

One Function, Two Regimes: Trusted Flaggers and Regulatory Fragmentation under the Digital Services Act

Mindia Davitadze, Licensed Attorney

LL.M. in Law and Technology, University of California, Berkeley

LL.M. in European Intellectual Property Law, Stockholm University

Irakli Shamatava, PhD in Law

Affiliated Associate Professor, Caucasus University School of Law, Georgia

Editor-in-Chief, Caucasus Law Journal, Tbilisi, Georgia

Approved: 15 October 2026

Posted: 17 October 2026

Copyright 2026 Author(s)

Under Creative Commons CC-BY 4.0

OPEN ACCESS

Cite As:

Davitadze, M., & Shamatava, I. (2026). *One Function, Two Regimes: Trusted Flaggers and Regulatory Fragmentation under the Digital Services Act*. ESI Preprints.

<https://doi.org/10.19044/esipreprint.10.2026.p500>

Abstract

Article 22 of the Digital Services Act (DSA) gives trusted flaggers a statutory role. It did not, however, put an end to the voluntary programs that platforms ran before the Regulation, and these continue to operate in parallel. This article looks at what that parallel existence means for accountability in content moderation. Using doctrinal legal analysis, the article traces Article 22 from the Commission's proposal through the Council's general approach and the European Parliament's amendments to the adopted text and examines eligibility, expertise, independence, transparency and safeguards against misuse. Designation by a Digital Services Coordinator brings a clear advantage, since qualifying notices must be prioritized on every covered platform and the flagger no longer has to bargain for that priority platform by platform. Voluntary programs, by contrast, sit outside the designation, reporting and revocation rules. Platform-level transparency, systemic-risk and audit obligations reach them only indirectly, as they do not require disclosure of which organizations receive priority, on what criteria or with what results. The article identifies this difference in accountability as a limitation of the statutory framework. It proposes separate reporting of notices from voluntary priority programs, published eligibility criteria for such programs and their inclusion in systemic-risk assessments, largely

achievable within the existing Regulation. Priority requires prompt assessment of qualifying notices; it does not establish illegality or require automatic removal.

Keywords: Trusted flaggers; Digital Services Act; content moderation; notice-and-takedown; intermediary liability; transparency; Digital Services Coordinators

Introduction

Flagging is the process by which third parties report content to hosting services for moderation. Anyone may flag: a right holder, a public authority, a civil-society organization or an individual user. Over time, some notifiers acquired privileges because of the expertise they had shown in detecting particular categories of content, from hate speech and terrorist material to copyright infringement and breaches of platforms' terms and conditions.

Those privileges usually consisted of some priority in the processing of notices and access to dedicated interfaces or points of contact. They did not confer exclusivity: flagging remained open to all, and trusted flagging was one route among several for detecting illegal content (Appelman & Leerssen, 2022, p. 453).

Article 22 of the Digital Services Act (DSA) turns this practice into a statutory status awarded by national Digital Services Coordinators (DSCs). It does not, however, replace the voluntary programs through which platforms continue to privilege selected notifiers. By May 2026, DSCs had awarded the status to more than 70 organizations (European Commission, 2026b). A Commission-funded study, whose manuscript was completed in November 2024 and published in 2026, identified 47 voluntary trusted-flagger schemes (Pozzo et al., 2026). The same notification function is therefore performed under two regimes with different rules on eligibility, transparency and oversight.

This coexistence constitutes regulatory fragmentation. Where the two regimes overlap (and the overlap lies chiefly in the priority handling of notices alleging illegal content), one and the same function is governed partly by public designation and partly by private arrangement.

This article asks whether that coexistence undermines the accountability that Article 22 was designed to secure. Section 1 sets out the method. Section 2 traces intermediary liability and voluntary trusted flagging before the DSA. Section 3 analyses the statutory framework, including the legislative history of Article 22, priority processing and eligibility. Section 4 examines transparency, safeguards against misuse and the position of voluntary programs, including the extent to which other DSA provisions

reach them. Section 5 then turns to the accountability gap that results and suggests how it might be addressed without amending the Regulation.

1. Methods

The study examines trusted flagger designation under the DSA with a focus on eligibility, independence, priority processing and accountability, and compares the Commission's proposal, the Council's general approach and the European Parliament's amendments with the regulation as adopted. The sources are the relevant EU instruments, case law and academic writing. The analysis relies mostly on earlier literature for voluntary trusted flagging before the DSA and on more recent scholarship for the statutory framework. Contextual information comes from Pozzo et al. (2026), a study based on mapping and stakeholder interviews. Its manuscript was completed in November 2024, before publication in 2026.

The analysis also takes into account the Commission's draft guidelines under Article 22(8), which were put out for consultation in May 2026 (European Commission, 2026a). It should be stressed that the article is concerned with legal design. No original empirical data were collected, and the study does not measure how designated trusted flaggers perform in practice. Some of the arguments were first developed in the first author's LL.M. thesis (Davitadze, 2024) and are revised and updated here.

2. Intermediary Liability and Voluntary Trusted Flagging

2.1. Historical Development of Intermediary Liability

Specific safe harbors for intermediaries first appeared in the United States. The Digital Millennium Copyright Act (DMCA) of 1998 introduced them for copyright infringement and, with them, a notice-and-takedown procedure (Frosio, 2018; United States Congress, 1998). The DMCA model shaped how the industry came to remove or block notified content, and it also influenced the adoption of a comparable mechanism in the EU (Urban et al., 2017, pp. 45-46).

The EU followed in 2000 with the e-Commerce Directive, which set up a common framework of conditional liability exemptions for online intermediaries (European Parliament & Council of the European Union, 2000). A hosting provider that meets the conditions enjoys the safe harbor. The reverse does not hold, however: a provider that fails to meet them is not, for that reason alone, liable for unlawful content uploaded by its users. Whether it is liable is a question for the applicable substantive rules, including national rules on contributing to the infringement of a right (European Commission, 2020a, Part 2, p. 158; Rosati, 2023, pp. 268-269).

Soft law came next. In 2017 the Commission adopted a Communication, followed in 2018 by a Recommendation, both setting out

principles under which hosting service providers and Member States were to take effective, appropriate and proportionate measures against illegal content online (de Streel & Ledger, 2021, pp. 32-33). Trusted flaggers were addressed expressly, alongside notice-and-takedown mechanisms and safeguards based on human oversight. The aim was to make the notice-and-action process more effective and more transparent, to encourage voluntary measures by hosting service providers and to strengthen cooperation with stakeholders, trusted flaggers and public authorities among them (European Commission, 2017, 2018). In intellectual property enforcement, effective protection must be balanced against fundamental rights, the public interest and legal certainty (Shamatava, 2026a). Legislative reform alone does not demonstrate effective implementation and enforcement (Shamatava, 2026b).

