algorithmic advancements. Conversely, the DSA's risk-based approach, as noted by van Hoboken et al. (2023), aligns more closely with fostering

[66] Case C-131/12 Google Spain SL v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014] ECLI:EU:C:2014:317, Judgment of the Court (Grand Chamber), delivered on 13 May 2014.
[67] Case C-360/10 Netlog NV v Société belge des auteurs, compositeurs et éditeurs (SABAM) [2012] ECLI:EU:C:2012:85, Judgment of the Court (Third Chamber), delivered on 16 February 2012.
[68] McKew Q, 'Executive Director of ARTICLE 19 Quinn McKew on Elon Musk, Twitter, and the EU's New Digital Services Act' (UNESCO Crossings Institute, 22 May 2022) https://unesco.uoregon.edu/2022/05/22/executive-director-of-article-19-quinn-mckew-on-elon-musk-twitter-and-the-eus-new-digital-services-act/ accessed 11 January 2025.

innovation while maintaining accountability[69]. Thus, striking a balance between regulatory enforcement and innovation-friendly policies remains a critical challenge for legislators.

Section 4. 3. Challenges and Future Directions

Section 4. 3. 1. Balancing Competing Rights in Practice

The practical implementation of these laws reveals inherent tensions. Algorithms designed to remove harmful content may inadvertently suppress legitimate speech, as demonstrated in *Twitter v. Australia's E-Safety Commissioner* (2023)[70].In this case, Twitter challenged a removal notice issued under the Online Safety Act 2021, which required the platform to take down content linked to a stabbing incident involving a religious figure. The platform argued that compliance through algorithmic measures led to the over-removal of lawful content, thus affecting users' freedom of expression. Courts must navigate these conflicts with evolving jurisprudence that considers the rapid pace of technological change and its societal implications.

4. 3. 2. Implementation Challenges and Regulatory Overlap

Evaluating the real-world impacts of the EU's DSA on combating online disinformation, Nannini et al. noted that the concurrent application of the DSA and GDPR may result in overlapping compliance obligations[71]. For example, the DSA's risk assessment requirements under Article 34 and the GDPR's data protection impact assessments under Article 35 could create redundancies, increasing administrative burdens for platforms. This overlap raises questions about how platforms can streamline compliance efforts while meeting the distinct objectives of each regulation, such as algorithmic transparency, privacy protection, and risk mitigation.

Protiviti, a California-based global consulting firm operating in 27 countries, noted in their

---

[69] van Hoboken J, Quintais JP, Appelman N, Fahy R, Buri I, Straub M, 'Putting the Digital Services Act Into Practice: Enforcement, Access to Justice, and Global Implications' (2023) Amsterdam Law School Research Paper No. 13, Institute for Information Law Research Paper No. 03, Verfassungsbooks https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4384266 accessed 13 January 2025.

[70] *eSafety Commissioner v X Corp (formerly Twitter) [2023]* FCA 1024 (Federal Court of Australia, 16 November 2023).

[71] Nannini, L., Bonel, E., Bassi, D. et al. Beyond phase-in: assessing impacts on disinformation of the EU Digital Services Act. AI Ethics (2024). https://doi.org/10.1007/s43681-024-00467-w

assessment of the global impact of Europe's digital regulatory regime, particularly the DSA, that while the DSA has been adopted by the European Parliament and will apply broadly across Europe, there are some aspects that may differ between countries[72].One of the DSA's core objectives is to prevent the spread of illegal content online, but the regulation broadly defines illegal content as "information relating to illegal content, products, services, and activities," leaving the precise nature of illegality to be defined by EU and/or national laws[73]. As a result, companies will need to interpret and adapt to country-specific definitions of illegal content, products, services, and activities. This variability across jurisdictions could further complicate compliance processes, particularly when considered alongside GDPR requirements for managing user data and respecting privacy.

Additionally, reactions from the global tech industry to the DSA agreement have been mixed. While the industry broadly supports the objectives of creating a safer internet, skepticism persists regarding the technical details and implementation challenges[74]. For instance, there is concern about the liability platforms may face for illegal content they are unaware of, which could disincentivize innovative algorithmic solutions. Other concerns include the ambiguity of terms like "harmful content," which may vary culturally and legally, and whether the DSA's transparency measures could inadvertently undermine GDPR protections for user privacy[75]. The combination of these challenges, along with the overlapping compliance demands of the DSA and GDPR, raises doubts about the feasibility of achieving both regulations' goals without significant administrative burdens or legal uncertainty[76].

Together, these complexities underscore the need for harmonization between the DSA and GDPR. As both frameworks intersect on critical issues such as content moderation, algorithmic accountability, and privacy, aligning their requirements is essential to balancing free speech with the protection of users' rights.

