Prof. Dr. Michael Denga,
LL.M. (London), Maîtr. en Droit (Paris)
Tel.: +49 (0)30 766 83 75-100
Fax: +49 (0)30 766 83 75-119
Email: michael.denga@businessschool-berlin.de

Business & Law School
Hochschule für Management und Recht

Campus Berlin
Siemens Villa
Calandrellistraße 1-9
12247 Berlin

Campus Hamburg
HafenCity
Am Kaiserkai 1
20457 Hamburg

Enforcement and optimization of social media platforms' responsibility

-

Expert opinion commissioned by HateAid gGmbH[*]

Prof. Dr. Michael Denga, LL.M. (London), Maîtr. en Droit (Paris)

September 9, 2025

[*] *In case of any contradictions between the German and English version of this expert opinion, the German version shall prevail.*

Contents:

A. Key findings

The DSA must be read and applied in the context **of the European Union's digital sovereignty**; accordingly, the DSA's provisions must be practical and effective in both substantive and procedural terms.

The provisions of the DSA are enforceable **against intermediary services** through regulatory oversight and private enforcement of tort claims. Art. 54 DSA grants users the right to seek damages. Considering geopolitical tensions and political contingency resulting from regulatory enforcement of the DSA, private enforcement is particularly important for the implementation of the DSA's objectives.

Although the DSA obligations do not directly affect the responsible personnel of intermediary services, they do specify an individual standard of care and, in the event of a breach, can trigger **direct tortious liability** under Section 823(1) of the German Civil Code (BGB).

Access to research data under Art. 40 DSA is undermined by superficial compliance and "information overkill". The EU Delegated Regulation of July 2025 only partially addresses these problems, making it necessary to tighten the obligations.

Social media should also be covered by newer AI regulation. Art. 7 of the AI Regulation allows the EU Commission to classify **social media algorithms as high-risk AI systems** through delegated acts, which would activate comprehensive transparency and data governance obligations.

The DSA should be developed further with a focus on ***safety by design***. Recommendations include a complete ban on social bots, video ID user verification, a right to configurable content filters, age restrictions for social media (16 years), and reversing the burden of proof in cases of platform damage.

B. The current risk situation for users[1] of online platforms

Since the introduction of online platforms, users, particularly of social media, have been exposed to “bad” content, including threats, sexual harassment, and identity theft. This content is generally illegal under German law, but it also violates the internal guidelines of platforms and has a negative impact on both individual users and on public debate. The constitutional conflict between negative and positive freedom of information and communication, also in the context of platforms’ entrepreneurial freedom, is complex and highly dependent on individual cases[2]. Currently, “bad” content refers solely to content that is illegal, i.e. content where the interests of recipients of information or of those affected by the information outweigh the interests of the senders of the information and the platform.

The problem is increasingly severe, with three key aspects worth highlighting:

1. Offensive user behaviour, which most often comes from pseudonymous accounts, remains a critical issue. These accounts spread infringing content in their own posts, as well as in comment sections and private messages. Such infringing content includes insults, threats, incitement to hatred, defamation, doxxing, and the non-consensual sending of pornographic content.

2. With the spread **of generative AI**, it is now easy for anyone to create false content. On social media platforms, generative AI is often used to spread fake images of people. Particularly concerning are fake, authentic-looking profiles on social media platforms and the creation and dissemination of false, offensive, or sexually explicit content about the persons concerned or third parties. The use of AI for the autonomous operation of fake accounts or the creation of chat groups on social media platforms that participate independently in platform discussion within a framework program and frequently spread false facts or insults (“fake news”, or simply: propaganda) is highly problematic[3].

3. There are still considerable problems on the platform side. Platforms enjoy extensive liability privileges and are generally not responsible for user-generated content (for more details on the DSA regime and the Copernican revolution, see below, E.). This is true even though platforms influence the dissemination of content in many ways through their algorithms, the exact functioning of which is known only to them. Emotional content that elicits intense interaction is rewarded with particularly wide reach and visibility; eliciting intense interaction is how platform users’ dwell time is increased, and platforms’ business models rely on monetising dwell time. The reach of emotional content is exploited by actors who deliberately seek to create the impression of representing a majority opinion through targeted and orchestrated interaction and the use of multiple profiles. Platforms do not distinguish between content that is hateful, or even criminal, and content that elicits constructive interaction. In addition, online platforms often moderate content based on their Community Standards and Terms of Service automatically by using AI and word filters. Platforms also use the curation power they gain in this way to delete content that does not align with the platform’s political views. In addition, complaint mechanisms are not yet sufficiently effective, often acting too late and thus failing to prevent the spread of “bad” content.

Social media platforms create essential spaces for debate and social participation. At the same time, these spaces are controlled in a highly opaque manner by the rules of private companies. These companies have little economic incentive to counteract the spread of harmful content; on the contrary, due to their attention-driven functioning, platforms may even promote its mass dissemination. Users who disseminate harmful and even illegal content have little to fear in terms of consequences, partly because of the extensive anonymity that the platforms afford them by allowing the use of fake profiles

[1] For the sole purpose of improving readability, this report does not use gender-specific spelling. All personal references are to be understood as gender neutral.
[2] See *Eifert* NJW 2017, 1450 (1451f.); *Klonick* Harvard L. Rev. 131 (2018), 1598 (1626ff.); *Denga* EuR 2021, 569 (572).
[3] *Drolsbach/Pröllochs*, Characterizing AI-Generated Misinformation on Social Media, 2025, p. 1.

or multiple profiles. This creates a climate in which internet users do not dare to freely express their opinions and participate in debates for fear of digital attacks[4].

This brief description is a non-exhaustive overview of the problem, but it makes clear that in the interest of protecting individual rights, as well as plurality of opinion and the functioning of publicly-accessible digital discourse spaces, regulatory enforcement mechanisms need to be activated and, if possible, corrections made.

C. Focus of the investigation

Against this background, the DSA, as the regulatory framework for digital platforms, must be critically examined to identify opportunities for design and reform, both in terms of the material obligations of platforms and the enforcement of these obligations. To start, online platforms are not neutral in the exchange of information, but they are central actors in the dissemination of information because of their curatorial power[5]. The European legislature made this clear in the DSA regarding "systemically important platforms" (according to Art. 33 ff. DSA), which initiated a Copernican shift away from "intermediary privilege" (see E. I.)[6].

The focus here is on two aspects:

1. The DSA does not yet appear to have improved the *prevention* of harmful content. Accordingly, platforms' **preventive systems or measures** and the enforcement and further development of such measures in the sense of *safety by design*[7] will be discussed here (see E., F., and H.).
2. The **transparency requirements** introduced by the DSA are not yet effective; and even if they were, the material content of platform notifications is often not meaningful. In addition, access to research data under Art. 40 DSA is still regularly thwarted. Options for improving the information obtained from online platforms will be discussed here (see G.).

[4] See, for example, the representative study by Das NETTZ, Society for Media Education and Communication Culture, HateAid, and Neue deutsche Medienmacher*innen as part of the Competence Network Against Hate on the Internet (eds.), Lauter Hass – leiser Rückzug. Wie Hass im Netz den demokratischen Diskurs bedroht. Results of a representative survey, 2024, available at: *https://kompetenznetzwerk-hass-imnetz.de/download_lauter-hass.php*

[5] See *Klonick* Harvard L. Rev. 131 (2018), 1598 (1610); on the paradigm of internet regulation via intermediaries, see *Goldsmith/Wu*, Who controls the internet?, 2006, p. 65 ff.

[6] Art. 17 of the DSM Directive should also be read from this perspective; see *Denga*, Attribution, 2022, p. 330.

[7] The term is familiar in regulatory discourse in Australia and the United Kingdom; see the statement by *the* Australian *eSafety Commissioner* of September 2024, available at: https://www.esafety.gov.au/industry/safety-by-design; see also *Woods* on the Online Safety Act, 2024, available at: https://www.onlinesafetyact.net/analysis/safety-by-design/.

D. Interpretation context – Europe's digital sovereignty

The DSA is not being applied in a vacuum; it is applied in the context of European Parliament and Council decisions on the design of the digital single market. European legislators are particularly focusing on the application of European values. Under the banner of digital sovereignty, the interests of EU citizens in the digital space are validated.

For example, the European Commission states:

> *"This Digital Single Market Strategy…has a multi-annual scope and is focused on key independent actions that can only be taken at EU level*[8]*."*
>
> *"This is why we need to build a genuine European single market for data - a European data space based on European rules and values* [9]*."*
>
> *"The European Digital Agenda for 2020-2030 responds to these changes by seeking to create secure digital spaces [...] and strengthen Europe's digital sovereignty, in line with both the digital and green transitions*[10]*."*
>
> *"However, competition policy alone cannot address all the systemic problems that may arise in the platform economy. Based on the single market logic, additional rules may be needed to ensure contestability, fairness and innovation and the possibility of market entry, as well as public interests that go beyond competition or economic considerations*[11]*.*

Digital sovereignty is a new principle in the law of the digital single market that needs further clarification. However, it is already clear that digital sovereignty is not just mere rhetoric. EU decisions are immediately effective[12]. Given its central importance to the EU, digital sovereignty can inform the vague legal concepts provided in EU digital regulation and orient them teleologically toward user protection[13]. Sovereignty is understood here as a claim to sovereignty[14], meaning that European legal interests apply and are protected in digital space just as they are in physical space. Therefore, the integrity of sovereignty interests must be ensured in situations of digital threats, with substantive protection at the material and procedural level. This will be explained below regarding the DSA.

