cerre Centre on Regulation in Europe

OVERLAPS - SERVICES AND HARMS IN SCOPE

REPORT

November 2022

Michèle Ledger

Sally Broughton Micova

As provided for in CERRE's bylaws and procedural rules from its "Transparency & Independence Policy", all CERRE research projects and reports are completed in accordance with the strictest academic independence.

The project, within the framework of which this report has been prepared, received the support and/or input of the following CERRE member organisations: ARCOM, Mediaset, Ofcom, Vodafone. However, they bear no responsibility for the contents of this report. The views expressed in this CERRE report are attributable only to the authors in a personal capacity and not to any institution with which they are associated. In addition, they do not necessarily correspond either to those of CERRE, or of any sponsor or of members of CERRE.

info@cerre.eu – www.cerre.eu

TABLE OF CONTENTS

ABOUT CERRE

Providing top quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE) promotes robust and consistent regulation in Europe's network and digital industries. CERRE's members are regulatory authorities and operators in those industries as well as universities.

CERRE's added value is based on:

- its original, multidisciplinary and cross-sector approach;
- the widely acknowledged academic credentials and policy experience of its team and associated staff members;
- its scientific independence and impartiality;
- the direct relevance and timeliness of its contributions to the policy and regulatory development process applicable to network industries and the markets for their services.

CERRE's activities include contributions to the development of norms, standards and policy recommendations related to the regulation of service providers, to the specification of market rules and to improvements in the management of infrastructure in a changing political, economic, technological and social environment. CERRE's work also aims at clarifying the respective roles of market operators, governments and regulatory authorities, as well as at strengthening the expertise of the latter, since in many Member States, regulators are part of a relatively recent profession.

ABOUT THE AUTHORS

Michèle Ledger is a CERRE Research Fellow and a researcher at the CRIDS research centre of the University of Namur where she also lectures on the regulatory aspects of online platforms at the postmaster degree course (DTIC).

She has been working for more than 20 years at Cullen International and leads the company's Media regulatory intelligence service.

Sally Broughton Micova is a CERRE Academic Co-Director and a Lecturer in Communications Policy and Politics at the University of East Anglia (UEA). She is also a member of UEA's Centre for Competition Policy.

Her research focuses on media and communications policy in Europe.

She completed her PhD in the Department of Media and Communications at the London School of Economics and Political Science (LSE), after which she was an LSE Teaching and Research Fellow in Media Governance and Policy and Deputy Director of the LSE Media Policy Project.

EXECUTIVE SUMMARY

This report compares four pieces of adopted and draft legislation that deal with illegal and harmful content on digital services: the rules on video-sharing platforms (VSPs) contained in the Audiovisual Media Services Directive (AVMSD), the Terrorist Content Regulation (TERREG), the Digital Services Act (DSA) and the UK's proposed Online Safety Bill (OSB). It compares the services and the harms in scope.

The international legal context examined (mainly Council of Europe conventions and recommendations) has evolved over the last two decades. There are international norms for 'platforms' that are defined as providers of digital services that connect participants in multisided markets, set the rules for such interactions and make use of algorithmic systems to collect and analyse data and personalise their services.

Given the global nature of digital services, each of the laws studied foresees an extra-territorial effect to make sure that providers with some sort of connection with their jurisdiction comply with the rules. The mechanisms differ however, creating a layer of complexity for the regulators who will need to enforce the rules and for the platforms that will need to comply.

The EU initiatives do not contain rules on the designation of services, except for the DSA in relation to very large online platforms (VLOPs) and very large online search engines (VLOSEs), which means that the overwhelming majority of services in scope will need to comply with the rules of the DSA without being formally identified or designated. In contrast, the OSB sets out a system whereby **Ofcom will need to establish and maintain a register** with the services that fall within the different tiers of services.

