Computer & Communications Industry Association
Tech Advocacy Since 1972

CCIA's Position Paper on the EU Digital Services Act

Introduction

The Computer & Communications Industry Association (CCIA Europe) welcomes the ambition of the Digital Services Act (DSA) proposal.[1] We fully support the objective to increase digital innovation, online safety, and fundamental rights protection in the European Union (EU) single market.

Intermediary service providers are committed to addressing illegal content, products, services, and activities online. While services offer wide-ranging economic and social benefits, technologies can be misused by some users.[2] Intermediary services have responded to this problem with a range of initiatives appropriate to the services they provide.[3] Among others, they have set up programmes to prevent the dissemination of illegal hate speech and the sale of counterfeits.[4]

As the European Parliament and the Council seek to define their positions on the DSA and reach a common agreement, CCIA offers the following comments.

1. Strengthen the EU single market

Over the past two decades, the EU eCommerce Directive (eCD) has been the foundation on which Europe's digital economy has developed.[5] Today, there are more than 10,000 high-growth online platforms in Europe,[6] an increase of more than 40% since 2018.[7] Many European platforms have become household names across the EU and some globally.[8]

Digital service providers reduce barriers to growth for small and medium-sized enterprises (SMEs), enabling them to immediately access infrastructure and customers without having to make large up-front investments.[9] This support for cross-border trade happens both within the EU and beyond, simplifying exports of goods and services by European SMEs, critical for making trade-based growth available to many European businesses.

The Internet and digital services have evolved over the last 20 years and so have everyone's expectations. We welcome the DSA's ambition to harmonise the interpretation of the eCD's section on intermediary service providers' liability.

An EU-wide DSA ruleset is essential to prevent a patchwork of national initiatives on intermediary liability and content regulation. Some EU Member States have already developed or are working on national rules (e.g., Austria,[10] France,[11] Germany,[12] and Hungary[13]). While national concerns are understandable, action at the EU level would be the most effective. A harmonised EU framework would also support startups to scale up in one EU single market.

CCIA calls upon the European Parliament and the Member States' governments to focus their efforts on delivering the DSA, rather than pursuing national legislative initiatives.

2. Scope

2.1. Set a horizontal and principle-based approach

The Digital Services Act seeks to introduce "a horizontal framework for all categories of content, products, services and activities on intermediary services".[14] We welcome this approach. However,

many questions remain open and several concepts should be clarified, e.g., "illegal content" (Art. 2(g)),[15] "online platform" (Art. 2(h)), and "actual knowledge" (Art. 5).

While the DSA does not aim to set sector-specific requirements, some provisions target specific sectors or types of intermediaries. For instance, some provisions might be appropriate for certain service providers but would be unworkable for other intermediaries. For example, Article 22 on the traceability of traders appears to be targeted only at online marketplaces that allow the consumer to conclude a distance contract with the trader on the online platform, and the article should be clarified as such.

The DSA rules should be horizontal and principle-based to stand the test of time. This DSA foundation can then, later, be complemented with more targeted and sector-specific measures, legislative and non-legislative, to tackle specific concerns. The DSA should be general enough to create a workable framework for the actors involved by avoiding over-prescriptive obligations that would require specific operational capabilities to make the legislation effective.

2.2. Be channel-neutral

The draft proposal sets many requirements on digital service providers, which wouldn't apply to offline service providers. For example, shouldn't the DSA data sharing requirements applying to online marketplaces also apply to retail shops selling third-party products? Different rules for so-called online and offline companies would slow down Europe's digital transformation, disadvantage online companies, and effectively decrease the level of protection for "offline" consumers.

2.3. Tackle bad behaviour, not size

The DSA should tackle bad players and user behaviours regardless of the platform's size and country of origin.

Having a specific regime for "very large online platforms" (VLOPs)[16] with additional obligations encourages rogue players to proliferate among smaller services that are subject to fewer requirements. For instance, terrorists from the Islamic State of Iraq and Syria (ISIS) switched to less visible platforms, like the social media platform Koonekti,[17] which is part of what prompted the EU to extend the terrorist content online regulation to hosting service providers of all sizes.[18]

If the EU plans to increase online safety and trust, the DSA should consist of proportionate and principle-based rules applicable to all intermediary service providers.[19]