[8] European Commission, Strategy for a Digital Single Market for Europe, May 6, 2015, p. 3, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192.
[9] European Commission, Shaping Europe's digital future, February 19, 2020, p. 5, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0067.
[10] European Commission, Fact Sheet on the European Union: Digital agenda for Europe, April 2025, available at: https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe?utm.
[11] European Commission, Shaping Europe's digital future, February 19, 2020, p. 9, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0067.
[12] See Art. 288(3); see also *Grabitz/Hilf/Nettesheim/Nettesheim* EUV/AEUV, 85th edition 2025, TFEU Art. 288 margin note 38.
[13] For a clear statement on the EU's self-assertion through digital regulation, see *Bradford*, Digital Empires, 2023, p. 105 ff., 324 ff.; on the simultaneously applicable requirement of state independence in media regulation, see *Wischmeyer* JZ 2024, 774 (779 ff.); on the teleological trinity of digital single market law, see *Denga* ZfPW 2024, 427 (445 ff.).
[14] See *Grabitz/Hilf/Nettesheim/Nettesheim* EUV/AEUV, 85th edition, 2025, TFEU Art. 288 marginal no. 14; on the application of democratic principles in the digital space, see also *Susskind*, The Digital Republic, 2022, esp. p. 135 ff.

E. Obligations of social media platforms

Art. 1(2) of the DSA details the regulatory program, which is broken down into three chapters: the limitation of intermediary services' liability in continuation of the intermediary privilege of the E-Commerce Directive[15] (Chapter II); special, graduated due diligence obligations (Chapter III)[16], and the implementation and enforcement of the regulation (Chapter IV). Social media platforms are intermediary services within the meaning of Art. 3(g) and are thus subject to the regime, specifically as online platforms within the meaning of Art. 3(i).

I. Notice and take-down in the context of the DSA's reporting and remedy procedures

The regulation of intermediary services is based on the E-Commerce Directive (ECD) from 2000[17], which was modified and became Chapter II of the DSA. The "intermediary privilege" in Chapter II states that, in principle, there is no liability for transmitting, caching, or hosting "illegal"[18] content, as long as the provider has no knowledge of such activity. However, providers must comply with official instructions regarding illegal content, orders to provide information about specific users, and in the case of caching and hosting, must remove illegal content as soon as they become aware of it. A general monitoring obligation on providers for their services is excluded to ensure the freedom of private communication in the digital space[19]. However, according to Art. 7 DSA, intermediary services may "in good faith and in a diligent manner, carry out voluntary own-initiative investigations into, or take other measures aimed at detecting, identifying and removing, or disabling access to, illegal content," without losing their intermediary privilege[20].

The ECD's simple regime intended to promote the development of the Internet economy in Europe at the beginning of the new millennium[21], and was thus transferred to the DSA. The key difference is the regulatory nature of the DSA, which now makes national implementation provisions superfluous. Furthermore, the ECD did not provide for official requests for information about users, which are included in Art. 10 DSA, nor did it explicitly legitimise voluntary investigations on a service's own Art. 7 initiative.

Art.14 DSA requires all intermediary service providers to disclose content restrictions, moderation mechanisms, and internal complaint procedures in their terms and conditions in **a clear, user-friendly, and machine-readable form—**in other words, community standards must be predictable and easy to

---

[15] Directive 2000/31/EC. However, on the recognised limitations of the intermediary privilege, see *Spindler*, Zivilrechtliche Sperrverfügungen gegen Access Provider nach dem EuGH-Urteil "UPC Telekabel" (Civil law blocking orders against access providers following the ECJ ruling "UPC Telekabel"), GRUR 2014, p. ? f.; on German interference doctrine, see *Volkmann*, Spindler/Schuster, Recht der elektronischen Medien (Law of Electronic Media), 4th ed. 2019, § 1004 BGB, margin no. 34 ff., 826 f.; on German interference doctrine, see *Spindler/Schuster/Volkmann*, Recht der elektronischen Medien (Law of Electronic Media), 4th ed. 2019, § 1004 BGB, margin no. 34 ff.

[16] This means that the function-centred duty model recommended by *Specht-Riemenschneider/Hoffmann* is being implemented, at least in principle, even though they also advocated for abandoning intermediary privilege and introducing a general clause, Verantwortung von Online-Plattformen (Responsibility of Online Platforms), 2021, e.g. p. 101; cf. *Steinrötter/Denga*, European Platform Regulation, 2023, § 6; *Kaesling*, Hofman/Raue, Digital Services Act, 2023, Preamble Art. 33 ff.

[17] Directive 2000/31/EC of 8.6.2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ 2000 L 178/1.

[18] According to Art. 3(h), this refers to "any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law."

[19] However, for recognized restrictions on the intermediary privilege, see *Spindler*, Zivilrechtliche Sperrverfügungen gegen Access Provider nach dem EuGH-Urteil "UPC Telekabel" (Civil law blocking orders against access providers following the ECJ ruling "UPC Telekabel"), GRUR 2014, 826 f.; on German interference doctrine, *see Spindler/Schuster/Volkmann,* Recht der elektronischen Medien (Law of Electronic Media), 4th ed. 2019, § 1004 BGB, para. 34 et seq.

[20] See also Recital 26; critically *Ruffert/Denga,* Die Regulierung Digitaler Plattformen (The Regulation of Digital Platforms), 2023, p. 14 et seq.

[21] *Hofmann* GRUR 2018, 21, 27 f.

understand. Users must be actively notified of changes to the terms of use. If a service is primarily used by minors, age-appropriate wording is mandatory. In addition, measures to enforce these regulations must be careful, objective, and proportionate, and be in line with fundamental rights, particularly freedom of expression and media plurality. Very large services—very large online platforms ("VLOPs") and very large search engines—are additionally required to provide a concise summary in all relevant EU languages.

Under the DSA, hosting providers, including online platforms, must also set up a reporting and complaint procedure for illegal content (Arts. 16–18). Restrictions on use because of illegal content or violations of community standards must be justified (Art. 17). Per Art. 16(2), the reporting system must be "easy to access and user-friendly". Under Art. 16(5), platforms must process reports upon receipt "without undue delay" and make reasoned decisions. Art. 16(6) details that those decisions must be issued "in a timely, diligent, non-arbitrary and objective manner", and allows for use of "automated means" if such use is disclosed. In accordance with Art. 17, if the platform decides to restrict content, it must inform the user of those restrictions. Finally, per Art. 20, online platforms must make an internal complaint system available for remedial measures.

Some scholarship has criticized Art. 16 as being too weak for users affected by illegal content[22]. While it is true that Art. 16 itself does not impose a direct obligation to block content, it is linked to the Art. 6 intermediary privilege for hosting providers. As clarified in Art. 16(3), reports under Art. 16 result in knowledge under Art. 6, which triggers liability for hosted illegal content if it is not blocked or removed immediately. Although the DSA does not order the deletion of illegal content upon knowledge of its existence, it provides a clear incentive to do so through liability law (and criminal law)[23].

II. Obligations of systemically important platforms

Chapter III, which affects virtually all social media platforms, is central to risk prevention in digital spaces[24].

Chapter III, Section 5 sets out stricter obligations for providers of VLOPs and very large online search engines. Due to the specific reference to systemic risks, the term "systemically important platforms" should be used here[25]; these platforms have at least 45 million active users in the European Union (Art. 33 (1)) and reach more than 10% of consumers within the Union[26]. Tightening due diligence obligations for systemically important platforms fits into the tiered structure of the DSA's due diligence obligations and is ultimately an expression of the principle of proportionality. This is because the nature and number of obligations are "directly linked to the reach of a service and its economic and social significance"[27].

Under Art. 34, providers of systemically important platforms are required to carry out regular risk assessments. These assessments should focus on "systemic risks" that may arise from the design or operation of the services, such as dissemination of illegal content, impact on elections, or impact on users' mental health. As a result, per Art. 35, providers must mitigate identified risks through appropriate and effective measures. Art. 36 requires that, in the event of a social "crisis", providers take special measures that go beyond the increased obligations of the section. Art. 37 provides that these platforms must undergo an annual independent audit.