The AVMSD contains rules on jurisdiction that are not reflected in the DSA or the TERREG to **determine which Member States are responsible for the oversight and enforcement of the rules in relation to VSPs**. Member States need to manage up-to-date lists of VSP providers and the Commission maintains these in a **central database**, accessible by the national regulatory authorities. The AVMSD also contains a mechanism to solve **conflicts of jurisdiction**, which is not echoed in the DSA.

The EU and UK initiatives refer to categories of services but the categories differ, leading to overlaps and grey zones. The DSA has the broadest scope of application since it covers the technical internet layer whereas the other pieces of legislation do not. The OSB is also wide and is striking as it covers pornography publishers (on top of user-to-user and search intermediaries). **Gaming presents a notable gap across the board as it is not mentioned in either of the initiatives (but could be covered), and it is already not entirely clear if the more holistic pieces of legislation (the DSA and OSB) cover the 'metaverse' or other future developments**.

The DSA does not contain **a special regime for edited or journalistic content**, whereas the other initiatives do. The AVMSD contains rules on prominence whereby the member states are allowed to take measures to ensure the "appropriate prominence of audiovisual media services of general interest". The Commission's proposed EMFA would now address this issue as it contains rules to ensure that VLOPs respect the editorial integrity of media services. The OSB contains a requirement

for the largest platforms to put in place special procedures to ensure the importance of the free expression of content of democratic importance and of journalistic content, and it exempts publishers and audiovisual media services from being considered to have committed certain criminal communications offences.

The DSA stands out as having the widest scope in terms of illegal harms whereas all the other initiatives are narrower in scope. Whereas as the AVMSD and TERREG each deal with specific types of illegal content, Illegality in the DSA is defined by reference to any breach of EU or national law, provided the national law is in line with EU law. This could present challenges in terms of implementation. An independent and transparent process to settle potential conflicts between national and EU legislation may need to be established by the Commission or in subsequent legislation. The OSB creates an obvious hierarchy by distinguishing between illegal content and priority illegal content. Content in the priority category mostly derive its illegality from criminal offences in existing legislation, but the OSB also creates several new communications offences.

The DSA has the widest scope of legal harms for VLOPs and VLOSEs in that it requires assessment of systemic risk, and mitigation, of an extensive list of harms to individual users and to wider society, including risks to fundamental rights. Its approach acknowledges the collective nature of many harms and risks to public institutions, opening the door to positive obligations on platforms. **The protection of minors** is a concern in all initiatives (except in TERREG). Harm to well-being is emerging as new category of harm in the AVMSD, the DSA and the OSB. This is particularly evident in the standards for commercial communications in the AVMSD, and in the DSA's attention to risks to public health and of gender-based violence, and the measures to prevent harm to individuals' mental and physical health.

1. INTRODUCTION

The **proliferation of digital services has provided people with enormous opportunities for communication, creativity, and commerce, but also enabled the spread of a vast range of harmful content and behaviour online**. Policy makers have struggled to keep up across the world and **policy responses have generally begun piecemeal**, addressing particularly egregious harms first such as the dissemination of child sexual exploitation and abuse material (CSAM) and terrorist content. The European Union adopted a revision to its Audiovisual Media Services Directive (AVMSD) in 2018 that aimed to address this type of illegal content on video-sharing platforms (VSPs) and followed that with a Regulation addressing the dissemination of terrorist content online (hereafter referred to as the terrorist content regulation, TERREG) in 2021. A comprehensive Digital Service Act (DSA) was informally endorsed by the Council and the Parliament in April 2022. The text was formally adopted on 4 October 2022 and published in the Official Journal on 27 October 2022.

The United Kingdom launched its process to develop an Online Safety Bill (OSB) at the same time the European Commission launched its proposal for the DSA. The UK's Bill was in legislative procedure as a second draft by April 2022, but its adoption was postponed by changes in government and debate is expected to resume in autumn 2022. The DSA, arguably, has the potential to be standard setting for the wider European region or even beyond, especially given the scope of content and harms it aims to address and its first-mover status. Nevertheless, the UK's future Online Safety legislation may prove to be a more flexible instrument and has the potential to be standard setting, given the role for Ofcom in adopting detailed codes of practice.