2.2. Voluntary Trusted Flagging before the DSA

Voluntary trusted flagging predates the DSA. YouTube introduced its programme in 2012, and other platforms subsequently developed comparable arrangements under different names. Appelman and Leerssen describe Facebook's trusted flaggers and Trusted Partners, TikTok's Safety Partners and Twitter's Trusted Partners. These programmes shared a reliance on selected external contributors, although their functions were not identical: TikTok's partnerships, for example, could also involve advice on community guidelines (Appelman & Leerssen, 2022).

The YouTube arrangements examined in that study required participating flaggers to sign non-disclosure agreements. The public could not readily establish how many flaggers participated, which organisations were involved, how much content they reported or how often their reports led to removal. The resulting limits on external scrutiny illustrate a recurring weakness of voluntary cooperation (Appelman & Leerssen, 2022, p. 475).

The historical importance of contextual judgment is also apparent in van Benthem's analysis of terrorist content. His account of YouTube's voluntary programme describes human review of flagged material and the difficulty of distinguishing propaganda from material with another legitimate purpose. It also calls attention to the need for procedural transparency. These observations concern the earlier voluntary system, not statutory designation under Article 22 (van Benthem, 2018, pp. 291–292).

An early attempt to formalize trusted flagging relationships was EU Code of Conduct. Organized under the auspices of the European Commission in 2016, in the context of prevention and countering the spread of illegal hate speech online, this Code was originally signed by Facebook, Microsoft, Twitter, and YouTube (Schwemer, 2019).

The 2016–2019 assessment credited the Code of Conduct with faster review and removal of hate speech and closer cooperation between

companies, civil society and national authorities through structured exchanges of expertise (European Commission, 2019).

The 2022 joint statement set out a framework for closer cooperation between providers and trusted flagger organisations. It highlighted the contribution of high-quality notices and civil-society knowledge of local contexts and particular forms of hatred to platforms' trust and safety work (European Commission, 2022).

The earlier non-binding instruments already encouraged providers to cooperate with trusted flaggers and existing specialist networks. Examples included Europol's Internet Referral Unit for terrorist and violent extremist material, INHOPE hotlines for child sexual abuse material, and organisations specialising in unlawful racist and xenophobic content (European Commission, 2016, 2017, 2018, 2019, 2022).

The usefulness of trusted flaggers depends on how trust is established. Expertise alone does not resolve questions about transparent selection, independence and objective reporting. The Commission's recommendation envisaged clear, objective conditions for recognising competent and diligent flaggers, but those conditions were not binding. Castets-Renard identifies this absence of enforceable safeguards as a limitation of the earlier framework (Castets-Renard, 2020).

A related limitation is the response to misuse. In the approach discussed by Castets-Renard, withdrawal of privileged status should follow clear criteria where notices or counter-notices are submitted in bad faith. Platforms should explain those criteria in their terms of service and disclose their application through transparency reporting. These protections need to be mandatory if they are to provide effective accountability.

The same analysis supports scrutiny of moderation outcomes as well as moderation rules. Users, public-interest organisations, courts and public authorities should be able to examine how decisions operate in particular cases. Independent expert review could help establish whether the declared safeguards are reflected in practice. Meaningful access to such scrutiny should be mandatory.

Transparency should also enable affected users to obtain remedies when moderation systems malfunction. It must therefore extend beyond explanations of platform procedures to the protection of users' rights and, where appropriate, compensation for harm. These recommendations concern the design of safeguards rather than a description of duties already imposed by the earlier framework (Castets-Renard, 2020).

3. The Regulatory Framework for Trusted Flaggers under the DSA

3.1. The DSA Framework and Notice Procedures

In addressing the challenge of combating illegal online content, several major platforms proposed that independent third-party experts could play a pivotal role. Trusted flaggers were seen as a useful supplement to platform moderation, but concerns about due process highlighted the need to define their roles and responsibilities clearly. Statutory designation also operates alongside platform rules and user norms, which continue to shape moderation decisions (Frazier, 2024, p. 20).

The DSA revises elements of the e-Commerce Directive while extending the procedural framework surrounding intermediary activity. Its form as a regulation also differs from the earlier directive. The horizontal liability architecture remains, accompanied by more detailed obligations and rules that operate alongside sector-specific EU legislation. Where relevant, that legislation continues to apply as *lex specialis* (Peukert et al., 2022).

Articles 4–6 substantially retain the e-Commerce Directive’s conditional exemptions for mere conduit, caching and hosting. Some provisions consolidate established interpretations; others address questions such as active involvement and voluntary investigation of unlawful content, drawing on CJEU case law (Wilman, 2023, pp. 43–47).

The distinction between a neutral intermediary and an active role providing knowledge of or control over content developed in *Google France*, *L’Oréal v eBay* and *YouTube*. Recital 18 of the DSA reflects that case law (Court of Justice of the European Union, 2010, 2011, 2021).

Article 3 retains the established concept of an information society service, and due diligence duties are differentiated across four tiers: intermediary services, hosting services, online platforms, and very large online platforms or search engines, the last being those with at least 45 million average monthly active recipients in the Union. Article 22 belongs to the third tier: it applies only to online platforms (European Parliament & Council of the European Union, 2022, Articles 3(a), (g) and (i) and 33(1)).

Due diligence and exemption from liability operate on separate legal planes. The obligations attached to a type of service continue to apply even when its provider cannot rely on the relevant exemption. A hosting service, for example, remains subject to the applicable due diligence duties if the provider’s involvement in particular content prevents it from satisfying the safe harbor conditions. Compliance with those duties is not itself a condition for obtaining the exemption (Husovec, 2023, 2024).

Hajnal, writing from a consumer perspective, separates the liability framework that the DSA retained from its new, tiered duties of care. Among the ways in which a provider may become aware of illegal content, the analysis lists voluntary investigations, reporting mechanisms and trusted

flaggers. This distinction is relevant to the present analysis. The legal consequences of a particular notice must be assessed under the applicable liability rule; trusted flagger status does not itself establish an infringement (Hajnal, 2023, pp. 29–32).