---

[72] Protiviti, The Global Consequences of Europe's New Digital Regulatory Regime https://www.protiviti.com/gl-en/whitepaper/global-consequences-europes-new-digital-regulatory-regime accessed 23 January 2025.
[73] Protiviti, The Global Consequences of Europe's New Digital Regulatory Regime https://www.protiviti.com/gl-en/whitepaper/global-consequences-europes-new-digital-regulatory-regime accessed 23 January 2025.
[74]Anu Bradford, 'The False Choice Between Digital Regulation and Innovation' (2024) 19 Northwestern University Law Review 377 https://scholarship.law.columbia.edu/faculty_scholarship/4548 accessed 23 January 2025.
[75]Giancarlo Frosio and Christophe Geiger, 'Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime' (2023) European Law Journal https://doi.org/10.1111/eulj.12475 accessed 15 January 2025.
[76] Turillazzi A, Taddeo M, Floridi L, Casolari F, 'The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications' (2023) Law, Innovation and Technology https://doi.org/10.1080/17579961.2023.2184136 accessed 13 January 2025.

Nigeria has over 35 million active social media users, and platforms are crucial for news, politics, activism, and commerce. Issues around algorithmic bias, shadow-banning, and de-platforming (removing or limiting users' reach) directly affect freedom of expression and democratic participation. Therefore, global debates on free speech and algorithmic control — as shaped by the DSA and GDPR — have direct parallels in Nigeria. Nigeria's Data Protection Act (NDPA, 2023) is inspired by the GDPR, adopting similar privacy principles (consent, purpose limitation, data subject rights). However, Nigeria lacks an equivalent to the DSA, meaning algorithm transparency, content moderation standards, and platform accountability are largely unregulated. Studying the DSA-GDPR framework helps policymakers understand how to design balanced laws that protect both free speech and digital rights.

Nigeria has experienced governmental attempts to restrict online speech, such as:The Twitter ban (2021) after the #EndSARS protest Ongoing debates about social media regulation bills. Lessons from the DSA's transparency rules and appeal mechanisms could inform rights-respecting regulation in Nigeria, ensuring accountability without censorship. The DSA compels platforms to disclose how algorithms amplify or restrict content — something Nigerian users currently have no visibility into. As misinformation, hate speech, and political manipulation spread online, Nigerian regulators can draw insights from the EU approach to demand greater algorithmic accountability.

Recommendation

The interplay between the Digital Services Act (DSA) and the General Data Protection Regulation (GDPR) highlights their shared potential to safeguard individual rights and ensure accountability in the digital landscape. However, challenges such as overlapping mandates, enforcement inconsistencies, and the transnational nature of social media platforms call for refined regulatory strategies. Drawing on real-world cases and established legal frameworks, the following recommendations provide actionable steps to strengthen EU efforts in regulating social media algorithms and protecting free speech.

The EU must harmonize regulatory frameworks to reduce overlaps between the Digital Services Act (DSA) and the General Data Protection Regulation (GDPR). Establishing unified compliance protocols that integrate key elements of both frameworks is essential. For example, combining the systemic risk assessments required under DSA Article 34 with the Data Protection Impact Assessments mandated by GDPR Article 35 would eliminate redundancies while enhancing both user protection and platform accountability. The European Data Protection Supervisor (EDPS) has underscored the importance of such integration in addressing algorithmic

risks[77]. Additionally, coordinated enforcement mechanisms are necessary to clarify the responsibilities of Digital Services Coordinators under the DSA and Supervisory Authorities under the GDPR. Formal collaboration between these entities, as suggested in the EDPB-EDPS Joint Opinion 03/2021, would promote coherence and prevent fragmented enforcement. A centralized Digital Rights Coordination Agency could further align interpretations of overlapping provisions, particularly concerning algorithmic transparency and data protection, as demonstrated by the successful creation of Europol's Innovation Hub. Strengthening legal clarity through updated interpretative guidelines is equally vital. Drawing from the Council of Europe's Recommendation CM/Rec(2018)2, these guidelines would address ambiguities and provide platforms with consistent and transparent regulatory direction[78].

Enhancing algorithmic transparency and accountability is another critical area of reform. A tiered approach to transparency, inspired by Recital 62 of the DSA, could strike a balance between public accountability and proprietary protection. Platforms should provide user-facing summaries of algorithmic operations, such as Facebook's "Why am I seeing this?" feature, while also submitting detailed algorithmic documentation to regulators under strict confidentiality agreements, in line with the EDPB Guidelines on Automated Decision-Making (2018)[79]. Independent algorithmic audits should also be mandated to increase accountability. DSA Article 26 and GDPR Article 22 already envision such audits, as evidenced by the Irish Data Protection Commission's 2022 audit of TikTok, which uncovered algorithmic biases and spurred policy changes[80]. Moreover, platforms should be required to publish annual transparency reports, as exemplified by Twitter's Transparency Center Initiative, in accordance with DSA Articles 13 and 23.