This **report examines these four pieces of adopted and draft legislation that deal with illegal and harmful content on digital services[1]. It presents the findings from a systematic comparison in two areas: the services in scope and the harms in scope**. It does not compare institutional design since doing so seemed inappropriate when looking at both EU and national level legislation, and because the institutional design for the governance of digital services within the EU was covered in a recent CERRE report by Giorgio Monti and Alexandre de Streel[2]. All these pieces of legislation[3] deal with the balancing of expression rights with other fundamental rights and critical public interests. This report, therefore, begins with a discussion of the international legal and normative context. It then presents the comparison of services in scope followed by a discussion of any exceptions for journalistic or otherwise regulated content. The report contains two sections on harms in scope, treating first those associated with illegal content and behaviour and then those that can be considered legal harms.

[1] In May 2022 the European Commission also proposed a specific regulation to combat child sexual exploitation, but as this project was already underway, it was not possible to bring it also into the scope of this report. The proposal can be found at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472

[2] https://cerre.eu/publications/improving-eu-institutional-design/

[3] Although at the time of writing, the OSB was not yet adopted, for ease of reading we will refer to all as legislation throughout. For the DSA analysis was based firstly on the proposal from the European Commission and then updated to reflect the text formally adopted in July, therefore throughout the report the authors refer to the text endorsed by the European Parliament on 4 July 2022 for the DSA: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0269_EN.html. The references to the articles of the DSA have been updated to refer to the version published in the Official Journal. For the OSB text used is available at https://publications.parliament.uk/pa/bills/cbill/58-03/0121/220121.pdf

In conclusion on each of the aspects covered, the differences are substantial and could lead to application difficulties in practice, which may have important and unintended consequences for citizens, companies, and regulators alike.

2. NORMS AND INTERNATIONAL LEGAL CONTEXT

To provide some context and normative framework for the four pieces of legislation for the regulation of content on digital services, this section gives a brief look at key elements of international law and soft law. It covers Council of Europe standards that come in the form of conventions, recommendations, and guidelines. All EU Member States are also members of the Council of Europe as is the UK. While not all these countries have ratified all the conventions, these are legally binding instruments for those that have, and are arguably still normative standards for those that have yet to ratify. The first set provides the basis for the scope of state or EU level regulation of the digital services that disseminate content. The second set covers the framework for the balancing of rights and public interest crucial to the later discussion of harms.

2.1. Standards for services in scope

In 2001 the Convention on Cybercrime was adopted by the Council of Europe to address the criminal use of what it defined as 'computer systems'. It provided a framework for the assertion of jurisdiction over the services that are provided on such systems. The Convention covers national criminalisation of the behaviour of individual users and set out basic standards for what states can require of a 'service provider' defined as:

- any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
- any other entity that processes or stores computer data on behalf of such communication service or users of such service (ETS 185, 2001; Art. 1).

It provides the basis for states to require traffic data, subscriber information, and content data in relation to serious criminal offences, such as the dissemination of CSAM. The Convention deals with jurisdiction only in relation to the offences, rather than to the service providers; however, it does empower signatories to adopt legislation that would place obligations on service providers.

Since then, Council of Europe standards have aimed to establish human rights-based principles for the governance of 'the internet' (Council of Ministers, 2011) and the protection of 'internet freedom' (CM/Rec(2016)5). The scope of what could be considered to constitute 'the internet' has not been defined, however other standards have established an understanding of what constitutes internet intermediaries as hosts or conduits to content. The 2011 Recommendation on a New Notion of Media (CMRec(2011)7) makes a distinction between services that are media and ones that are intermediaries or auxiliaries involved in media ecosystems. It maintains that these may host content or be the conduits for the dissemination of content and therefore are important subjects of regulation aimed at protecting users and human rights but merit a different response than media. The Council of Ministers later elaborated specific recommendations to states on ensuring the protection of human rights on internet intermediaries (CM/Rec(2018)2). A body of case law in the European Court of Human Rights has emerged as the court has navigated this distinction. As McGonagle and Frosio (2020) elaborate the court has developed an approach that promotes freedom of expression and public debate for the media and has begun to apply these principles to the internet.