---

[22] *Holznagel* merely refers to "notice and take action," CRi 2024, 172, 178.
[23] On behaviour control through liability, see *Becker* Journal of Political Economy 1968, 76 (2); *Calabresi/Melamed,* Harvard Law Review 85 (1972), 1089; *Kötz* FS Steindorff, 1990, 643; *Arlen/Kraakmann,* NYU Law Review, Vol. 72, No. 1 (1997), 687; *Schäfer/Ott,* Lehrbuch der ökonomischen Analyse des Zivilrechts, 6th ed. 2020, p. 159 ff.; Wagner AcP 206 (2006), 352.
[24] In this respect, there is also a high degree of congruence with the concept of gatekeepers under the DMA, cf. *European Commission,* press release of September 6, 2023, IP/23/4328.
[25] See *Heinze/Steinrötter/Denga/Denga,* EU Platform Law, 2025, § 6.
[26] This is based largely on the "average monthly number of active users in the Union", which in future is to be calculated as an average over a period of six months, cf. Recital 6; see also *Müller* MMR 2022, 1007 (1008).
[27] Recitals 75, 79; *Müller* MMR 2022, 1007 (1009); see also *Janal* ZEuP 2021, 227 (232); with an analogy to "critical infrastructure" *Berberich/Seip* GRUR-Prax 2021, 4 (7).

Arts. 38 and 39 focus on recommendation systems and online advertising, requiring that platforms provide an option without profiling and maintain the content and criteria of advertisements. Providers of VLOPs and very large search engines must, upon request, grant both the Digital Services Coordinator and the Commission access to their internal data; Art. 40 also allows qualified researchers to obtain access to data in this way.

Art. 41 requires that VLOPs and very large search engines set up an adequately resourced compliance department to ensure independent internal monitoring of their compliance with the regulation. In addition, Art. 42 subjects providers to stricter transparency reporting requirements.

III. Impact of the AI Act

Application of the AI Act[28] to social media platforms reveals a structural incongruity between the significant societal risks of algorithmic content moderation and the regulatory mechanisms of the AI Act that are in effect[29].

Social media platforms fall within the definition of "provider[s]" under Art. 3 No. 2 AI Act, as they develop, provide, or use AI systems for automated content moderation, recommendation algorithms, and user interaction analysis[30]. Nevertheless, to the extent that these systems are considered "general AI systems" within the meaning of Art. 3 No. 63 AI Act, they are only subject to the relatively weak obligations of Art. 53 et seq. AI Act. Essentially, as providers of general AI systems, social media platforms are limited to documentation obligations and the provision of application information pursuant to Art. 53(1)(a), (b) AI Act, without establishing substantial transparency or risk assessment obligations (except for the IP compliance strategy under Art. 53(c) AI Act). Providers of particularly powerful AI models[31] are subject to the obligations of Art. 55 for "general-purpose AI models with systemic risk", which specifically include assessment and mitigation obligations for systemic risks comparable to the risk monitoring and mitigation concept of Art. 34 et seq. DSA (Art. 55(1)(b)). In addition, model evaluation, communication with supervisory authorities, and an appropriate level of cybersecurity are required[32].

Social media platforms' algorithmic systems *materially* meet the criteria for high-risk AI systems under Art. 6(2) AI Act, as they pose significant risks to public safety and fundamental rights. Recommendation algorithms on online platforms influence the formation of political opinions, radicalisation processes, and social discourse to an extent comparable to the areas of application listed in Annex III. Nevertheless, social media platforms' algorithmic systems do not *formally* fall under the categories listed there, which means that the far-reaching transparency and governance obligations of Art. 8 ff. AI Act do not apply; providers of social media platforms are not required to implement substantive data governance comparable to the regime of Art. 10 AI Act[33].

However, Art. 7 AI Act gives the European Commission the option of extending Annex III by means of delegated acts if AI systems "pose a risk of harm…[that] is equivalent to, or greater than, the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III." This provision should be used strategically to classify social media algorithms as high-risk systems, thus activating the data governance obligations of Art. 10 AI Act. Art. 10 AI Act would require platforms to

---

[28] EU Regulation (EU) 2024/1689.

[29] On the interaction between the DSA and the AI Regulation, see *Heinze/Steinrötter/Denga/Bastians,* EU Platform Law, 2024, § 21.

[30] For the broad definition of provider, see Art. 3 No. 3 AI Regulation.

[31] For the definition, see Art. 51 AI Regulation.

[32] The obligations for providers of general AI systems are specified in the AI Code of Conduct and in guidelines issued by *the European Commission*, available at https://digital-strategy.ec.europa.eu/de/policies/contents-code-gpai.

[33] For comprehensive information, see BeckOK *AI Law/Kilian/Schefzig*, 2nd ed. 1.5.2025, AI Regulation Art. 10 margin nos. 1-98.

comprehensively document their training data, data quality checks, and bias monitoring[34]—transparency obligations that are essential for democratic control of algorithmic opinion formation.

F. Enforcement of platform obligations

Platforms' practices (as described in B.) show a considerable discrepancy from the ideal state of compliance with the program of obligations. The question of how to enforce platform obligations is therefore critical. This section focuses on the liability of the platform itself (I.) and of its personnel (II.).

I. Liability of the platform provider

The primary addressees of the DSA are providers of intermediary services; the term "provider" refers to economic entities, so liability cannot be shielded, not even through consolidation[35]. Under European law, unlike in German liability law, companies are strictly liable for the conduct of their staff, with a few exceptions for purely private activities[36]. Distinction must be made between the supervisory responsibility (1.) and private enforcement (2.) of the platform provider's liability.

1. Supervisory powers of the DSA

The DSA's powers can be, first of all, classified as supervisory, as its obligations are enforced by public authorities, within the European administrative network[37].

In Germany, the Federal Network Agency acts as the Art. 51 DSA central coordinator for digital services, supplemented by the special responsibilities of the Federal Centre for Child and Youth Media Protection (BzKJ) and the Federal Commissioner for Data Protection and Freedom of Information[38]. However, pursuant to Arts. 56(2) and 56(4) DSA, the EU Commission has exclusive responsibility for enforcing Chapter III, Section 5 against systemically important platforms (see above, E. II.), while the Member States are responsible for the remaining obligations of systemically important platforms, unless the Commission initiates proceedings.

The enforcement powers of the Member State coordinators for digital services under Art. 51 DSA are far-reaching and include entering business premises during normal business hours, seizing evidence, and informing the public about ongoing proceedings and decisions on fines. These powers enable authorities to take effective action against infringements and to create transparency. Art. 51(3)(1)(b) DSA even provides for the possibility of temporarily restricting services in the event of persistent infringements of the DSA[39].

The DSA's sanction system also provides for substantial fines. In principle, all sanctions under Art. 52(2) DSA must be "effective, proportionate, and dissuasive" in order to ensure effective enforcement of the DSA[40]. According to Art. 52(3) DSA, fines of up to 6% of the global annual turnover in the

---

[34] See *Wachter/Mittelstadt/Russell*, Bias Preservation in Machine Learning: The Legality of Fairness Metrics Under EU Non-Discrimination Law, 2021, p. 25; *Legner* RDi 2024, 426.
[35] On the applicability of the antitrust concept of economic unity as a fundamental principle of internal market regulation, see *Denga*, Zurechnung, 2022, p. 203 et seq., 328 et seq.; specifically in the context of digital market *regulation, see Bauermeister/Schwamberger/König,* Private Enforcement im Digitalen Binnenmarkt, 2025, p. 128 ff.
[36] See *Denga,* Attribution, 2022, p. 329 ff.; specifically in the context of *digital market regulation, see Bauermeister/Schwamberger/König,* Private Enforcement in the Digital Single Market, 2025, p. 128 ff.
[37] On the concept of supervisory law in the context of banking, see *Kümpel/Mülbert/Früh/Seyfried/Früh,* Banking Law and Capital Market Law, 7th ed. 2025, para. 1.53 f.
[38] Federal Network Agency, Federal Network Agency to become central platform supervisor for Germany, May 14, 2024, available at: https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2024/20240514_DSC.html; see also *Müller,* MMR 2022, 1007 (1010).
[39] See Section 29 of the Digital Services Act.
[40] See Recital 117, 144 of Regulation (EU) 2022/2065.

previous financial year may be imposed for breaches of obligations[41]. Specific infringements, such as providing incorrect, incomplete, or misleading information or not allowing inspections, can result in fines of up to 1% of global annual turnover. In addition, penalty payments of up to 5% of average global daily turnover or daily revenues may be imposed under Art. 52(4) DSA.

Special provisions apply to systemically important platforms, with fines of up to 6% of global annual turnover under Art. 74(1) DSA and penalty payments of up to 5% of average daily revenue under Art. 76(1) DSA.

While this theoretically is a substantial enforcement framework, in practice there are considerable issues, starting with the excessive length of proceedings for even simple requests from affected parties.

However, enforcement of the DSA has become a high-profile and geopolitical issue, especially since Donald Trump took office in 2025. On February 21, 2025, the Trump administration published a memorandum intended to protect American tech companies from "extortion and unfair fines from abroad", explicitly mentioning tariffs as a countermeasure. The memorandum clearly states that American companies would no longer support "failed foreign economies" through "extortionate fines and taxes"[42].

Platform entrepreneurs such as Elon Musk, Mark Zuckerberg, and Tim Cook have, at least demonstratively, sided with Trump to fight European regulations, specifically the DSA. During the election campaign, US Vice President Vance threatened to make American NATO support contingent on the EU not taking action against X[43].