Under Article 16, hosting providers must put in place a mechanism that allows individuals and entities to notify them of content they consider illegal. The mechanism has to serve effective enforcement while respecting the fundamental rights that moderation affects. A notice gives rise to actual knowledge or awareness for the purposes of Article 6 only if a diligent provider could identify the illegality of the specific information or activity from it without a detailed legal examination. It follows that submitting a notice does not, by itself, establish that the material reported is unlawful (European Parliament & Council of the European Union, 2022, Article 16(3)).

Article 3(h) defines illegal content by reference to non-compliance with EU law or compatible Member State law, irrespective of the law's subject matter or nature (European Parliament & Council of the European Union, 2022, Article 3(h)).

Recital 17 gives the liability exemptions a horizontal reach across the nature, origin and subject matter of the underlying liability rules, including intellectual property, defamation and hate speech (European Parliament & Council of the European Union, 2022, recital 17).

Hosting service providers assess notices against the applicable legal rules, taking account of context where relevant. If the assessment identifies illegal content, the provider may remove it or disable access to it. The notifying party must be informed of the decision where the applicable rules require this (Grimmelmann & Zhang, 2023). Where the relevant DSA provisions apply, users can challenge decisions on removal or disabling access through the internal complaint-handling system or seek out-of-court dispute settlement.

Any decision restricting access, visibility, monetization, or accounts of users, regardless of whether based on illegality or terms and conditions, should be reviewable. Both notifiers and affected authors of content can complain. Decisions about restrictions should be non-arbitrary, non-discriminatory, and proportionate (European Parliament & Council of the European Union, 2022, Articles 20(1) and 21(1)).

Each Member State must designate a Digital Services Coordinator to supervise and enforce the DSA. DSCs must act independently of public and private influence, and their contact information must be publicly available (European Parliament & Council of the European Union, 2022, Articles 49(2)–(3) and 50(2); European Commission, n.d.-a).

Member States may allocate enforcement functions among several authorities, reflecting the DSA's connections with consumer protection, media and data protection. A single DSC nevertheless coordinates those functions and cooperation at EU level (European Parliament & Council of the European Union, 2022, Article 49(2)–(3)).

Digital Services Coordinators perform supervisory functions of their own, rather than merely connecting other authorities. Jaursch argues that effective supervision requires capabilities such as data analysis, engagement with relevant communities and flexible case work. The statutory requirement for adequate technical, financial and human resources is consequently central to their ability to discharge their responsibilities (Jaursch, 2023).

DSCs hold significant enforcement powers, including the power to order the cessation of infringements, impose remedies, fines and periodic penalty payments, and adopt interim measures (Frosio & Geiger, 2023).

The Regulation distinguishes between the Digital Services Coordinator of establishment, in the Member State where the provider's main establishment is located or its legal representative resides or is established, and the Digital Services Coordinator of destination, in a Member State where the service is provided (European Parliament & Council of the European Union, 2022, Article 3). As Section 4.2 shows, neither is necessarily the authority competent for a trusted flagger.

National DSCs cooperate through the European Board for Digital Services, an independent advisory group composed of high-level representatives of the DSCs, which supports the consistent application of the DSA (European Parliament & Council of the European Union, 2022, Articles 61–62).

3.2. Legislative Negotiations on Article 22

The Commission published the DSA proposal on 15 December 2020, together with an explanatory memorandum and an impact assessment. The proposal addressed trusted flaggers in one recital (recital 46) and one article (Article 19 of the proposal, not to be confused with Article 19 of the adopted Regulation, which exempts micro and small enterprises). Following the negotiations, the adopted text addresses them in two recitals (recitals 61 and 62) and Article 22 (European Commission, 2020b, Article 19 and recital 46; European Parliament & Council of the European Union, 2022, Article 22 and recitals 61–62).

The DSA entered into force on 16 November 2022 and became generally applicable on 17 February 2024 (European Parliament & Council of the European Union, 2022, Article 93).

Article 19(2)(b) of the proposal required an entity seeking trusted flagger status not only to be independent from any online platform but also

to represent collective interests. This requirement was contested during the trilogue negotiations because it determined which entities could benefit from the system.

Had the requirement been retained, corporate entities representing only private interests would have been excluded from the regime (Rosati, 2024).

The final text retains independence from any provider of online platforms in Article 22(2)(b) but omits the reference to collective interests, which was deleted at the Council's proposal (Council of the European Union, 2021).

Article 19(1) of the proposal required online platforms to process and decide upon notices from trusted flaggers, submitted through the mechanisms referred to in Article 14 of the proposal, with priority and without delay. It did not limit that priority to notices within the flagger's designated area of expertise (European Commission, 2020b, Article 19(1)). A flagger designated for hate speech could therefore have claimed priority for notices concerning copyright, an area in which it had no recognized expertise.

At the Parliament's suggestion, the adopted text limits priority to notices submitted within the flagger's designated area of expertise (European Parliament, 2022).

Nor did the proposal impose reporting obligations on trusted flaggers. These were added during the trilogue negotiations, also at the Parliament's suggestion (European Commission, 2020b, Article 19; European Parliament, 2022, amendment 249).

Under Article 22(3), trusted flaggers must publish, at least once a year, easily comprehensible and detailed reports on the notices they have submitted and send them to the awarding DSC. The reports must explain the procedures in place to ensure that the trusted flagger maintains its independence and must not contain personal data (European Parliament & Council of the European Union, 2022, Article 22(3)).

The Parliament also proposed a limited but renewable two-year term for trusted flagger status (European Parliament, 2022, amendment 250).

The adopted text contains no such term, and this omission is defensible. The DSA already provides for continuing control: the DSC that awarded the status supervises the trusted flagger and can investigate it, suspend its status or revoke it. A fixed term would simply have layered a periodic re-examination over safeguards that already operate on an ongoing basis (European Parliament & Council of the European Union, 2022, Article 22(6)-(7)).

3.3. Priority Processing and Designated Expertise

In the DSA, the statutory system of trusted flaggers is found in Article 22 and recitals 61 and 62, which have to be read together with the related provisions of the Regulation. Its core is an obligation on online platforms to process and decide upon notices from trusted flaggers, submitted through the Article 16 mechanism, with priority and without undue delay. Article 22 thus complements the general notice-and-action mechanism (European Parliament & Council of the European Union, 2022, Articles 16 and 22).