The recent Recommendation of the Committee of Ministers to Member States on principles for media and communication governance (CM/Rec(2022)11) maintains a distinction between media and other online services, but uses the term platforms, which it defines as "providers of digital services that connect participants in multisided markets, set the rules for such interactions and make use of algorithmic systems to collect and analyse data and personalise their services." It gives examples of search engines, news aggregators, video-sharing services, and social networks. This recommendation specifically addresses both media and platforms as necessary subjects of governance, with platforms identified as requiring a risk-based approach to illegal and legal but harmful content.

2.2. Rights and harms

Three aspects of the right to freedom of expression are of crucial importance to the context of these four pieces of legislation. Firstly, this right protects not only the person expressing, but also the audience for that expression. As both the Universal Declaration of Human Rights (UDHR) and the European Convention on Human Rights (ECHR) state in Articles 19 and 10 respectively, the right to freedom of expression covers the right to both receive and impart information. It is also directly linked to the freedom to form and hold opinions. The wording of the UDHR and the ECHR is mirrored in the EU Charter on Fundamental Rights, which has had full legal effect within the EU since the 2009 Lisbon treaty. The freedom of expression enshrined in wider international law was thus reenforced by EU level law, maintaining the recognition of the two-way nature of expression rights.

The exemption from liability for content and the ban on imposing requirements for general monitoring contained in the EU's landmark 2000 e-Commerce Directive (ECD) and common in other jurisdictions were put in place to protect the users of information society services and providers of information society services. Such provisions were intended to ensure that service providers did not have incentives to overly interfere with users' rights to impart information and ideas as content creators or to seek and receive the information shared by others, as well as to provide the legal certainty required to encourage investment and innovation in such services. The Council of Europe's Council of Ministers confirmed these policies as essential safeguards for freedom of expression in the 2018 Recommendation on the roles and responsibilities of Internet intermediaries CM/Rec(2018)2. The DSA updates the ECD in a manner that clearly upholds these two policies.

A second aspect of freedom of expression is that it is a collective right as well as an individual right. The purposes of guaranteeing freedom of expression are to enable effective participation in decision-making within society and to provide conditions for individual self-realisation or self-fulfilment (Baker, 1989). The collective aspect of decision-making with a society lies not only in the consequences of any outcomes, but also in the act of decision-making because confrontation with other views and information is required. Self-realisation also requires the ability to test one's ideas among a multiplicity of views (Lichtenberg, 1990). The collective nature of expression rights generates the positive obligations on states to provide vehicles for expression that have been part of media regulation at national levels (Broughton Micova, 2020; Kenyon, 2021b), but have thus far not been part of platform regulation.

A third important aspect of the freedom of expression is that it is not absolute. International and EU law allow for restrictions on freedom of expression as long as they are necessary and prescribed by

law. Certain types of expression are explicitly illegal in international law. Article 20 of the International Covenant on Civil and Political Rights (ICCPR) prohibits "propaganda for war" and "any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence". There is no need to balance any protection of such expression with justifiable reasons for restriction, as they are unprotected forms that merit outright bans.

Other expression is protected unless there is legitimate reason for restriction. Article 19 of the ICCPR cites the rights and reputation of others as well as national security, public security, and public health or morals as potentially legitimate reasons for restricting expression. The ECHR contains a more extensive elaboration of the condition under which freedom of expression can be constrained:

> *"The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary"*

Expression is therefore protected to the point at which its protection is balanced against these other rights of individuals or collective public interests.