The Wall Street Journal reports that, in the trade dispute between the US and the EU, the enforcement of the Digital Markets Act[44] could also be put on hold for US companies such as Alphabet, Meta, and Apple[45]. According to the report, a draft "reciprocal trade agreement" is circulating in the office of the US Trade Representative, covering not only the digital sector but also CO2 border taxes and other areas. Meanwhile, the US House of Representatives openly portrays the DSA as a *censorship law* in working reports[46].

Overall, there appears to be justified concern that European digital laws could become a bargaining chip between the EU and the Trump administration to prevent tariffs on European goods such as wine, steel, or motor vehicles; thus, European digital laws would not be enforced by the European Commission or Member State authorities. This would clearly contradict the goal of digital sovereignty for the European Union and its citizens (see above, D.). Legal principles must not be compromised for economic reasons, and the EU Commission and coordinators for digital services must not retreat from their role as enforc-

[41] The DSA does not define the term "provider", but it can be assumed that the antitrust concept of economic entity applies to the calculation of turnover, see *Denga*, Attribution, 2022, p. 203 ff.
[42] *The White House*, Fact Sheet: President Donald J. Trump Issues Directive to Prevent the Unfair Exploitation of American Innovation, February 21, 2025, para. 1.
[43] *Gehrke* SZ 31.03.2025, available at: https://www.sz-dossier.de/tiefgaenge/2025-03-31-die-meinungsfreiheit-der-dsa-und-raum-fuer-verbesserung-ff27f597.
[44] EU Regulation (EU) 2022/1925.
[45] *Hancock* WSJ 03.06.2025, available at: https://www.wsj.com/tech/meta-to-challenge-eu-tech-crackdown-on-platforms-8f10f1e6.
[46] Interim Staff Report of the *Committee on the Judiciary of the U.S. House of Representatives*, THE FOREIGN CENSORSHIP THREAT: HOW THE EUROPEAN UNION'S DIGITAL SERVICES ACT COMPELS GLOBAL CENSORSHIP AND INFRINGES ON AMERICAN FREE SPEECH, July 25, 2025, available at: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/2025-07/DSA_Report%26Appendix%2807.25.25%29.pdf.

ers. Rather, pursuing effective European digital sovereignty requires a significant reduction in the discretion of the commissioned authorities, which may *oblige* to intervene into business models[47]. However, this makes private enforcement even more important if supervisory mechanisms fail to ensure the effectiveness of European digital regulations such as the DSA.

2. Private enforcement of the DSA

a) *Effet utile* and complementarity of private and supervisory law

The idea of private enforcement of European law in the digital single market reflects the typical expansion of traditional enforcement mechanisms under EU law. While classic enforcement models primarily rely on state actors and the European Commission as central enforcement authorities, private enforcement models allow for decentralised enforcement by private actors such as civil society organizations, consumer associations, and affected users. Private enforcement thus functions both as a complement to official supervision and as a democratic corrective against potential enforcement deficits on the part of state authorities—private law and supervisory law are thus mutually "fallback arrangements"[48]. The concept of *effet utile* from Art. 4(3) TEU is central to this theory of private enforcement[49], especially when public enforcement appears questionable[50].

The legal challenge lies in ensuring consistent enforcement while maintaining the institutional balance between supranational, national, and private enforcement mechanisms; the effectiveness of this hybrid model depends largely on the procedural design of the complaint mechanisms and coordination between various enforcement actors.

A specific feature of European law is the separation of powers between the enforcement levels. The ECJ only requires Member States to ensure that private law sanctions are "effective, proportionate, and dissuasive[51]". Liability law is a key instrument in this regard due to its compensatory and preventive functions[52].

b) Requirements for private enforcement

While there is broad agreement on the above premises, it is not clear exactly when private enforcement can take effect by way of tort law. Outside of written norms, such as the Antitrust Damages Directive[53],

[47] On the analogous question in antitrust law, see *Dogs,* Die Verpflichtung der EU-Kommission zum Eingreifen gegen unternehmerische Wettbewerbsverstöße (The EU Commission's obligation to intervene against corporate violations of competition law), 2022; on the independence deficit of the European Digital Services Board, see *Schnidrig* ZUM 2025, 584.
[48] *Hoffmann-Riem/Schmidt-Aßmann/Hoffmann-Riem,* Public Law and Private Law as Reciprocal Fallback Arrangements, 1996, p. 261, p. 290 f..
[49] Central to this is ECJ v. 17.9.2002 – C-253/00, ECLI:EU:C:2002:497 – *Muñoz,* – para. 30; in detail *Poelzig,* Normdurchsetzung durch Privatrecht (Enforcement of Norms through Private Law), 2012, p. 77 et seq., 208 ff.; for a historical classification up to the law of the digital single market, see *Bauermeister/Schwamberger/Pauer,* Private Enforcement im Digitalen Binnenmarkt, 2025, pp. 1-9; for criticism in the literature of overly blanket application, see only *Schmolke* NZG 2016, 721 (728).
[50] See ECJ, September 20, 2001 – C-453/99, ECLI:EU:C:2001:465 (Courage and Crehan) – para. 26; *Heinze,* Schadensersatz im Unionsprivatrecht (Damages in EU Private Law), 2017, p. 521 ff.
[51] ECJ, October 2, 1991 – C-7/90, ECLI:EU:C:1991:363 (Paul Vandevenne) – para. 11; July 10, 1990 – C-326/88, ECLI:EU:C:1990:291 (Anklagemyndigheden) – para. 17; *Poelzig,* Normdurchsetzung durch Privatrecht, 2012, p. 362.
[52] See *Heinze,* Schadensersatz im Unionsprivatrecht (Damages in EU Private Law), 2017, p. 539 et seq.; for economic studies, see the references in footnote 23; for differences in the rights to damages in the Member States, see *Bauermeister/Schwamberger/Messner-Kreuzbauer,* Private Enforcement im Digitalen Binnenmarkt (Private Enforcement in the Digital Single Market), 2025, p. 59 ff.
[53] EU Directive 2014/104/EU; see *Kersting/Preuß,* Implementation of the Antitrust Damages Directive (2014/104/EU) – A Legislative Proposal from Academia, 2015, p. 2, 156, 183, among others.

this is uncertain territory[54]. The requirement for direct application of the norm will likely remain uncontested,[55] but this is a given in the predominantly regulatory nature of European digital market law. Yet, the requirement for individual entitlement is already problematic[56] and has become more relevant since the ECJ's *Thermofenster* ruling[57]. In that case, against the backdrop of the legal policy implications of the *Dieselgate* proceedings, the ECJ interpreted individual entitlement based on the German doctrine of protective laws ("Schutzgesetzdoktrin") and affirmed the individual protection of Type Approval Regulation 715/2007, even though its wording was geared towards a high level of environmental protection. However, if private enforcement relies on "fundamental purpose[58]" and importance to the EU market regime[59], this covers many European digital law standards, especially those related to digital sovereignty (above, D.), and the main prevention and guarantee mechanisms of the DSA. The exclusion of private enforcement by means of liability law is neither expressly mentioned in the DSA, nor does it follow from other private law instruments[60]; on the contrary, the DSA expressly mandates private enforcement in Art. 54:
"Recipients of the service shall have the right to seek, in accordance with Union and national law, compensation from providers of intermediary services, in respect of any damage or loss suffered due to an infringement by those providers of their obligations under this Regulation[61]."

c) Civil law points of reference

If the DSA standards are appropriate for private enforcement under liability law, they can be implemented through three distinct constructs of German civil law[62]: the protective law doctrine ("Schutzgesetzdoktrin") under Section 823(2) BGB; the duty of care doctrine ("Sorgfaltspflichtendoktrin") under Section 823(1) BGB; and the ancillary obligation doctrine ("Nebenpflichtendoktrin") under Section 241(2) BGB. Current focus on the protective nature of directly-applicable EU law standards as a result of the ECJ's *Thermofenster* ruling overlooks the role these standards play in specifying the general duties of care. Harm to the protected goods and rights in Section 823(1) BGB can raise the question of breach of protective duties (in a corporate context, "organizational obligations"[63]), making the conduct of management personnel and representatives within the meaning of Section 31 BGB relevant[64]; the detour via