Furthermore, a threshold discourages European digital services from becoming "very large" to avoid the administrative burdens. Consequently, the proposal's approach could inadvertently disincentivise competition by increasing the costs of growing beyond a particular size. Setting a threshold would also have adverse effects on business users and consumers, as customers would fragment across a larger number of platforms, increasing the administrative burden and reducing scale and scope efficiencies.[20]

2.4. Focus on illegal content, products, services, and activities disseminated to the public

The DSA should focus on the fight against illegal content, products, services, and activities on intermediary services. The European Commission has explicitly stated that it does not purport to define what illegal content is. This remains a matter for applicable national and EU law. However, when referring to illegal content in Article 2(g), the scope should be narrowed down by removing the "reference to an [illegal] activity," which could lead to excessive takedowns.[21]

'Illegal' and 'lawful but harmful' content should be treated under different instruments. 'Lawful but harmful' content cannot be treated as 'illegal' content without risking infringement of essential rights, such as freedom of expression and access to information. Any initiative should build on existing efforts (e.g., EU Code of Practice on Disinformation, Memorandum of Understanding on the sale of counterfeit goods online).

Clearer definitions or the introduction of caveats are needed to enable legal certainty and predictability over the classification of different intermediary services under the DSA. It appears that cloud infrastructure services could be considered to fall under the category of online platform or VLOP. However, such services don't have the technical ability to monitor or moderate the content they store on behalf of customers.[22] Moreover, in a business-to-business context, cloud providers' ability to access customers' content is limited by privacy obligations reflected in customer contracts. This has already been recognised in EU legislation, including the terrorist content regulation, which explicitly excludes certain cloud services and other Internet infrastructure services from its scope.[23] To be consistent with existing European laws, we suggest clarifying that the DSA targets illegal content, products, services, and activities on intermediary services, which store and disseminate to the public information and material provided by a recipient of the service at his or her request.

3. Liability Regime and Due Diligence

3.1. Develop a harmonised approach to notice-and-action (Art. 14)

CCIA supports the DSA proposal's harmonised approach of the 'notice-and-action' mechanism. More clarifications are needed in certain places, particularly on the concept of 'actual knowledge' and in Article 14.3, which could be read to imply that fulfilling all notice formalities automatically gives rise to knowledge. Lawmakers should remove any doubt by clarifying, in Article 14.3, that 'actual knowledge' is triggered when the notification requirements have been fulfilled and treated by an individual from the hosting service provider for the specific illegality it alleges.

The requirements in Art. 14.2 should be technology-neutral. For example, provision (c)[24] does not take into account that the users could be logged into the app and that an in-app communication channel may be a more efficient way to communicate with the hosting service provider rather than via email.

3.2. Adopt an inclusive scheme to appoint 'trusted flaggers' (Art. 19)

Online platforms are open to working with independent 'trusted flaggers'. However, additional safeguards and clarifications are needed on how that status is granted and revoked.[25] The possibility for 'trusted flaggers' to notify infringing content, products, activities, or services should be based on their area of expertise and be specific to their jurisdiction.

'Trusted flaggers' would have an influential role in how intermediaries moderate content, products, services, and activities. It is, therefore, appropriate to involve online platforms, allowing them to provide input on the process and decision to grant or revoke the status of 'trusted flaggers'. Trust should be earned and regularly evaluated.

Expectations of online platforms and their management of 'trusted flaggers' must be proportional to the resources at their disposal. For example, small and medium-sized platforms should have the possibility to set a dedicated email address for 'trusted flaggers' to satisfy the prioritisation requirements.

3.3. Set an effective framework for the traceability of traders (Art. 22)

While the DSA aims to be a horizontal regulation, the provision on the traceability of traders, also known as 'know your business customer' (KYBC), seems to only apply to certain kinds of online platforms that allow "consumers to conclude distance contracts with traders."[26] However, this characterisation could be broadly interpreted, causing legal uncertainty. If EU policy-makers aim to apply this provision to online marketplaces, they must clarify the scope of this provision and exclude other online platforms, including those selling goods as a "purely ancillary feature" (e.g., ticketing services).

The requirements listed to verify the identity of the trader should be proportionate to the objective. Art. 22.1(d)[27] requires an excessive burden as an "economic operator" can be different for each of the products sold by any trader, meaning that the required paperwork may not be available to the trader nor the marketplace.

Likewise, clarifications are needed on the concepts of (i) "reasonable efforts" expected from platforms to assess the information shared by the traders, and (ii) "excessive or costly online fact-finding exercises" required by platforms to verify the information given by the traders.