The obligation applies only to online platforms, a subcategory of hosting services. It does not apply to other hosting services or to mere conduit and caching services. The limitation reflects the public dissemination of content on online platforms and the correspondingly greater impact of illegal content (European Parliament & Council of the European Union, 2022, Articles 3(i) and 22(1)).

Not every online platform is covered. Article 19 exempts online platforms that qualify as micro or small enterprises within the meaning of Recommendation 2003/361/EC from the obligations in this Section, Article 22 included (European Parliament & Council of the European Union, 2022, Article 19(1)).

The exemption in Article 19 is subject to its conditions, including the exception for designated very large online platforms. Article 16 notice-and-action duties apply to hosting services; the size exemption from Article 22 does not remove those duties (European Parliament & Council of the European Union, 2022, Articles 16 and 19(1), (3)).

Article 22(1) requires providers of online platforms to take the necessary technical and organizational measures to ensure priority. Technically, the Article 16 mechanism must allow a trusted flagger to identify itself, and the platform must be able to verify that claim against the list published under Article 22(5). How this is done is left to the platform; Raue and Hofmann mention two options, adapting the notice form or giving trusted flaggers a separate access route such as a dedicated log-in (Raue & Hofmann, 2024). Organizationally, a platform that relies on human review must allocate enough staff for priority notices to be handled ahead of others.

Processing without undue delay does not entail an identical response time for every notice. Recital 62 relates the appropriate speed to the circumstances of the case and the category of illegal content; the quality of a notice also affects the assessment that can be made. Its reference to reviewing most valid hate-speech notifications within 24 hours recalls the Code of Conduct commitment. It does not create a general 24-hour deadline under Article 22 (European Parliament & Council of the European Union, 2022, recital 62).

Article 22 concerns only notices of illegal content within the meaning of Article 3(h). Paragraph 1 does not say so expressly, but three features of the provision point that way. Priority attaches to notices submitted through the Article 16 mechanism, which is confined to illegal content. The expertise required by Article 22(2)(a) relates to detecting, identifying and notifying illegal content. And the annual reports under Article 22(3) must categorise notices by the type of allegedly illegal content notified (Raue & Hofmann, 2024). Article 22 does not, however, prevent platforms from voluntarily prioritising notices from the same entities that concern breaches of their terms and conditions (European Parliament & Council of the European Union, 2022, Articles 3(h), 16 and 22).

For the same reason, the award decision should state the area or areas in which the applicant has shown expertise and competence under Article 22(2)(a). Priority under Article 22(1) is limited to notices within the flagger's 'designated area of expertise', so that area has to be identifiable (Quintais & Schwemer, 2022).

3.4. Eligibility and Public Designation

Trusted flagger status is granted only to entities meeting specific conditions outlined in Article 22(2) of the DSA. Given the substantial impact trusted flaggers can have on moderation of digital content online, the selection of entities entrusted with this power is of paramount importance (Chander, 2023, p. 1079).

Article 22(2) lays down three conditions. The competent Digital Services Coordinator awards the status, on application, to an entity that shows (a) that it has particular expertise and competence for the purposes of detecting, identifying and notifying illegal content; (b) that it is independent from any provider of online platforms; and (c) that it carries out its activities for the purpose of submitting notices diligently, accurately and objectively (European Parliament & Council of the European Union, 2022, Article 22(2)(a)-(c)). All three must be met.

Article 22(2) refers to 'entities', not to natural persons. Recital 61 confirms that the status should be awarded only to entities, not individuals, and adds that the overall number of trusted flaggers should be limited so as not to diminish the added value of the mechanism (European Parliament & Council of the European Union, 2022, recital 61). The recital does not explain why a smaller pool adds value; the most plausible reading is that priority loses its meaning if it is widely shared.

Within that limit, the organizational and legal form of the applicant is irrelevant. Recital 61 refers to public entities, such as the internet referral units of national law enforcement authorities or of Europol, and to non-governmental organizations and private or semi-public bodies, such as

members of the INHOPE network of hotlines. Public authorities may therefore apply, provided they meet the conditions in Article 22(2).

Recital 61 also encourages industry associations representing their members' interests to apply for the status, without prejudice to the right of private entities or individuals to enter into bilateral agreements with providers of online platforms. This qualifies the significance of the deletion of the 'collective interests' requirement discussed in Section 3.2. Even without that requirement, the recital points designation towards bodies that aggregate the interests of several members, such as right-holder associations in intellectual property, rather than towards individual companies. The first designation under the DSA, of the Finnish Copyright Information and Anti-Piracy Centre, fits that pattern. The same sentence expressly preserves bilateral arrangements, anticipating the voluntary programs discussed in Section 4.3 (European Parliament & Council of the European Union, 2022, recital 61).

Article 22(2) also presupposes that applicants are established in the Union, because the status is awarded by the DSC of the Member State in which the applicant is established. That DSC is also responsible for supervising the entity after the award.

The procedure for applications is governed, in principle, by the national administrative law of the awarding DSC. Article 22(8) allows the Commission, after consulting the Board, to issue guidelines to assist providers of online platforms and DSCs in applying paragraphs 2, 6 and 7. The Commission published draft guidelines for consultation on 29 May 2026. They address the award, suspension and revocation of the status, the content of trusted flaggers' reports and the technical measures platforms should adopt to process their notices with priority. Adoption was planned for the second half of 2026 (European Commission, 2026a, 2026b). Although guidelines do not bind DSCs as a matter of law, they are likely to reduce divergence in national award practice.

The concept of establishment is to be interpreted autonomously. By analogy with the case law of the CJEU in a different jurisdictional context, an establishment within the meaning of Article 97(1) of Regulation (EC) No 207/2009 presupposes a 'certain real and stable presence, from which commercial activity is pursued, as manifested by the presence of personnel and material equipment'. In other words, there must be management on site that has the power to conclude transactions and is equipped with the necessary resources to do so. A temporary, short-term presence, such as an exhibition stand, does not constitute an establishment (Court of Justice of the European Union, 2017).

Article 22 does not address reapplication after revocation. Nothing prevents an entity whose status has been revoked from applying again once it

meets the conditions in Article 22(2). Raue and Hofmann suggest that such an applicant should have to show that it has durably remedied the shortcomings that led to revocation, and that a typical waiting period could be set at EU level (Raue & Hofmann, 2024). Guidelines under Article 22(8) would be an appropriate vehicle for such a rule.