---

[54] For an overview, see *Heinze,* Damages in EU Private Law, 2017, p. 518 ff.; see also *Wagner JZ 2018, 130 (132); Mörsdorf RabelsZ 83 (2019), 797 (817 et seq.); similarly Ebers, Rechte, Rechtsbehelfe und Sanktionen im Unionsprivatrecht (Rights, Legal Remedies and Sanctions in EU Private Law), 2016, p. 52; Cless, Unionsrechtliche Vorgaben für eine zivilrechtliche Haftung bei Marktmissbrauch (EU Law Requirements for Civil Liability in Market Abuse), 2018, p. 76.*
[55] See only *Wagner* AcP 206 (2006), 352 (418).
[56] See also *Heinze,* ibid., p. 520 f.
[57] ECJ NJW 2023, 1111 para. 68 et seq., 85; critical on this point *MüKoBGB/Wagner,* 9th ed. 2024, BGB § 823 para. 638: "disturbingly unclear".
[58] See ECJ 20.9.2001, Case C-453/99, ECR 2001, I-6297 para. 20 – Courage; see also *Weyer* ZEuP 2003, 318 (335): "This [reference in Courage to the fundamental nature of Article 101 TFEU] leaves open the possibility of limiting the new concept to fundamental provisions of the EC Treaty".
[59] ECJ 20.9.2001, Case C-453/99, ECR 2001, I-6297 para. 27 – Courage: "actions for damages before national courts can contribute significantly to maintaining effective competition in the Community"; ECJ 17.9.2002, Case C-253/00, ECR 2002, I-7289 para. 31 – Muñoz: "actions brought by competitors before national courts are particularly well suited to contributing significantly to ensuring fair trade and market transparency in the Community"; See also *Riesenhuber,* Europäisches Vertragsrecht (European Contract Law), 2006, para. 237, for capital market conduct obligations.
[60] On these negative criteria, see *Heinze,* ibid., p. 524 ff.
[61] See, for example, *Bauermeister/Schwamberger/Zurth,* Private Enforcement in the Digital Single Market, 2025, p. 28 et seq.; see also *Weigl/Wittershagen* BRZ 2/2024, 106 et seq.
[62] On the relevance of national tort law, see, for example, *Heinze/Steinrötter/Denga/Achleitner,* EU Platform Law, 2024, p. 48 f.
[63] See also *MüKoBGB/Wagner,* 9th ed. 2024, BGB § 823 marginal no. 111; *Denga,* Attribution, 2022, p. 91 ff.; fundamental to the concept of joint tort *Kleindiek,* Tort Liability and Legal Persons, 1997; most recently also *König,* Corporate Liability, 2023.
[64] Even further, without reference to the company's personnel, *König,* Unternehmenshaftung, 2023, p. 541 ff.

Section 823(2) or Section 826 BGB thus only applies in the case of pure financial losses[65]. If there is a platform usage agreement between the platform and the injured user[66], the standards of the DSA can also specify the ancillary obligations owed[67]. In addition to enforcement under liability law, injunctive relief claims analogous to Section 1004 BGB may also be considered[68]. The activation of German liability standards will undoubtedly lead to problems of proof; however, they must be interpreted in light of the regulatory objectives of the DSA in order to be effective in practice (see above, D.). This means the principles of producer liability may apply via the reversal of the burden of proof (see below, H. VII.).

d) Active and passive legal standing

Private enforcement also raises the question of active and passive legal standing. In addition to injured parties, associations may also have active legal standing. Collective rights enforcement is made possible by the Consumer Rights Enforcement Act (VDuG), the Injunctive Relief Act (UKlaG), and the Model Declaratory Judgment Act (MuFKG). According to Section 3(1) UKlaG, associations can take legal action if they are organized as associations with legal capacity whose statutory tasks include the promotion of commercial or independent professional interests, or if they are recognized as qualified institutions under Section 4 UKlaG. In addition, pursuant to Section 3(3) UKlaG, associations must have at least 75 members, or at least one member association with 75 members. Associations qualifying as consumer protection associations under Section 4 UKlaG must be registered in the list of qualified institutions at the Federal Office of Justice. Art. 86 DSA confirms the right of users to be represented by associations in the enforcement of their rights, an essential instrument for realising digital sovereignty in asymmetrical power situations in a platform economy.

Although Art. 54 DSA guarantees a claim for compensation against providers of intermediary services, personal liability of staff is not excluded, which will be discussed below.

II. Personal liability of staff

Platform obligations are enforced not only through regulatory and private law liability of the providers of intermediary services, but also through the personal liability of their staff. This is a fundamental aspect of intermediary regulation on the internet—companies' ability to act as intellectual constructs and disseminate their content globally relies on the personal localisation of their staff[69]. Individuals are therefore also personally liable for systemic risks[70]. The liability of organs and acting personnel under German[71] private law[72] is shown schematically[73] here.

---

[65] For example, in the context of the "diesel scandal," Federal Court of Justice, judgment of May 25, 2020 – VI ZR 252/19.
[66] On this Röhricht/Graf von Westphalen/Haas/Mock/Wöstmann *HGB/Bernzen/Specht-Riemenschneider*, 6th ed. 2023.
[67] On the specific problem of enforcing community standards from general terms and conditions, see *Holznagel* CR 2023, 539-545.
[68] On general personal rights within the framework of Section 1004 BGB, see *MüKoBGB/Raff*, 9th ed. 2023, BGB Section 1004 margin no. 37f.
[69] See *Goldsmith/Wu*, Who controls the internet?, 2006, p. 79 ff.; a general principle of limiting the liability of management personnel or concentrating liability on the association is not apparent in the law and cannot be recognized from an effectiveness perspective. On the limited scope of the limitation of liability of corporations, see *Pistor*, Code of Capital, 2019, p. 60 ff.; on personal responsibility as the basis of the market economy, see, for example, *Euken*, Grundsätze der Wirtschaftspolitik, 6th ed. 1990, p. 279 ff.; in principle also *Friedman*, Free to choose: A personal statement, 1980, p. 138; on the legal situation in the US, even with a discussion of strict liability of management personnel for corporate offenses with numerous references*, see Anderson/Gerding*, Directors' personal liability for corporate fault: a comparative analysis, 2008, p. 301 ff.
[70] This is contrary to the diffusion of responsibility in complex, systemic risk situations; from a sociological perspective, see *Beck*, Gegengifte: Die Organisierte Unverantwortlichkeit, 1988, p. 218 f.; for a detailed dogmatic justification of liability, see below, F. II. 2.
[71] See 3. below; classification under private international law remains necessary in individual cases.
[72] An examination of the basis for claims in individual cases remains necessary.
[73] Criminal liability, in particular from a position of guarantor or aiding and abetting, is not considered here.

1. Corporate liability under company law

Corporate liability under §43 GmbHG and §93 AktG constitutes purely internal liability of management towards the company, which serves to protect the company's assets. At the same time, executive bodies' duties of care towards the company are concentrated to avoid a race among injured parties for the personal liability of the executive bodies[74]. Instead, third parties can initially only seek compensation from the company for damages they suffer due to organizational errors made by the company's management personnel—at least insofar as the management personnel cannot be proven to have committed a personal offense (see below, F. II. 2. for more details)[75].

Management must exercise the "care of a prudent and conscientious manager" (cf. §43 GmbHG; §93 AktG). This standard of care follows the "business judgment rule"[76], which shields management decisions from judicial review and liability if: (1) there is no relevant management interest in the decision (disinterested judgment); (2) the decision is based on sufficient information (informed judgment); and (3) the decision is in the best interests of the company (rational belief and good faith)[77].

Management bodies must comply with all laws[78], including the DSA provisions. Compliance obligations extend to all company activities and require continuous monitoring of all business processes. In addition, establishing a functional compliance organization (beyond Art. 40 DSA, as a "duty to monitor legality") is mandatory[79], which includes training in critical legal matters such as DSA compliance. Management must ensure a corporate culture geared towards legality and focused on preventing DSA violations and infringements of personal rights. This cultural dimension of compliance requires not only formal rules and regulations, but also a living legal culture that permeates all levels of the company, from the "tone from the top"[80] and the establishment of a whistle-blowing system[81] to appropriate handling of specific compliance violations in the "triad"[82] of education, correction, and punishment.

Per the *ARAG/Garmenbeck* ruling of the Federal Court of Justice, the supervisory board has a duty to independently examine the corporation's claims for damages against members of the management board since it is responsible for monitoring tasks and has control over the activities of the management board. In conducting these examinations, the supervisory board will take into account the broad scope of action granted to the management board[83]. The *ARAG/Garmenbeck* ruling applies to other legal structures[84]. As a last resort, if both the management board and the supervisory board neglect their duties, enforcement can take place via *actio pro socio*.

[74] *Hopt/Hopt,* 44th ed. 2025, HGB Annex § 179 marginal no. 19; cf. *MHLS/Ziemons,* 4th ed. 2023, GmbHG § 43 margin no. 368; *BeckOGK/Fleischer,* as of 01.06.2025, AktG § 93 margin no. 384.
[75] *MüKoBGB/Wagner*, 9th ed. 2024, BGB § 823 margin no. 155, 159.
[76] Fundamental BGH II ZR 175/95 – ARAG/Garmenbeck; codified in § 93 (1) sentence 2 AktG.
[77] With further references *MüKoAktG/Spindler,* 6th ed. 2023, AktG § 93 margin no. 44.
[78] With further references: *MüKoAktG/Spindler,* 6th ed. 2023, AktG § 93 margin no. 89 ff.
[79] LG Munich I 5HK O 1387/10 marginal no. 93 – Siemens/Neubürger; *BeckOGK/Fleischer,* as of June 1, 2025, AktG § 91 marginal no. 47.
[80] *MüKoGmbHG/Fleischer,* 4th ed. 2023, GmbHG § 43 margin no. 190-193
[81] See Forgó/Helfrich/Schneider Betr. *Datenschutz-HdB/Chr. Schröder,* 3rd ed. 2019, Part VI. Chap. 3 margin no. 48 ff.; see also *Gerdemann,* Europe's New Whistleblowing Laws, 2023, p. 7.
[82] See *Moosmayer* Compliance, 4th ed. 2021, margin note 4.
[83] BGH II ZR 175/95.
[84] Lutter/Hommelhoff/Kleindiek GmbHG, 21st edition 2023, GmbHG § 43 margin note 23; Scholz/Verse GmbHG, 13th edition 2025, GmbHG § 43 margin note 71.