Overall, the KYBC requirements should be aligned with the obligations set in existing EU legislation, such as the fifth anti-money laundering directive,[28] the transfer of funds regulation,[29] and the seventh revision of the administrative cooperation directive[30]. Where a payment processor is used by the service, confirmation from that service that certain data elements have already been checked by them should satisfy this requirement on the digital service. The verification process shouldn't be a barrier preventing access to digital services for small businesses, and it should not result in potential liability. EU policy-makers should encourage Member States to make their corporate registries electronic, uniform, and ready for real-time information requests.

3.4. Extend the scope of voluntary own-initiative investigations (Art. 6)

CCIA welcomes the provision allowing intermediaries to take voluntary own-initiative investigations without being penalised for their good faith efforts. Such measures will increase trust online as intermediaries will be empowered to more effectively tackle illegal content, products, activities, and services. To further incentivise online trust and safety, the provision should clarify that it also covers voluntary own-initiative investigations or other actions aimed at enforcing the intermediaries' terms and conditions.

3.5. Maintain the ban on general monitoring (Art. 7)

While there is a consensus on keeping the ban on general monitoring, CCIA is concerned that regulators could later impose monitoring or 'stay-down' obligations as part of their broad oversight powers, for example, through their authority to set VLOPs' risk mitigation measures. Academics have highlighted that the prohibition on general monitoring is under attack due to an inaccurate interpretation of what 'specific monitoring' is vs. 'general monitoring'.[31] The DSA should make clear that regulators do not have the authority to include monitoring or 'stay-down' requirements as part of risk mitigation remedies.

3.6. Ensure effective redress (Art. 15, Art. 17, Art. 18 and Art. 20)

Platforms invest significant resources into internal complaint-handling systems. These systems are tailored to be cost- and time-efficient for both parties. The DSA provisions on the statement of reasons,

complaint handling, out-of-court redress mechanism, and user suspension are not sufficient to ensure that bad actors do not take advantage of them. These articles do not scale to the millions of decisions online platforms make, and they open up too many potential avenues for abuse.

For example, bad actors could use the public compendium with statements of reasons as a guide to getting around a company's terms of service, or could use out-of-court redress mechanisms to arbitrate every content removal at a company's expense, slowing down the process for legitimate seekers of redress. Limits in automation for complaint handling could also hinder services' efforts to deal with scaled abuse, such as spam.

We urge policy-makers to consider carving out cases where a statement of reasons of such detail may not be appropriate (e.g., spam or for child abuse content) to avoid interfering with potential law enforcement action. Services should also be able to set their own rules for suspending users, and certainly should not be put in a position to evaluate the "intention" of potential abusers, an assessment that online platforms are not appropriately placed to investigate or judge.

3.7. Ensure online rights when requesting notifications of suspicions of offences (Art. 21)

When it comes to the "notification of suspicions of criminal offences", the DSA improperly shifts the function of law enforcement investigation from the government to private actors. This provision should be aligned with the language used and safeguards included in the other EU laws, such as the terrorist content online regulation.[32] This would ensure the DSA reflects Europe's strong tradition of protecting privacy as a fundamental right.

4. Transparency

4.1. Be achievable and proportionate (Art. 13, Art. 23, Art. 29 and Art. 33)

Digital intermediary services provide, where appropriate, meaningful transparency on their content moderation practices.[33] The DSA proposal, however, seeks more transparency from digital intermediaries. While some transparency requirements might be useful, EU policy-makers should find the appropriate equilibrium between transparency, the protection against rogue players' attempts to game the system, and the protection of operators' trade secrets. Any new requirements must be achievable, proportionate to known risks, and provide real added value taking due account of their target audience. The requirement should be consistent with other EU law requirements, such as the regulation on promoting fairness and transparency for business users of online intermediary services.[34]

The added value of reporting requirements remains unclear, and the corresponding requirements appear therefore disproportionate, especially when the information collected (e.g., average monthly active recipients) has a pure commercial relevance and it is not connected with any significant public interest.

4.2. Clarify data access

4.2.1. National authorities' investigatory powers (Art. 31, Art. 38, Art. 41, Art. 52)

Additional safeguards are required regarding competent authorities and "Digital Services Coordinators"' (DSCs) access to data. For instance, their ability to require "the data necessary to assess the risks and possible harms brought about by the platform's systems" could be broadly interpreted, and therefore disproportionate (Recital 64).