As Bychawska-Siniarska (2017) elaborates, the European Court of Human Rights (ECtHR) has derived a three-part test to determine whether a state's interference, which can mean from a formality or set condition to outright restriction or penalty, with freedom of expression is legitimate.

- The interference is prescribed by law.
- The interference is aimed at protecting one or more of the following interests or values: national security; territorial integrity; public safety; prevention of disorder or crime; protection of health; morals; reputation or rights of others; preventing the disclosure of information received in confidence; and maintaining the authority and impartiality of the judiciary.
- The interference is necessary in a democratic society.

The Convention on Cybercrime already in 2001 set out some specific categories of offences where state law should prescribe interference, namely the sexual exploitation of children, fraud, impingement on the integrity of computer systems, and intellectual property. The Council of Europe Council of Ministers has recently adopted a recommendation on combatting hate speech that lays out in detail how it should be covered in criminal law and civil law (CM/Rec(2022)16). Both documents acknowledge the harms to individuals and to a group and wider society from these illegal harms.

There is therefore an established understanding of both individual and collective harms from illegal content and behaviour and of an individual and collective aspect to freedom of expression. There is less evidence of established norms on the nature of legal harms, and efforts to combat them should be effectively balanced with both individuals and collective rights.

3. SERVICES IN SCOPE

There are many differences and similarities among the instruments in terms of the services in scope. A common feature is that all instruments are defined by reference to categories of services. The difficulty stems from the fact that the categories of services differ, leading sometimes to overlaps and grey zones. Taken together, this creates a complex picture, especially given the fact that platforms will often need to comply with all the instruments, because of the extra-territorial effect of each piece of legislation.

3.1. Definition of the services in scope

3.1.1. Types of services

The **DSA and the OSB have the broadest scopes of application**.

The **DSA** refers to the notion of **intermediation service** (itself a subset of 'information society services'). The reference to information society services (ISS) is therefore central. ISS are defined in the EU Regulatory Transparency Directive[4] as a service provided at a distance, by electronic means and at the individual request of a recipient of the service. ISS are widely referred to in EU legislation and in particular in the ECD. **The DSA only covers a subset of these ISS**: intermediary services[5], which are:

- Mere conduit
- Caching
- Hosting services which are also subdivided into online platforms, and Very Large Online Platform (VLOPS)
- Online search engines, including Very Large Online Search Engines (VLOSES).

[4] Article 1 (1) (b) Directive 2015/1535 (which replaced Directive 98/34/EC).
[5] Article 3 (g) of the DSA.