2. Direct liability of acting personnel

Under Section 823(1) BGB, platform personnel may be liable for commission of personal torts. The general right of personality[85] could be violated, for example, by personal defamation in user posts published on a social media platform.

Since German liability law does not require a *causa proxima*, operating a social media platform can give rise to a violation of personality rights[86]. Under Section 830(1) BGB, any contribution to the operation of the platform is sufficient cause for the time being.

The central question is therefore whether the personnel in question are independently guilty of negligence under Section 276 BGB. The question of intentional or negligent action arises in connection with a breach of duty of care (also: traffic safety obligations); if there is a breach of the duty of care, negligent behaviour is necessarily present[87]. Indirect violations of legal interests in broad causal chains can also be attributed in this way, so that the distinction between action and omission is superfluous[88].

The duty of care is a general behavioural guideline according to which every participant in legal transactions must protect the legal interests of others. This "general formula" is loaded with context-specific meaning[89].

The obligations of the DSA specify the nature of the general duty of care, even if the obligations are placed directly on the platform, not on its staff. The duty of care of the staff is not identical to that of the company; as is the case with public law requirements, a normative consolidation of the supervisory program is required to create a specific set of obligations for the staff[90]. However, the DSA certainly has an *indirect* effect on staff, as the legal act objectively defines the quality of the intermediary services provided. The public interests of digital market regulation (see D. below) and the very specific, and therefore predictable, obligations under the DSA can justify an externally-effective duty of care on the part of the staff of an intermediary service to comply with the requirements of the DSA.

The benefits and burdens of liability law also favour binding the staff of intermediary services to the DSA's obligations. This is because anyone who is employed by an intermediary service, i.e., who benefits from its business activities, is also responsible for compliance[91]. Of course, this responsibility applies exclusively within the scope of each individual's professional responsibilities [92] confined to their respective areas and the objectively identifiable risks[93]. Challenging questions may arise regarding the

---

[85] See *MüKoBGB/Wagner,* 9th edition 2024, BGB § 823 margin note 220; see also Jauernig/Teichmann, 17th edition 2018, BGB § 823 margin note 65; BVefG NJW 2006, 595.
[86] MwN *Denga,* Attribution, 2022, p. 101.
[87] Grüneberg BGB, 83rd ed. 2024, BGB § 823 margin no. 175; *MüKoBGB/Wagner,* 9th ed. 2024, BGB § 823 margin no. 497.
[88] *Medicus/Petersen,* Civil Law, 30th ed. 2025, § 25.
[89] On the establishment of obligations as an attribution operation, see *Denga,* Attribution, 2022, p. 304 ff.
[90] Analogous to personal liability for breach of capital market law obligations, see, for example, BGH III ZR 105/22 (= BKR 2024, 325 with note by *Denga)*; cf. also with further references *Kleindieck,* Deliktshaftung und juristische Person, 1997, p. 391 et seq.
[91] On the benefit-burden paradigm as a basis for liability, see *Denga,* Attribution, 2022, p. 79 et seq. In the context of corporate social responsibility (CSR), responsibility is understood as a basic condition of the market economy, cf. e.g. COM (2011) 681 final, p. 7; on the concept of CSR, see *Fleischer/Kalls/Vogt/Fleischer,* Corporate Social Responsibility, 2017, pp. 1-38; see also *Schnitker* zfpp 2017, pp. 246f.; fundamental to the framework of the free market economy *Euken,* Grundsätze der Wirtschaftspolitik, 6th ed. 1990, p. 279.
[92] On this basic idea of civil law liability, *see Canaris,* Die Vertrauenshaftung im Deutschen Privatrecht, 1971, § 38 III; in the context of supply chain liability, see also *MüKoBGB/Wagner,* 9th ed. 2024, § 823 margin note 123 et seq.; in the context of AI liability, see *Denga* CR 2018, 69 (72); fundamental to the framework of the free market economy, *see Hayek,* The Constitution of Liberty, 3rd ed. 1991, p. 102.
[93] On the objective standard for breaches of duty of care: *MüKoBGB/Grundmann,* 9th ed. 2022, BGB § 276 margin no. 55 f.

delineation of duties, particularly regarding institutional departmentalisation[94] where management retains oversight responsibility[95]. Delegating tasks to subordinates does not relieve individuals of their general duty to oversee legality; they must supervise those they assign tasks to[96]. Management bodies remain responsible and, in the event of a breach of their duty to monitor legal compliance, are jointly and severally liable with the direct participants under Sections 830 and 840 BGB.

Although determining a breach of duty of care is always done on a case-by-case basis, the following are typical points of reference for activities on behalf of intermediary service providers:

- Failure to comply with, or suppression of, reports of illegal content, under Art. 16 f. DSA;
- Failure to delete illegal content that the provider is aware of, under Art. 6 DSA;
- Manipulative design of the user interface, under Art. 25 DSA;
- Allowing profile-specific advertising to minors, under Art. 28;
- Failure to establish an adequate compliance department, under Art. 41 DSA; and
- Failure to report illegal activities within the company, for example to the compliance department.

Due diligence issues enter a grey area when fundamental rights are involved: for example, when content is misjudged. In such cases, the personnel involved should consult their superiors or the compliance department.

Illegality stems from legal rights' violations[97], and causality is usually straightforward, but calculating damages is more complicated since the national damage doctrine must be interpreted in light of effectiveness and implementation of European law[98].

3. Applicability of German law and jurisdiction of German courts

If a person with habitual residence in Germany is affected by content disseminated via a social media platform, German civil law is applicable and German courts have jurisdiction.

When a violation of personal rights occurs through dissemination via a social media platform, German civil law is applicable and German courts have international jurisdiction as long as there is a sufficient domestic connection, such as when someone with habitual residence in Germany is directly affected by the content in question. In such a case, the alleged damage—the violation of general personal rights—occurs in Germany, which means that there is a sufficient connection to the German legal system under both private international law and international civil procedural law.

Regarding applicable law, Regulation (EC) No. 864/2007 (Rome II Regulation) does not expressly apply to violations of personality rights pursuant to Art. 1(2)(g). This means that the connection is not determined by the Rome II Regulation, but by national private international law under Art. 40-42 EGBGB[99]. According to these provisions, tort claims are based on the place where harm occurs. In supreme court case law, when there are violations of personal rights via the Internet, the place of harm is where the interference with the person's legal interests becomes noticeable, i.e., where the violation of personal

---

[94] On the relevance of departmentalization under tort law, see *Mascherini,* Die Ressortverteilung als Instrument zur Enthaftung der GmbH-Geschäftsführung, 2021, p. 26f.; see also *Wilhelmi,* Risikoschutz durch Privatrecht, 2009, p. 219.
[95] See only *Bachmann,* Expert Opinion E for the 70th DJT, 2014, p. E 42.
[96] From the literature on stock corporation law, see *Grigoleit/Grigoleit* AktG, 2nd ed. 2020, § 77 marginal no. 3; *Grigoleit/Koch* AktG, 2nd ed. 2020, § 76 marginal no. 8; *Langenbucher* ZHR 2023, 187, (725 ff).
[97] *MükoBGB/Wagner,* 9th ed. 2024, BGB § 823 margin no. 5.
[98] On the autonomous concept of damage *Hofmann/Raue/Raue,* 2023, DSA Art. 54 margin note 10, 26, 4; for more details see *Bauermeister/Schwamberger/Hornkohl,* Private Enforcement in the Digital Single Market, 2025, p.
[99] *MüKoBGB/Junker,* 9th ed. 2025, Rome II Regulation Art. 1 margin note 59.

rights has a concrete effect[100]. If the person harmed habitually resides in Germany, the damage is considered to take place there. Thus, German tort law, in particular Section 823(1) BGB in conjunction with the general right of personality under Art. 1(1) GG, is applicable.

German courts have international jurisdiction in such cases under Art. 7 No. 2. EU Regulation No. 1215/2012 (Brussels Ia Regulation), which allows a person to be sued in another Member State if the damaging event occurs, or is likely to occur, there. The ECJ defines "damaging event" as both the place of action and the place of harm. For violations of personal rights through online publications, the place of harm is where the person concerned has the centre of their interests, which typically is their habitual residence. The ECJ expressly clarified this in its landmark decision ***eDate Advertising***[101], which confirms that a German court has jurisdiction over persons habitually residing in Germany as their social standing and personal integrity are affected there[102].