We recommend basing data access obligations on specific requests from the relevant auditors and national or European authorities. These should be subject to judicial oversight given the material's sensitivity from both commercial confidentiality and privacy perspectives. Given the basis of the DSA, much of the data requested will relate to third-party individuals and businesses. Furthermore, specifying the tasks and objectives of the competent authorities and DSCs may support the proportionate exercise of investigatory powers.

4.2.2. European Commission's monitoring actions (Art. 57)

The European Commission's access to databases and algorithms lacks safeguards and legal clarity, which is of heightened importance given that the provision relates to highly commercially sensitive information. Providing explanations over databases and algorithms in response to information requests by the Commission would be more proportionate than granting direct access. Such information requests should only occur in the context of a non-compliance investigation.

4.2.3. Vetted researchers (Art. 31)

The current proposal grants vetted researchers access to very sensitive information. It is critical to further frame this access by including safeguards around confidentiality, the scope and nature of what data may be requested, the purposes for which the data may be used, and how that data may be accessed. The processes and criteria to obtain the 'vetted researcher' status should also be strengthened, for example, by including transparency on the funding that researchers may receive for their academic projects, and by giving VLOPs the right to appeal the vetting of a particular researcher. Further, given the lack of any corresponding obligation on offline services, this provision's conception needs careful re-examination.

5. Online advertising (Art. 24, Art. 30 and Art. 36)

Overall, more nuance should be brought to the debate around how online advertising is treated in the DSA. Several possibilities could be considered, such as differentiating between political and commercial advertising or setting up verticals on some issue-based advertising. The associated risk varies depending on the specific business model and/or on the different advertising types. Introducing common transparency obligations for all the online platforms running ads does not consider any of these differences. It would impose disproportionate requirements for some players.

A repository requirement for VLOPs to maintain vast databases of advertisements of everyday products without any distinctive proportional criteria creates even more inconsistencies with the offline ads market. More clarity would also be needed vis-à-vis the repository's operational obligations; e.g., regarding disapproved ads, or how sensitive business-rules and ads parameters should be treated to preserve fair competition.

6. Enforcement

6.1. Keep the country of origin, essential for the single market (Art. 8 and Art. 9)

The 'country of origin principle' remains key to the creation of an EU single market. It is essential for removing unnecessary administrative burdens for small companies that seek to scale up in one EU, rather than 27 national markets.[35]

The DSA proposal should be aligned with the cross-border cooperation approach considered under the regulation preventing the dissemination of terrorist content online[36] and the eEvidence regulation[37]. A "Digital Services Coordinator of destination" (DSCoD) should only be able to take action against illegal content considered as manifestly illegal in its jurisdiction and in the jurisdiction of the "Digital Services Coordinator of establishment" (DSCoE). The DSCoD should also be required to notify the DSCoE, as the latter should be granted the possibility to contest the DSCoD's request within 24 hours. The order's territorial scope should "not exceed what is strictly necessary to achieve its objective".[38]

Where an intermediary service provider has reasonable grounds to believe that the order to take action against illegal content manifestly and seriously breaches the fundamental rights and freedoms set out in the EU Charter of Fundamental Rights, it should be able to request a review by the DSCoE of the issued request from the DSCoD.

To develop well-functioning, cross-border cooperation will require more clarification about who can request what information, how that information can be sought, and how that information will be provided. For instance, the obligation to specify the "moment when the action was taken" would be operationally burdensome.[39] Intermediaries are asked to act, without undue delay, against illegal content and to inform the authority of their action. An alternative could be to ask intermediaries to share the email response timestamp, which closely follows when action was taken.

6.2. Set a simple and clear framework

We welcome strengthened cooperation between the Member States. However, to ensure legal certainty for national authorities, intermediaries, and users, more precision is needed on the purpose of the cooperation; the processes, mission statements, and areas covered by the different authorities; and under which circumstances.

We welcome DSCs' position as the main point of contact as it facilitates the processes for companies, especially SMEs. We would nevertheless invite policy-makers to clarify the competences of the DSCs and the processes for cooperation (e.g., joint investigations).

The DSA requires the Member States to designate competent authorities with appropriate expertise across the range of online services (Art. 38). Suppose a Digital Services Coordinator has an area of expertise (e.g., audio-visual). In that case, it might be difficult for it to treat other kinds of services offered by intermediaries (e.g., collaborative economy or online marketplace services). Digital intermediary services should have clarity that they do not face legal uncertainty or multiple jeopardy through the layering of involvement of other DSCs, the Board, and the European Commission in the proposed structure.