Balancing content moderation with free speech requires a nuanced and contextual approach. Drawing from the principles of proportionality outlined in ECHR Articles 8 and 10, regulators

[77]European Data Protection Supervisor, EDPS Opinions on the Digital Services Act and the Digital Markets Act (2021). Available at: https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opinions-digital-services-act-and-digital_en Accessed: 10 January 2025.
[78]Council of Europe, Recommendation CM/Rec(2018)2 on the Roles and Responsibilities of Internet Intermediaries (2018). Available at: https://rm.coe.int/0900001680790e14 Accessed: 12 January 2025.
[79]European Data Protection Board, Guidelines on Automated Individual Decision-Making and Profiling under Regulation 2016/679 (2018). Available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/automated-decision-making-and-profiling_en Accessed: 15 January 2025
[80]Irish Data Protection Commission, TikTok Audit Report (2023). Available at: https://www.dataprotection.ie/en/dpc-guidance/law/decisions-made-under-data-protection-act-2018/Inquiry-into-TikTok-Technology-Limited-September-2023 Accessed: 17 January 2025.

should encourage context-sensitive moderation standards to avoid excessive takedowns, as highlighted in the *Delfi AS v. Estonia* (2015) case[81]. Platforms should also implement transparent dispute mechanisms to empower users under DSA Article 17. Independent ombudsman services, similar to the UK's Independent Complaints Reviewer, could mediate disputes, while standardized appeals process across platforms would enhance fairness. Education and awareness campaigns funded by the EU could further promote digital literacy and inform users about the impact of algorithms on free speech and data privacy. Programs like the UK's Be Internet Citizens initiative provide a successful model for these efforts.

Addressing enforcement challenges in a global context necessitates enhanced international cooperation. The EU should advocate for global treaties on digital governance, similar to the OECD's Guidelines on AI Principles (2019), to align transparency standards and enforcement protocols across borders[82]. Public-private partnerships could also play a vital role in fostering innovation while ensuring ethical AI development. Initiatives like the AI Ethics Lab at Google DeepMind exemplify how such collaborations can promote responsible AI research. The EU should adopt flexible enforcement models tailored to platform size and nature. Smaller platforms could receive technical assistance, while larger entities face stricter penalties for non-compliance, as recommended in the European Commission's 2020 Digital Strategy[83].

Empowering users requires simplified privacy tools, strengthened individual rights, and enhanced accessibility. Platforms should adopt GDPR-compliant tools, such as Mozilla's Facebook Container, to improve user control over algorithmic curation. Centralized portals that allow users to manage GDPR rights across platforms, as proposed in the EDPB's 2023 Guidelines on Data Portability, would streamline the enforcement of rights[84].Furthermore, regulatory communications, including terms of service, must comply with the EU Accessibility

[81]Delfi AS v. Estonia, App No. 64569/09, European Court of Human Rights (ECtHR), 2015. Available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-155105%22]} Accessed: 20 January 2025.

[82]Organisation for Economic Co-operation and Development (OECD), AI Principles (2019). Available at: https://www.oecd.org/en/topics/sub-issues/ai-principles.html Accessed: 8 January 2025.

[83]European Commission, A European Strategy for Data (2020). Available at: https://digital-strategy.ec.europa.eu/en/policies/strategy-data Accessed: 18 January 2025.

[84]European Data Protection Board, Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01 (2023). Available at: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-right-data-portability-under-regulation-2016679_en Accessed: 11 January 2025.

Directive (2019) to ensure inclusivity for users with disabilities[85]. By implementing these measures, the EU can create a regulatory ecosystem that safeguards user rights, promotes transparency, and fosters innovation.

The DSA and GDPR collectively form a robust regulatory foundation for governing algorithms and protecting free speech. However, their effectiveness depends on harmonized implementation, interdisciplinary collaboration, and adaptability to global challenges. By prioritizing user empowerment and transparency, the EU can solidify its leadership in digital governance while fostering a fair and accountable online ecosystem.

[85]European Union, European Accessibility Act, Directive 2019/882 (2019). Available at: https://eur-lex.europa.eu/eli/dir/2019/882/oj/eng Accessed: 14 January 2025.

Conclusion

The interplay between the DSA and GDPR aims to protect individual rights and ensure accountability in the digital sphere. However, overlapping mandates, inconsistent enforcement, and the global reach of social media platforms present challenges.

Harmonized compliance protocols, integrated risk assessments, and centralized coordination can improve enforcement efficiency. Transparency through disclosures and algorithmic audits can balance innovation and accountability. To safeguard free speech, regulators should adopt proportional content moderation, transparent dispute resolution, and user education on algorithms.

Strengthened international cooperation and GDPR-compliant privacy tools will empower users and support ethical AI development. These measures position the EU as a global leader in balancing privacy, free speech, and innovation in digital governance.