The designation model also carries a risk. Denmark (2023) warns of political interference: a government could withhold recognition from independent entities or favor those willing to report content critical of those in power. Article 23(2) does not address this risk, because it targets abusive submissions rather than the selection of flaggers. The main safeguards lie instead in the complete independence required of DSCs under Article 50(2) and in the publicity of designations under Article 22(5) (European Parliament & Council of the European Union, 2022).

4. Accountability and the Limits of Statutory Regulation

4.1. Transparency and Independence

The transparency framework distributes responsibilities among trusted flaggers, the awarding DSCs and the Commission. Each contributes different information needed to scrutinise designation, reporting activity and the continuation of trusted status.

To start with the trusted flaggers, reporting obligation was not suggested by the proposal, however in the final text, reporting responsibilities were imposed on trusted flaggers. Paragraph 3 states that trusted flaggers are obliged to publish and submit to the awarding DSCs easily understandable and detailed reports on their notifying activities at least once a year. Reports shall indicate the number of notices submitted in the reporting period and break them down according to the minimum categories given in points (a), (b) and (c) of paragraph 3 (European Parliament & Council of the European Union, 2022, Article 22(3)).

Meaningful scrutiny of independence requires information about the relationships between a flagger and the platforms whose content it reports. Relevant matters include donations and other funding arrangements, overlapping personnel or governing bodies, and membership, ownership or similar organisational connections. Disclosure of these relationships makes it possible to assess whether the safeguards adopted by a flagger are effective in practice (van de Kerkhof, 2025).

Arun's analysis of epistemic authority examines how platforms use external experts, including trusted flaggers, to inform or legitimise content decisions. Expertise may therefore serve both an informational and a legitimating function. For the present analysis, this suggests that public recognition should not substitute for scrutiny of the relationships through which expertise is exercised. The point is a conceptual contribution to the

independence debate, not a finding that designated flaggers lack independence (Arun, 2026, pp. 1393–1394).

Under Article 22(4), DSCs must communicate to the Commission and the Board the names, addresses and email addresses of the entities to which they have awarded, suspended or revoked the status. The information required is modest (European Parliament & Council of the European Union, 2022, Article 22(4)).

The Commission publishes and updates information on entities whose trusted status has been awarded, suspended or revoked, using the information supplied by the competent DSCs. Accessible, machine-readable publication supports scrutiny of this designation framework (European Parliament & Council of the European Union, 2022, Article 22(5)).

Publication alone may be insufficient for effective oversight. Strowel and De Meyere make a related point: extensive reporting risks overwhelming regulators, whereas giving vetted researchers access may lead to more meaningful scrutiny of moderation systems. Their study deals with disinformation and with the transparency framework in general, not with trusted flaggers. Its relevance lies in the distinction between disclosing information and making that information usable for accountability (Strowel & De Meyere, 2023, pp. 67–68).

The Commission keeps a public list of the entities that DSCs have designated as trusted flaggers (European Commission, n.d.-b). The list grew slowly at first. In May 2024 it contained a single entry: The Copyright Information and Anti-Piracy Centre (CIAPC), designated by Traficom, the Finnish DSC, for 'Intellectual Property (Copyright)' (Traficom, n.d.). By May 2026, more than 70 organizations held the status, and the designated areas had widened to include, among others, financial scams, online harassment and child sexual abuse material (European Commission, 2026b).

For each entity, the list gives its name and contact details, the awarding DSC and the designated area of expertise. The last of these is what makes Article 22(1) workable in practice, since priority applies only to notices falling within that area. What the list does not show is how many notices each flagger sends, how often they lead to action, or what funding relationships might bear on independence. That information must be sought in the flaggers' annual reports under Article 22(3) and in platforms' transparency reports, which are published separately and in different formats. Publication of the list therefore establishes who holds statutory status; it does not by itself make the operation of the system assessable.

4.2. Safeguards against Misuse

One of the important novelties which this system brought is establishing safeguards against misuse resulting in the revocation of the

status of trusted flaggers. Although the status is awarded without a time limit, it remains conditional on general eligible requirements, which means that continued status depends on meeting the criteria prescribed in Article 22(2), subject also to suspension during investigation.

The first and obvious process is initiated by online platforms, when they have gathered information, indicating that trusted flagger has submitted ‘a significant number of insufficiently precise, inaccurate or inadequately substantiated notices’ (Article 22(6)). Communication of the above-mentioned information is an obligation of the online platform, not an option (Quintais & Schwemer, 2022, p. 214; European Parliament & Council of the European Union, 2022, Article 22(6)).

Article 22(6) concerns information acquired through notices submitted under Article 16, including information obtained through internal complaint handling under Article 20(4). It applies to entities awarded statutory status; voluntary partners do not hold a status capable of revocation under Article 22 (European Parliament & Council of the European Union, 2022, Articles 20(4) and 22(6)).

Information indicating possible misuse, as described above, is communicated by online platforms to the DSCs, which awarded the status of the trusted flaggers to the entity concerned, but not to the ‘DSCs of establishment’ or ‘DSCs of destination’. Which means that, for example, if a hypothetical platform established in Ireland and thus under the supervision of the Irish DSC, decides to initiate a revocation procedure against trusted flagger – ‘X’, which is established in Italy and, thus, is awarded the status by the Italian DSC, shall communicate the information discussed above to the Italian DSC, which is the only competent authority to consider the case and issue a decision (European Parliament & Council of the European Union, 2022, Article 22(6)).

The relation between suspension and revocation of the status of trusted flagger according to paras. 6, 7 and the measures of online platforms against misuse under Art.23(2) is not specified. The Digital Services Coordinator alone has the competence for suspension and revocation of the trusted flagger status. Article 23 concerns the suspension of notice processing by a platform, whereas Article 22 concerns suspension or revocation of statutory status. These measures should therefore be distinguished rather than treated as automatically excluding one another (van de Kerkhof, 2025).

The second step following the communication of the information to the DSC is upon its discretion, to evaluate the information and assess whether the information is sufficient and legitimate to proceed. If DSC considers it relevant, it initiates investigation, which shall be carried out without undue delay, and suspends the status of trusted flaggers for that

period. Respective DSC solely decides the case and, following the investigation, if it determines that the trusted flagger no longer meets the eligibility criteria, it revokes the status, but before that an opportunity for the trusted flagger to react to the findings of the investigation and DSC's intention to revoke the status, is guaranteed (European Parliament & Council of the European Union, 2022, Article 22(6)–(7)).