6.3. Adopt proportionate penalties and fines (Art. 42 and Art. 59)

The penalties and fines for DSA breaches should be proportionate to the risks involved. We believe that a fine should only be considered for systematic violations of a specific DSA provision.

More clarity should be given on the rationale of the penalty figures and how they would be calculated by the Member States or the European Commission. A more harmonised approach would promote consistency across the Member States.

6.4. Use effectively delegated acts (Art. 69)

There are many critical provisions of the DSA that are far too important and will have far too significant an impact on the entire proposal for these to be left to delegated acts. For example, the DSA proposal mentions that the criteria to define VLOPs (Art. 25) and the framework for VLOPs' data sharing (Art. 31.5) will be determined in delegated acts. Nevertheless, it is essential for an intermediary service provider that might be considered as a VLOP to know how the 45 million recipients of the service will be calculated. Complying with the DSA VLOP provisions would entail a high cost in terms of resources, time, and money.

6.5. Allocate a realistic 'entry into force' period (Art. 74)

The new obligations will require substantial changes from digital intermediaries, as well as from national authorities. To ensure a well-informed, planned, and effective execution, the implementation period should be extended to 24 months, as there is a limit to what industry can do in the suggested three-month period.

Conclusion

CCIA believes the DSA to be an opportunity to create a better functioning EU Digital Single Market, provide clarity on everyone's responsibilities, and safeguard online rights.

We look forward to working with policy-makers and providing information on how industry counteracts illegal content, products, services, and activities on intermediary services while safeguarding users' fundamental rights. We stand ready to work with the EU institutions to tackle any remaining challenges that existing initiatives haven't solved.

About CCIA

CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For nearly fifty years, CCIA has promoted open markets, open systems, and open networks. For more, visit www.ccianet.org.

Endnotes

1. European Commission, Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 15 December 2020, available at: https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFI.N.

2. Oxford Economics, Digital Services in Europe, November 2020, available at: https://www.oxfordeconomics.com/recent-releases/Digital-services-in-Europe.

3. Ibid., p. 29 - p. 47.

4. On hate speech, the fifth evaluation on the EU Code of Conduct on Countering Illegal Hate Speech Online shows that on average 90% of the notifications are reviewed within 24 hours and 71% of the content is removed. For instance, YouTube has reported that between July and September 2020, it removed 7.9 million problematic videos. Of these, 43% had not been viewed, and 76% had received fewer than 11 views.

On the sale of counterfeits, online marketplaces have developed brand registration programmes to enable the rapid identification of fakes; streamlined reporting procedures; and increasingly use technology to track individual products from seller to marketplace to end-consumer. Evaluations of the European Commission's Memorandum of Understanding (MoU) on the sale of counterfeit goods found that between 90% and 98% of listings removed for alleged IP infringements had been removed proactively by online platforms. Some 2.4 million listings were removed for an alleged infringement of intellectual property in May and June 2019.

5. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ L 178, 17.7.2000, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=en.

6. European Commission, Impact Assessment Annexes accompanying the proposal for a regulation on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 15 December 2020, available at: https://ec.europa.eu/digital-single-market/en/news/impact-assessment-digital-services-act.

7. European Commission, Impact Assessment Annexes accompanying the proposal for a regulation on promoting fairness and transparency for business users of online intermediation services, 26 April 2018, available at: https://ec.europa.eu/digital-single-market/en/news/impact-assessment-proposal--promoting-fair ness-transparency-online-platform.

8. For instance: Allegro, Booking.com, cDiscount, Criteo, DeliveryHero, Spotify, Wolt, or Zalando.

9. Oxford Economics, op. cit., p. 15 - p. 21.

10. The Austrian Parliament approved the Anti-Hate Speech Law (KoPl-G), together with the 'Hate on the Net Fighting Act' (10 Dec 2020). It aims to fight anti-Semitism, both offline and online, available at: https://www.parlament.gv.at/PAKT/PR/JAHR_2020/PK1391/#XXVII_I_00463.

11. France, Amendment presented by the government on "le respect des principes de la république", 15 January 2021, available at: https://www.assemblee-nationale.fr/dyn/15/amendements/3649/CSPRINCREP/1770.pdf.

12. Germany, Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act, NetzDG), available at: https://www.bmjv.de/DE/Themen/FokusThemen/NetzDG/NetzDG_EN_node.htm.