G. Making information obligations more effective

By imposing far-reaching information obligations on platforms, the DSA ties in with the information model[103], enabling users and authorities to make their own risk assessments.

I. Transparency program of the DSA

The DSA establishes a comprehensive transparency regime that covers various actors in the digital ecosystem. For intermediary services, the DSA establishes a tiered system of transparency obligations based on the size and social significance of the platforms. The DSA's fundamental transparency obligations are the general reporting obligations under Art. 15, which apply to all providers of intermediary services and include publishing transparency reports on content moderation measures[104].

Systemically important platforms (i.e., VLOPs and very large online search engines) are subject to extended transparency obligations under Art. 33 et seq. DSA. These include annual assessment of systemic risks (Art. 34 DSA), external, independent compliance audits (Art. 37 DSA), and data access provisions (Art. 40 DSA) which grant the Digital Services Coordinator or the Commission access to data necessary for monitoring and assessing DSA compliance. Art. 40(4) DSA also standardizes the provision of data to "vetted researchers". The DSA's transparency program aims to strengthen democratic accountability of large platforms and make their social impact measurable.

II. Problems, particularly regarding research data access

The effectiveness of research data access under Art. 40 DSA is undermined by significant practical challenges. To date, implementation of Art. 40 DSA has revealed clear weaknesses in the enforcement of transparency obligations, with two contrasting but equally problematic patterns of response emerging from the platforms.

---

[100] From the comprehensive case law on cross-border violations of personality rights, see only BGH VI ZR 489/16; with further references *MüKoBGB/Junker*, 9th ed. 2025, EGBGB Art. 40 margin note 74 et seq., 79 et seq.
[101] ECJ, judgment of October 25, 2011 – C-509/09 and C-161/10, *eDate Advertising* and *Martinez*, ECR 2011, I-10269 = NJW 2012, 137, para. 45 et seq.; most recently also ECJ, judgment of December 21, 2021 – C 251/20, *Gtflix Tv* = GRUR-RS 2022, 39577.
[102] *MüKOZPO/Gottwald*, 6th ed. 2022, Brussels Ia Regulation Art. 7 margin note 61.
[103] The information model relies on the provision of information as a means of achieving a regulatory purpose – see, for example, *Fleischer,* Informationsasymmetrie im Vertragsrecht, 2001, pp. 203–208, 570–572; *Kerton/Bodell* 29 Journal of Consumer Affairs 1995, 1, esp. 20–24; *Grundmann/Kerber/Weatherill*, Party Autonomy and the Role of Information in the Internal Market, 2001, esp. the introduction. On the limitations of the model, see, for example, ECJ judgment of May 16, 1989, Case 382/87 – Buet; *Schön* FS Canaris, 2007, 1191.
[104] See *Müller-Terpitz/Köhler/Barudi*, 2024, DSA Art. 15 para. 16ff.; *Mast/Kettemann/Dreyer/Schulz/Seckelmann*, 2025, DSA Art. 15 para. 31-34.

On one hand, platforms often refuse to provide substantial data by giving generic, meaningless answers. These superficial responses circumvent the intention of Art. 40 DSA by formally complying with the requirements, but in fact not providing any scientifically usable findings. Platforms deliberately exploit the vagueness of the legal requirements and limit themselves to general descriptions of their systems without granting access to their actual algorithms or providing concrete usage data. This strategy of "compliance by form" significantly undermines the DSA's transparency purpose.

On the other hand, some platforms practice "information overkill", overwhelming researchers with unstructured data sets that are extensive but unusable for scientific purposes. Without appropriate contextualisation, documentation, or methodological preparation, this flood of data makes meaningful scientific evaluation practically impossible. The provision of raw data without corresponding metadata, explanations of data structures, or information on data quality and limitations forces researchers to spend more time preparing data than analysing it, if analysis is even possible.

Both problems are exacerbated by the vague definition of data in Art. 40 DSA, which gives platforms considerable leeway in interpretation. Implementing secure access modalities is technically complex, and the 80-working-day deadline for justified requests is often not met. The enforcement of transparency obligations such as Art. 40 by digital services coordinators (in Germany, the BNetzA) has significant weaknesses, particularly in assessing the quality and usability of the data provided. Coordinated application among Member States is likely to be difficult, which could lead to inconsistent standards and allow platforms to exploit the weakest regulatory approaches.

III. Current measures by the European Commission

In the Delegated Regulation of July 1, 2025, the European Commission standardised technical conditions and procedures for data access[105]. By standardising procedures through the establishment of the "DSA data access portal", which serves as a central digital infrastructure for data exchange between researchers, data providers, and digital services coordinators, this new regulation addresses key implementation issues. Art. 9 of the Delegated Regulation specifies the technical, legal, and organisational measures that data providers must implement for data access. Secure processing environments are key for providing access.

Art. 8 of the Delegated Regulation specifies the requirements for access and sets out the conditions for justified requests, including the requirements for researchers' independence from commercial interests and disclosure of research funding. Art. 13 of the Delegated Regulation also introduces a noteworthy procedure that allows data providers to request voluntary mediation in the event of disagreements over amendment requests, with the aim of achieving more efficient dispute resolution.

The Delegated Regulation attempts to harmonise supervisory practices and standardise procedures between the various authorities. Having to use the central DSA data portal and standardise assessment criteria addresses the previously fragmented application practices. In its July 2, 2025 opinion, the European Board for Digital Services described the Delegated Regulation as a "milestone innovation" for the DSA and recognised the critical role of researchers in ensuring greater online transparency[106].

IV. Further considerations

There is a significant transparency deficit in access to external audits under Art. 37 DSA. These audits, which must be carried out annually by independent auditors, remain largely confidential, with only final

[105] No official title yet, C (2025) 4340 final.
[106]See Press statement of the *European Board for Digital Services*, July 2, 2025, available at https://cdn.table.media/assets/press_statement_board_meeting_020725_adopted_sl70ejhpiq7xk3z1ziruimonbnk_117852.pdf

reports being published[107]. Extending transparency requirements to include full audit logs could significantly strengthen democratic control of very large platforms. The ongoing development of guidelines by the Commission, particularly on "trusted flaggers" and on the protection of minors, demonstrates the continuous development of the transparency regime. These guidelines specify the general DSA provisions and create practicable standards for implementation.

A critical aspect of DSA transparency is the "meaningful consultation" of stakeholders in systemic risk analyses[108]. Practical implementation of this consultation requirement has considerable quality deficiencies. Platforms often limit themselves to superficial hearings without substantially incorporating stakeholder input their risk analyses. Approaches for improvement should include structured consultation procedures, binding obligations for platforms to respond to stakeholder input, and external review of the quality of consultations.

The DSA's transparency obligations are a classic information model approach[109]. The Delegated Regulation of July 2025 addresses important implementation issues, particularly regarding access to research data. Nevertheless, significant challenges to practical enforcement remain unchanged. Successful implementation requires continuous development of regulatory instruments and consistent enforcement by the competent authorities. The DSA transparency regime's long-term success depends on its ability to reduce structural information gaps between platforms and social actors. Achieving this requires a high-quality information standard, such as including complete audit logs (Art. 37 DSA) within the scope of Art. 40 DSA.

H. Key legal policy measures to increase the security of social media platforms

Social media platforms pose dangers to the legal interests of general personal rights and the formation of public opinion, as briefly described above (under B.), which raises the question of how to optimise accountability structures. The following suggested regulatory measures could improve the situation; however, they are intended to supplement existing obligations and can only be briefly summarised here[110].

I. Ban on social bots

Banning social bots would contribute significantly to increasing security on social media platforms. Such a ban would be justified legally because there is a lack of legitimate interest in automated expressions of opinion on social networks. Social bots systematically manipulate public discourse by simulating broad public sentiment, which distorts the democratic decision-making process. These bots are used by scammers, terrorists, and totalitarian regimes to manipulate users of social media platforms[111]. Identifying social bots is technically feasible, as they often exhibit conspicuous activity patterns and the creation of a user account can be linked to user identification (see II.). The fundamental rights of bot operators at issue here—entrepreneurial freedom and freedom of expression—weigh significantly less than the impaired freedom of information of all other users[112]. Therefore, any lingering uncertainty regarding the true impact of social bots does not change the fact that social media platform users have a

---

[107] Critical of the procedure *Holznagel*, Shortcomings of the first DSA Audits — and how to do better, 2025, available at: https://dsa-observatory.eu/2025/06/11/shortcomings-of-the-first-dsa-audits-and-how-to-do-better/; also critical *Laux/Wachter/Mittelstadt*, Computer Law & Security Review, Volume 43, November 2021, 105613.
[108] See Art. 42 DSA.
[109] *Denga* ZfPW 2024, 427 (450).
[110] A concept for the regulation of digital technologies, in particular social media platforms, based on democratic principles can be found in *Susskind*, The Digital Republic, 2022, esp. p. 267 ff. (Part Ten).
[111] See, for example, the study by *the Office of Technology Assessment at the German Bundestag*, Social Bots, TA Preliminary Study, 2017; see also *von Ungern-Sternberg* RW 2022, 94.
[112] With a comprehensive assessment, but ultimately against a ban, *see Dürr*, Social Bots, 2024.

constitutionally-protected right to be free from artificially generated expressions of "opinion"[113]. A ban on social bots would restore the authenticity of digital discourse and strengthen users' self-determination by enabling them to form their opinions based on genuine human expressions. A mere labelling requirement, as already provided for in the AI Regulation[114] and the State Media Treaty[115], cannot offer sufficient protection in view of the grave threats in the digital space.