Another path to revocation can be initiated by the respective DSCs. Important to take into account is that only DSC which awarded the status to trusted flagger has legal power to take decisions. DSC may decide to start investigation either on its own discretion, or on the basis of information provided to them by third parties, who may be user who have been affected by unreliable notices from a trusted flagger. Nothing in the provision requires from DSC or third parties to submit the same/similar information what is required from online platforms discussed above, however, the information must be legitimate, potentially proving 'that the entity no longer meets the conditions set out in paragraph 2' of article 22. Opportunity for trusted flaggers in question to react on decisions of DSC is guaranteed in this scenario as well. In this scenario public reports of trusted flaggers may be used as a tool to initiate proceedings following paragraph 7 of article 22 (European Parliament & Council of the European Union, 2022, Article 22(7)).

As a last point, The criteria of Art.23(3) can be used accordingly to assess whether there is a 'significant number' (French: un nombre significatif) of unreliable notices: The absolute numbers of unreliable notices or their relative proportion within a given time frame, the gravity of the misuses and its consequences as well as, if applicable, the intentionality of the false notice. However, in the case of Art.22, a lower threshold could be justified so that the status can be withdrawn even in the case of fewer unreliable notices. This is because the preferential system for trusted flaggers is based on the fact that they notify with above-average diligence, accuracy, and objectivity (Raue & Hofmann, 2024).

4.3. Coexistence with Voluntary Trusted Flaggers

Since the first initiation of the program, statutory formalization of the system of trusted flaggers happened through the DSA, imposing specific legal requirements, reporting and transparency obligations to them, however, the law left room for voluntary system of trusted flaggers, without institutionalizing the whole system.

Following the recital 61, DSA creates possibility to disregard the requirements prescribed by article 22 to obtain the "privilege" of trusted flaggers, enabling private individuals and entities to enter into bilateral agreement with the providers of online platforms, where requirements are set

by online platforms themselves. Furthermore, online platforms may treat self-appointed trusted flaggers ‘in a similar manner’ (European Parliament & Council of the European Union, 2022, recital 61; Rosati, 2024).

Voluntary cooperation may cover infringements of platform terms as well as illegal content. Article 22 priority, by contrast, attaches to qualifying notices of illegal content submitted through the DSA notice-and-action mechanism. Platforms may maintain separate reporting arrangements for material contrary to their terms and may cooperate with entities outside the statutory trusted flagger framework. The continued existence of these arrangements is therefore compatible with Article 22 (European Parliament & Council of the European Union, 2022, recital 61; Rosati, 2024).

The voluntary system, in contrast to the formalized trusted flaggers, has a number of issues, including the following:

- No Article 22-specific clear requirements for eligibility standard, which will be solely decided by platforms;
- No Article 22-specific obligations regarding publishing reports on submitted notices and details thereof;
- No Article 22-specific transparency measures, to ensure publicity of voluntary trusted flaggers.

Article 23 of the DSA addresses misuse by both content providers and those submitting notices or complaints. After a prior warning, platforms must suspend their services for a reasonable period to recipients who frequently provide manifestly illegal content. The same requirement applies to the processing of frequently submitted, manifestly unfounded notices or complaints (European Parliament & Council of the European Union, 2022, Article 23(1)–(2)).

Voluntary cooperation with trusted flaggers predates the DSA and was encouraged by Recommendation (EU) 2018/334. Such arrangements may continue alongside the statutory system, but they fall outside Article 22’s designation and revocation framework. Article 23 partly addresses this gap because its safeguards against abusive submissions also apply to participants in voluntary arrangements (Quintais & Schwemer, 2022).

Article 23 is not the only provision that reaches voluntary arrangements, but the others do so indirectly. Notices submitted by voluntary partners through the Article 16 mechanism remain notices under that provision, so platforms must assess them and, where they restrict content, provide a statement of reasons under Article 17. Article 15(1)(b) shows how limited that reach is. Providers must report how many notices they received, broken down by type of alleged illegal content, and must state separately how many came from trusted flaggers. That separate figure, however, covers only entities designated under Article 22. Notices from voluntary partners

disappear into the general total, and a reader of the report cannot tell them apart.

The systemic-risk framework that applies to very large online platforms and search engines goes further. When these services carry out risk assessments under Article 34(2), they must consider, among other factors, how their content moderation systems are designed. Article 35(1)(g) then names cooperation with trusted flaggers as one possible mitigation measure, although it does so by reference to Article 22. Both sets of obligations, together with any commitments under codes of conduct, are subject to independent audit under Article 37. The Code of Conduct on Countering Illegal Hate Speech Online+, integrated into the DSA framework in January 2025, shows how this works in practice: very large platforms that have signed it may rely on it to show that they mitigate the risk of illegal content being disseminated, and their commitments are assessed in the annual audits (European Commission, 2025).

The difficulty is that all of these mechanisms look at the platform, not at the flagger. They can reveal whether a platform's moderation system is adequate overall. They do not, however, oblige the platform to say which organizations receive priority outside Article 22, on what criteria or with what results, and no public authority is given the power to suspend or revoke the privileges of a voluntary partner. Nor is this a marginal issue. The Commission-funded mapping found 47 voluntary schemes, 31 of them run by online platforms, with intellectual property infringement among their principal areas (Pozzo et al., 2026). The contrast is sharpest in intellectual property, where right holders can choose between statutory designation and a bilateral arrangement.

5. Discussion

The DSA has institutionalized trusted flagging, but only up to a point. Designated trusted flaggers are regulated under Article 22, while voluntary programs are allowed to carry on beside them. Designation and reporting requirements therefore cover only part of the trusted flagger ecosystem, and arrangements that perform much the same notification function end up being overseen in quite different ways (Davitadze, 2024).

This is not to say that statutory recognition has changed little. The status is now awarded by a Digital Services Coordinator, not by an individual platform, and qualifying notices must be given priority on every platform covered by Article 22. An entity no longer has to negotiate priority with each platform in turn. The price of these advantages is a set of eligibility and transparency requirements, which may be administratively burdensome for applicants. In short, the DSA keeps the established practice

of expert notification but changes the footing on which designated entities take part in it.

What remains problematic is the relationship between the statutory and voluntary programs. Both provide platforms with expert notices, and both can lead to priority treatment. Only one of them, however, involves public designation, reporting at the level of the flagger and the possibility of revocation by a public authority. The platform-level obligations discussed in Section 4.3 make the gap smaller, but they do not close it.