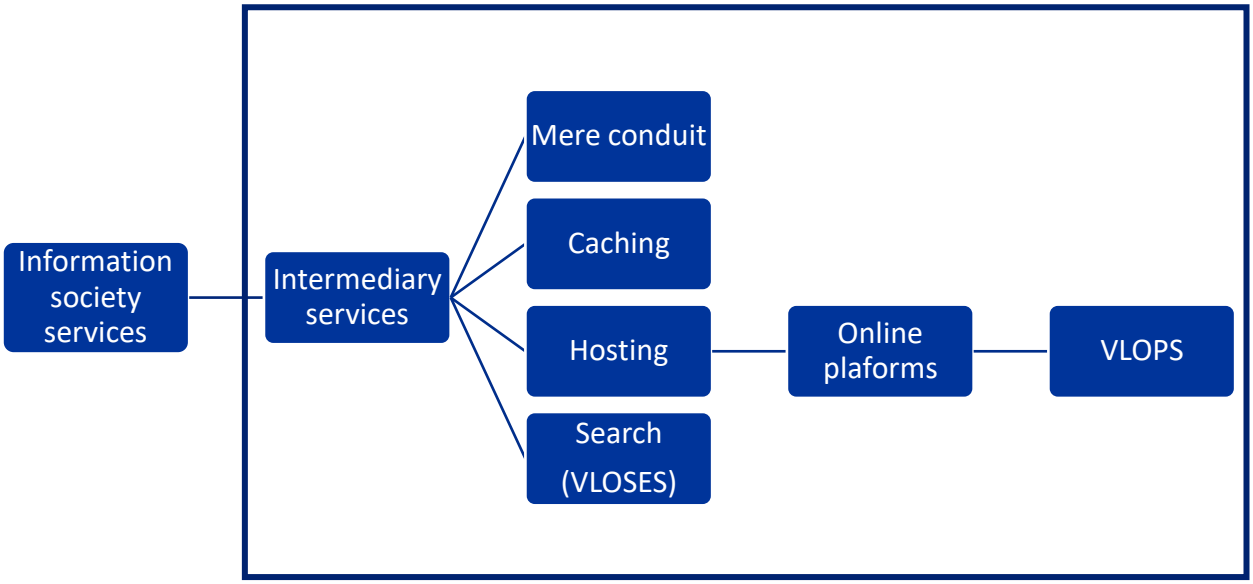

Figure 1. Scope of application of the DSA

The **DSA has a risk-based approach meaning that VLOPS and VLOSES will be subject to the most obligations (in particular risk assessments) and to stronger oversight, because they are likely to cause the largest societal risks owing to the widest dissemination of illegal and harmful content, whereas the online platforms and search engines that do not meet the threshold of 45 million monthly active users will be subject to fewer duties, albeit to more duties than the hosting services that do not disseminate content to the public. Providers of mere conduit and caching services (referred to below as technical internet services) are subject to a basic tier of rules.**

The **OSB** covers certain internet services: **user-to-user (U2U) services**, search services (see below for a more detailed account), and a narrower category of services that publish pornographic content, which does not host user-generated content or enable U2U. A U2U service is defined as an internet service by means of which content that is generated directly on the service or uploaded to or shared on the service by a user of the service, may be encountered by another user, or other users of the service.[6] The provider of a U2U service is the entity that has control over who can use the U2U part of the service. If no entity has this control, but if one (or more) individual(s) has control, the individual(s) will be considered as the provider of the service.

Different tiers or rules are foreseen for category 1 (high risk/reach U2U), 2A (high risk/reach search) and 2B (high risk/reach U2U but without reaching category 1 threshold) services which are characterised at least by a number of users and functionality. These will be the services with the highest reach and that carry the highest risk. The thresholds will be set in secondary legislation, following research to be conducted by Ofcom.

[6] S. 3(2) of OSB.