13. Euractiv, "Hungary to regulate 'digital damaging' of tech giants", 27 January 2021, available at: https://www.euractiv.com/section/politics/short_news/hungary-to-regulate-digital-damaging-of-tech-giants/.

14. 2020/0361(COD) Proposal of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 15 December 2020, p. 4, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=EN.

15. While the DSA mentions that the definition will be left to the Member States, the DSA gives an understanding which is very broad, leading to legal uncertainty, primarily by extending its scope via the formula: "*by its reference to an* [illegal] *activity*". This solution can exponentially increase the number of content pieces to be considered illegal, without any criteria to assess how "strong" the "reference" should be to lead to a meaningful equalization between the illegal content as such and the information referring to it.

16. Ibid., Article 25 to Article 33.

17. Tech against terrorism, "Analysis: ISIS use of smaller platforms and the DWeb to share terrorist content", April 2019, available at: https://www.techagainstterrorism.org/2019/04/29/analysis-isis-use-of-smaller-platforms-and-the-dweb-to-share-terrorist-content-april-2019.

18. European Commission, Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, COM/2018/640 final, Recital 10, available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52018PC0640.

19. Proportionality should be assessed in concrete leading, where appropriate to a case-by-case evaluation to determine what obligations can be most effective for a given service provider.

20. Oxera, "The impact of the Digital Services Act on business users", for Allied for Startups, 23 October 2020, p.3., available at: https://alliedforstartups.org/wp-content/uploads/2020/10/Impact-of-DSA-on-EU-business-policy-paper-2020-10-23-1.pdf.

21. For instance, a video of a car speeding.

22. As concerns cloud-based file-sharing services for consumers, their primary purpose is not sharing information to the public but rather storing personal content and sharing within closed circles. The ability to access a piece of content to a broader group is an ancillary feature and does not constitute an act of communication per se.

23. European Commission, Proposal on preventing the dissemination of terrorist content online, op. cit. Recital 10.

24. European Commission, Proposal for a Digital Services Act, op. cit., Article 14.2(c): "the name and an electronic mail address of the individual or entity submitting the notice, except in the case of information considered to involve one of the offences referred to in Articles 3 to 7 of Directive 2011/93/EU".

25. How will Digital Services Coordinators appoint 'trusted flaggers'? How will they verify their expertise? Would it make sense for a recognised Greek trusted flagger to interfere with Scandinavian content or service providers? Should a content-specific 'trusted flagger' have the same ability to notify infringing products to a marketplace? What happens if a 'trusted flagger' abuses its position?

26. European Commission, Proposal for a Digital Services Act, op. cit., Article 22.1.

27. Ibid., Article 22.1(d): "*the name, address, telephone number and electronic mail address of the economic operator, within the meaning of Article 3(13) and Article 4 of Regulation (EU) 2019/1020 of the European Parliament and the Council 51 or any relevant act of Union law*".

28. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, PE/72/2017/REV/1, OJ L 156, 19.6.2018, p. 43–74, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32018L0843.

29. Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006, OJ L 141, 5.6.2015, p. 1–18, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R0847.

30. Council Directive (EU) 2020/876 of 24 June 2020 amending Directive 2011/16/EU to address the urgent need to defer certain time limits for the filing and exchange of information in the field of taxation because of the COVID-19 pandemic, OJ L 204, 26.6.2020, p. 46–48, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32020L0876.

31. Senftleben, Martin and Angelopoulos, Christina, The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the E-Commerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market, Amsterdam/Cambridge, October 2020, available at: https://ssrn.com/abstract=3717022.

32. European Commission, Proposal on preventing the dissemination of terrorist content online, op. cit.

33. Oxford Economics, op. cit., p. 43 - p. 44.

34. Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (OJ L 186, 11.7.2019), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2019%3A186%3ATOC&uri=uriserv%3AOJ.L_.2019.186.01.0057.01.ENG.

35. Micro, small and medium-sized digital platforms represent 92% of Europe's online platforms. See European Commission's Presentation on the Digital Services Act Package for the 21st meeting of the eCommerce Expert Group, Slide 6, 26 May 2020, available at: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=41347.

36. European Commission, Proposal on preventing the dissemination of terrorist content online, op. cit., Article 4 and Article 4(a).

37. European Commission, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final - 2018/0108 (COD), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN.

38. European Commission, Proposal for a Digital Services Act, op. cit., Article 8.2(b).

39. European Commission, Proposal for a Digital Services Act, op. cit., Article 8.1.