Three measures could address the gap within the existing regulation. The first concerns transparency reporting: platforms' reports under Articles 15 and 24 could list notices from voluntary priority programs as a separate category, next to those from designated trusted flaggers, and the reporting templates adopted under Article 15(3) would be the natural place to do this. The second concerns the programs themselves. Platforms that grant priority outside Article 22 could be expected to publish the eligibility criteria for their programs and the names of the participating organizations, with justified exceptions for safety-sensitive partners such as hotlines and law enforcement referral units. Codes of conduct under Article 45 could set that expectation. The third concerns very large platforms, which could be expected to address voluntary priority programs expressly in their Article 34 risk assessments; this would also bring the programs within the Article 37 audit.

None of this would turn voluntary partners into designated trusted flaggers. What it would do is make visible the basis on which some notifiers are treated preferentially, and without that, neither model can be properly scrutinized. Public recognition and priority processing can help trusted flaggers in their work. In the end, though, what they contribute depends on how reliable their notices are and on how carefully platforms then assess them.

Conclusion

To return to the question asked at the outset: yes, but with a qualification. Where the two regimes overlap, that is, in the priority handling of notices alleging illegal content, a notifier can obtain through a bilateral arrangement a priority comparable to the one Article 22 grants only in return for public designation, reporting and the possibility of revocation. To that extent, coexistence weakens the accountability that the provision was meant to secure. Voluntary programs dealing with breaches of platforms' terms and conditions are a different matter. They fall outside the purpose of Article 22, and the same concern does not arise.

Under the DSA, the legal position of trusted flaggers has changed, but not every trusted flagger program has been brought within the same

framework. Public designation and mandatory priority set entities recognized under Article 22 apart from participants in voluntary platform arrangements. In both cases the underlying activity is expert notification; what differs are the rules on who may take part and how they are held to account.

This difference is the main limitation identified in the article. Voluntary programs operate alongside the statutory system without having to meet Article 22's designation and reporting requirements. The DSA has thus institutionalized only part of the trusted flagger ecosystem and has left open how the two models relate to each other (Davitadze, 2024).

A more complete framework would extend to voluntary programs the minimum conditions that make privileged notification accountable: criteria that are published, participants who can be identified, and reporting that distinguishes their notices from others. Much of this could be achieved without amending the Regulation, through separate reporting of voluntary priority notices, public eligibility criteria and the inclusion of such programs in systemic-risk assessments. Whichever model applies, one point should not be lost. Priority processing is not a determination of illegality: the platform still has to assess the notice, and the identity of the sender cannot take the place of that assessment.

Conflict of Interest: The authors reported no conflict of interest.

Data Availability: All data are included in the content of the paper.

Funding Statement: The authors did not obtain any funding for this research.

References:

1. Appelman, N., & Leerssen, P. (2022). On “trusted” flaggers. *Yale Journal of Law & Technology*, 24, 452–475.
2. Arun, C. (2026). Digital platforms and epistemic authority. *Texas Law Review*, 104(7), 1385–1416.
3. Castets-Renard, C. (2020). Algorithmic content moderation on social media in EU law: Illusion of perfect enforcement. *University of Illinois Journal of Law, Technology & Policy*, 2020(2), 283–324.
4. Chander, A. (2023). When the Digital Services Act goes global. *Berkeley Technology Law Journal*, 38(3), 1067–1088. <https://lawcat.berkeley.edu/record/1288003?v=pdf>
5. Council of the European Union. (2021, November 18). Proposal for a regulation on a single market for digital services: General approach (13203/21).
6. Court of Justice of the European Union. (2010). Google France and Google (Joined Cases C-236/08 to C-238/08). ECLI:EU:C:2010:159.

7. Court of Justice of the European Union. (2011). *L'Oréal and Others v eBay and Others* (Case C-324/09). ECLI:EU:C:2011:474.
8. Court of Justice of the European Union. (2017). *Hummel Holding* (Case C-617/15). ECLI:EU:C:2017:390.
9. Court of Justice of the European Union. (2021). *YouTube and Cyando* (Joined Cases C-682/18 and C-683/18). ECLI:EU:C:2021:503.
10. Davitadze, M. (2024). *From voluntary to institutionalized: A comprehensive legal examination of trusted flaggers. To what extent will the proposed "Trusted Flaggers" system fall short in attaining its intended goals?* [Master's thesis, Stockholm University].
11. de Streel, A., & Ledger, M. (2021). Regulating the moderation of illegal online content. In M. Cappello (Ed.), *Unravelling the Digital Services Act package* (pp. 23–42). European Audiovisual Observatory.
12. Denemark, J. (2023). Strengthening the European Union by regulating the Digital Single Market. *Acta Universitatis Carolinae Iuridica*, 69(2), 107–123. <https://doi.org/10.14712/23366478.2023.18>
13. European Commission. (2016). Code of conduct on countering illegal hate speech online. https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en
14. European Commission. (2017). Tackling illegal content online: Towards an enhanced responsibility of online platforms (COM(2017) 555 final).
15. European Commission. (2018). Recommendation (EU) 2018/334 on measures to effectively tackle illegal content online. *Official Journal of the European Union*, L 63, 50–61.
16. European Commission. (2019). Information note: Progress on combating hate speech online through the EU Code of Conduct 2016–2019.
17. European Commission. (2020a). Impact assessment report accompanying the proposal for a Digital Services Act (SWD(2020) 348 final, Parts 1 and 2).
18. European Commission. (2020b). Proposal for a regulation on a single market for digital services and amending Directive 2000/31/EC (COM(2020) 825 final).
19. European Commission. (2022). Joint statement by IT companies and trusted flagger organisations to enhance cooperation [Annex to the EU Code of Conduct on countering illegal hate speech online].