II. User identification via video identification

Introducing a real-name registration requirement for users of social media platforms vis-a-vis the platform would significantly enhance security by promoting actual individuals using the platform while maintaining pseudonymity in public platform traffic[116]. Registration could be done in the same way it is handled in financial services, via video identification procedures that are now standardised, user-friendly, and can be completed quickly—in less than ten minutes using mobile devices[117]. This system strikes a balance between effective law enforcement and freedom of digital discourse. While platforms can determine the true identity of users in the event of legal violations, anonymous and pseudonymous expression of opinion in the public sphere remains guaranteed. This aligns with constitutional requirements that restrictions of fundamental rights must be proportionate and use the least severe means available. The video identification solution would combine the advantages of reliable identity verification with the protection of anonymous speech, an essential element of democratic participation. Naturally, there would need to be sufficient safeguards against unauthorized access to user identities[118].

III. Right to content filtering

The obligation for platforms to filter content in real time by automatically blocking problematic content is highly questionable in terms of fundamental rights, as it would effectively amount to prior censorship[119]. Instead, the introduction of a right to content filtering, which requires platforms to provide configurable filter options but leaves use of the filters up to users themselves, is preferable from a legal perspective[120]. These filters should offer various levels of severity and allow users to tailor content to their individual preferences. In addition, preventing taking screenshots of content—at least as an optional right for users—should be considered to make the unauthorised distribution of private content more difficult. However, the practical limitations of this strategy and circumvention ability must be considered. It is also important to consider whether restricting documentation of possible criminal offenses could cause unintended harm.

IV. Qualification of management

Social media platforms should have specific qualification requirements for their executives and local representatives to ensure they are able to meet the challenges of digital opinion spaces, similar to the "fit and proper" requirements in capital market law[121]. Under Art. 4 of the AI Act, AI competency is

[113] On negative freedom of information, see, for example, BeckOK *InfoMedienR/Kühling*, 48th ed. 01.05.2025, GG Art. 5 Rn. 44.
[114] See Art. 50(1) AI Regulation.
[115] See Sections 18(3) and 93(4) MStV.
[116] This is also the conclusion of the study by *G'sell*, Has the time come to end anonymity on social media?, 2023.
[117] See *Moosmayer/Lösler/Diergarten* Corporate Compliance, 4th ed. 2024, chap. 3, para. 749 ff.
[118] On the risks of mandatory identification, using China as an example, see *Lee/Liu*, 25 Wash. Int'l L.J. 1 (2016).
[119] This is also contrary to Art. 8 DSA, see *Müller-Terpitz/Köhler/Köhler*, 2024, DSA Art. 8 para. 49.
[120] See European Parliament, The impact of algorithms for online content filtering or moderation, 2020, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/657101/IPOL_STU(2020)657101_EN.pdf.
[121] See Art. 9(1), (6) MiFID II Directive 2014/65/EU; Art. 8-12 Delegated Directive (EU) 2017/593; Art. 8(1)(b) AIFM Directive 2011/61/EU; Art. 7 UCITS Directive 2009/65/EC; supplemented by CRD V Directive 2019/878/EU and CRR II Regulation (EU) 2019/876 for credit institutions providing investment services.

already required due to the significant role of algorithmic systems for modern platforms[122]. Introducing publicly organized or certified training is also desirable.

V. Transparency and legal remedies for shadow banning

Shadow banning, where content or users are algorithmically suppressed without being aware of it, poses a significant challenge to freedom of expression and the role of digital spaces in debate. While Art. 38 DSA covers personalised recommendation systems and requires a profiling-free option[123], the more comprehensive curatorial power of platforms remains largely unregulated in terms of content. Despite the Federal Court of Justice emphasising in its Facebook ruling the need to adapt terms and conditions to actual moderation practices[124], concrete criteria for shadow banning measures have not been established, let alone enforced. Art. 14(1) and (4) DSA require diligence, objectivity, proportionality, and respect for fundamental rights in enforcing restrictions to content, but these requirements have yet to be defined in detail.

This means that the obligation to provide reasons for restrictions under Art. 17(1)(a) DSA is not an effective control instrument. Platforms could simply use "incompatibility with the terms of use", as determined by automated means under Art. 17(3) DSA, as the reason for the restriction.

Platforms also do not communicate when shadow banning has taken place, and users are thus unaware that their content has been suppressed. Users would have to know that a restriction has taken place in order to demand a justification for the restriction under Art. 17 DSA. Further, the Commission cannot verify whether notification of content blocking under Art. 24(5) DSA has occurred. The right to inspect the calibration of platform moderation under Art. 40 DSA is subject to the problems already mentioned (above, G.); thus, access rights under Art. 40 DSA should extend to audit logs here as well.

The right to object to a shadow ban is also necessary: there should be an obligation to end a shadow ban and restore the user or the content's visibility if there is no objective reason for the ban. Art. 21 DSA does not provide a remedy here, as it only covers decisions under Art. 20 DSA. Yet, a right to object to shadow bans based on terms and conditions would allow users to enforce their own freedom of communication. Freedom of communication is an explicitly mandated right under Art. 14(4) DSA that Art. 54 DSA stipulates can, if necessary, be privately enforced (see above, F. 2.).

VI. Age restriction for social media

Requiring social media users to be at least 16 years old is in line with the latest psychiatric findings on the medical and social effects of digital media on brain development[125]. This age limit corresponds to other social age restrictions like the consumption of light alcohol and reflects the comparable effect of digital stimulation on the developing brain. Countries such as France and Australia have already implemented corresponding measures[126]; the Leopoldina also recommends regulating social media by age group due to the psychological dangers of apps[127]. The European Commission has taken the first steps toward a safer online space for children with its guidelines on age verification and app prototypes[128].

---

[122] See BeckOK *KI-Recht/Kaufmann*, 2nd ed. 1.5.2025, AI Regulation Art. 4 margin note 30ff.
[123] See *Müller-Terpitz/Köhler/Beyerbach/Seyer*, 2024, DSA Art. 38 margin note 7; on the "pay or okay" payment solution, see D'Amico Technology and Regulation 2024.
[124] BGH III ZR 179/20 and III ZR 192/20 = ZIP 2021, 1955-1956 (with note by *Denga)*.
[125] See the study by *the Center for Countering Digital Hate,* YouTube's Anorexia Algorithm, 2025; see also the lawsuit filed against Facebook on November 16, 2023, in California by 42 US attorneys general (4:23-cv-05448); see *Denga*, NJW-aktuell 3/2024, 15.
[126] See *Schmid/Feld*, Social Media in the EU soon only for ages 16 and up?, Tagesschau 06/07/2025, available at: https://www.tagesschau.de/ausland/europa/social-media-alter-eu-100.html.
[127] *Leopoldina*, Social media and the mental health of children and adolescents, July 2025 (in particular p. 36 ff.).
[128] See the European Commission press release of July 14, 2025, available at: https://digital-strategy.ec.europa.eu/de/news/commission-presents-guidelines-and-age-verification-app-prototype-safer-online-space-children.

The DSA's protection of minors, which so far has been limited to Art. 28 and general duties of care, needs to be substantially expanded, as platforms' designs exploit the vulnerability of young people[129]. Age identification could be carried out in the same way as financial services (see also H. II.).

VII. Reversal of the burden of proof in court

The burden of proof for liability cases in connection with platform damage should be reversed, following the example of the amended Product Liability Directive[130]. This would account for the structural information asymmetry between platform operators and injured users[131]. Platforms have comprehensive data on their algorithmic systems, moderation practices, and user behaviour, while injured parties have little insight into internal processes. A reversal of the burden of proof would force platforms to prove the legality of their practices and the absence of causal links to potential damage. Clarifying the reversal of the burden of proof would not only facilitate enforcement for those affected but would also provide incentives for platforms to make their systems more secure and transparent. Even *de lege lata*, the principles of producer liability could reverse the burden of proof[132], but clarification as to the reversal would promote legal certainty and have a preventive effect.

***

September 9, 2025

Prof. Dr. Michael Denga

[129] See also the evidence in footnote 125.
[130] See Art. 9 10 EU Product Liability Directive 2024/2853; see also Art. 3, 4 of the AI Liability Directive (COM (2022) 496), which was ultimately not pursued.
[131] Already decisive for the reversal of the burden of proof in product liability, BGHZ 51, 91 (104 ff.) – Hühnerpest; for an understanding of platform law as product law, cf. *Denga/Jungblut* ZfPC 2025 (in press).
[132] *Erman/Wilhelmi* BGB, 17th edition 2023, BGB § 823, margin note 112.