20. European Commission. (2025, January 20). Commission welcomes the integration of the revised Code of Conduct on Countering Illegal Hate Speech Online into the Digital Services Act. <https://digital-strategy.ec.europa.eu/en/news/commission-welcomes-integration-revised-code-conduct-countering-illegal-hate-speech-online-digital>
21. European Commission. (2026a). Draft Commission guidelines on trusted flaggers under Article 22 of Regulation (EU) 2022/2065 [Consultation draft]. <https://digital-strategy.ec.europa.eu/en/library/draft-commission-guidelines-trusted-flaggers>
22. European Commission. (2026b, May 29). Commission seeks feedback on draft trusted flaggers guidelines under the Digital Services Act. <https://digital-strategy.ec.europa.eu/en/news/commission-seeks-feedback-draft-trusted-flaggers-guidelines-under-digital-services-act>
23. European Commission. (n.d.-a). Digital Services Coordinators. Retrieved October 4, 2026, from <https://digital-strategy.ec.europa.eu/en/policies/dsa-dscs>
24. European Commission. (n.d.-b). Trusted flaggers under the Digital Services Act (DSA). Retrieved October 4, 2026, from <https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa>
25. European Parliament & Council of the European Union. (2000). Directive 2000/31/EC on electronic commerce. Official Journal of the European Communities, L 178, 1–16.
26. European Parliament & Council of the European Union. (2022). Regulation (EU) 2022/2065 on a single market for digital services (Digital Services Act). Official Journal of the European Union, L 277, 1–102.
27. European Parliament. (2022, January 20). Amendments on the proposal for a regulation on a single market for digital services (P9_TA(2022)0014).
28. Frazier, K. (2024). The past, present, and future of platform governance. *Loyola University Chicago Journal of Regulatory Compliance*, 12, 20–89.
29. Frosio, G. (2018). Why keep a dog and bark yourself? From intermediary liability to responsibility. *International Journal of Law and Information Technology*, 26(1), 1–33. <https://doi.org/10.1093/ijlit/eax021>
30. Frosio, G., & Geiger, C. (2023). Taking fundamental rights seriously in the Digital Services Act's platform liability regime. *European Law Journal*, 29(1–2), 31–77. <https://onlinelibrary.wiley.com/doi/10.1111/eulj.12475>

31. Grimmelmann, J., & Zhang, P. (2023). An economic model of online intermediary liability. *Berkeley Technology Law Journal*, 38(3), 1011–1066. <https://lawcat.berkeley.edu/record/1288000>
32. Hajnal, Z. (2023). The new liability forms of online platforms in the new European digital legal framework from the consumers' perspective. *Acta Universitatis Sapientiae, Legal Studies*, 12(2), 19–35. <https://doi.org/10.47745/AUSLEG.2023.12.2.02>
33. Husovec, M. (2023). Rising above liability: The Digital Services Act as a blueprint for the second generation of global Internet rules. *Berkeley Technology Law Journal*, 38(3), 883–920. <https://doi.org/10.15779/Z38M902431>
34. Husovec, M. (2024). Principles of the Digital Services Act. Oxford University Press. <https://doi.org/10.1093/law-ocl/9780192882455.001.0001>
35. Jaursch, J. (2023). Platform oversight: Here is what a strong Digital Services Coordinator should look like. In J. van Hoboken, J. P. Quintais, N. Appelman, R. Fahy, I. Buri, & M. Straub (Eds.), Putting the DSA into practice: Enforcement, access to justice, and global implications (pp. 91–106). Verfassungsbooks.
36. Peukert, A., Husovec, M., Kretschmer, M., Mezei, P., & Quintais, J. P. (2022). European Copyright Society – Comment on copyright and the Digital Services Act proposal. *IIC – International Review of Intellectual Property and Competition Law*, 53(3), 358–376. <https://doi.org/10.1007/s40319-022-01154-1>
37. Pozzo, G., Sadauskaitė, A., & Teplyshova, A. (2026). Study for supporting the implementation of the trusted flaggers mechanism under the Digital Services Act. Publications Office of the European Union. <https://doi.org/10.2759/5727827>
38. Quintais, J. P., & Schwemer, S. F. (2022). The interplay between the Digital Services Act and sector regulation: How special is copyright? *European Journal of Risk Regulation*, 13(2), 191–217. <https://doi.org/10.1017/err.2022.1>
39. Raue, B., & Hofmann, F. (Eds.). (2024). Digital Services Act: Article-by-article commentary. C. H. Beck, Hart Publishing and Nomos.
40. Rosati, E. (2023). Copyright and the Court of Justice of the European Union (2nd ed.). Oxford University Press. <https://doi.org/10.1093/law/9780198885580.001.0001>
41. Rosati, E. (2024, February 22). The DSA's trusted flaggers: Revolution, evolution, or mere gattopardismo? Verfassungsblog. <https://doi.org/10.59704/37e9e89d5812f78a>

42. Schwemer, S. F. (2019). Trusted notifiers and the privatization of online enforcement. *Computer Law & Security Review*, 35(6), Article 105339. <https://doi.org/10.1016/j.clsr.2019.105339>
43. Shamatava, I. (2026a). Europeanization of intellectual property enforcement beyond EU membership: The Georgian experience after the Association Agreement [Preprint]. Zenodo. <https://doi.org/10.5281/zenodo.21601497>
44. Shamatava, I. (2026b). Georgia's intellectual property law in an evolving European legal framework: Legislative reform and the challenge of sustained alignment. *Health Policy, Economics and Sociology*, 10. <https://doi.org/10.52340/healthecosoc.2026.10.03.06>
45. Strowel, A., & De Meyere, J. (2023). The Digital Services Act: Transparency as an efficient tool to curb the spread of disinformation on online platforms? *JIPITEC*, 14(1), 66–83.
46. Traficom. (n.d.). Trusted flaggers. Retrieved October 4, 2026, from <https://www.traficom.fi/en/data-economy-and-data-intermediation/trusted-flaggers>
47. United States Congress. (1998). Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (codified in relevant part at 17 U.S.C. § 512). <https://www.law.cornell.edu/uscode/text/17/512>
48. Urban, J. M., Karaganis, J., & Schofield, B. L. (2017). Notice and takedown in everyday practice (Version 2, updated March 2017). University of California, Berkeley, School of Law. <https://doi.org/10.2139/ssrn.2755628>
49. van Benthem, T. (2018). Social media actors in the fight against terrorism: Technology and its impact on human rights. *Cambridge International Law Journal*, 7(2), 284–300.
50. van de Kerkhof, J. (2025). Article 22 Digital Services Act: Building trust with trusted flaggers. *Internet Policy Review*, 14(1), 1–26. <https://doi.org/10.14763/2025.1.1828>
51. Wilman, F. (2023). Between preservation and clarification: The evolution of the DSA's liability rules in light of the CJEU's case law. In J. van Hoboken, J. P. Quintais, N. Appelmann, R. Fahy, I. Buri, & M. Straub (Eds.), *Putting the DSA into practice: Enforcement, access to justice, and global implications* (pp. 35–50). *Verfassungsbooks*.