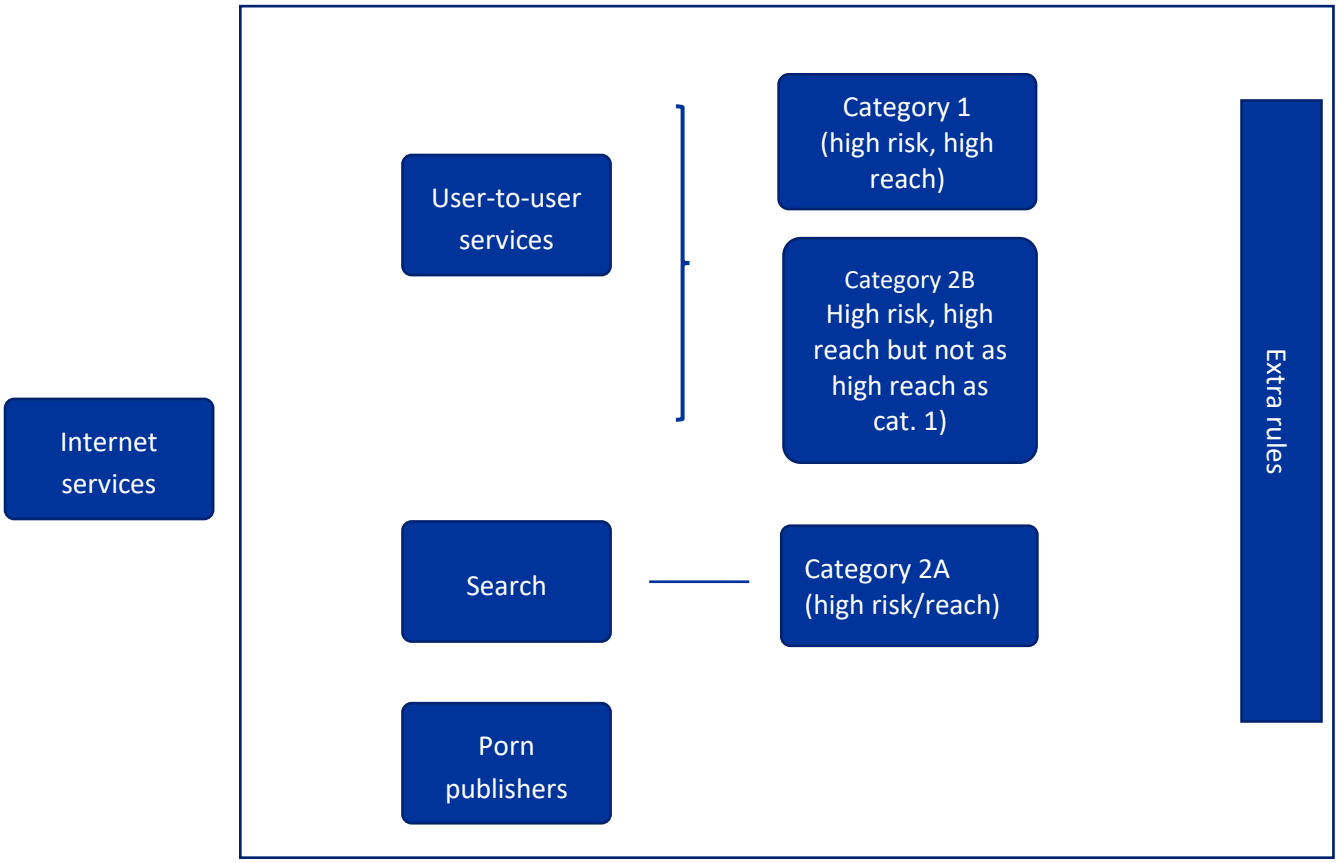

Figure 2. Scope of application of the OSB

The **TERREG** applies to **hosting services** (defined like in the DSA as information society services consisting of the storage of information provided by and at the request of a content provider) that disseminate content to the public, but not to private hosting services. It does **not have a tiered** approach, all platforms in scope are subject to the same obligations in relation to terrorist content. If a platform has been exposed to terrorist content, it will then have to adopt additional measures, but these are not dependent on the size or reach of the service.

The **AVMSD** has the narrowest scope of application as it only applies to platforms or to a dissociable section of the platform (service) where the principal purpose or essential functionality is to **provide programmes and/or user-generated video content** where the service does not have editorial responsibility.[7] This means that a service with essentially text or images is excluded. It does not have a tiered approach beyond the fact that the appropriate measures to be taken by VSPs must be

[7] Article 1 (1) (b) (aa) of the revised AVMSD defines a VSP "a service as defined by Articles 56 and 57 of the Treaty on the Functioning of the European Union, where the principal purpose of the service or of a dissociable section thereof or an essential functionality of the service is devoted to providing programmes, user-generated videos, or both, to the general public, for which the video-sharing platform provider does not have editorial responsibility, in order to inform, entertain or educate, by means of electronic communications networks within the meaning of point (a) of Article 2 of Directive 2002/21/EC and the organisation of which is determined by the video-sharing platform provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing."

practicable and proportionate, considering the size of the VSP and the nature of the service that is provided.

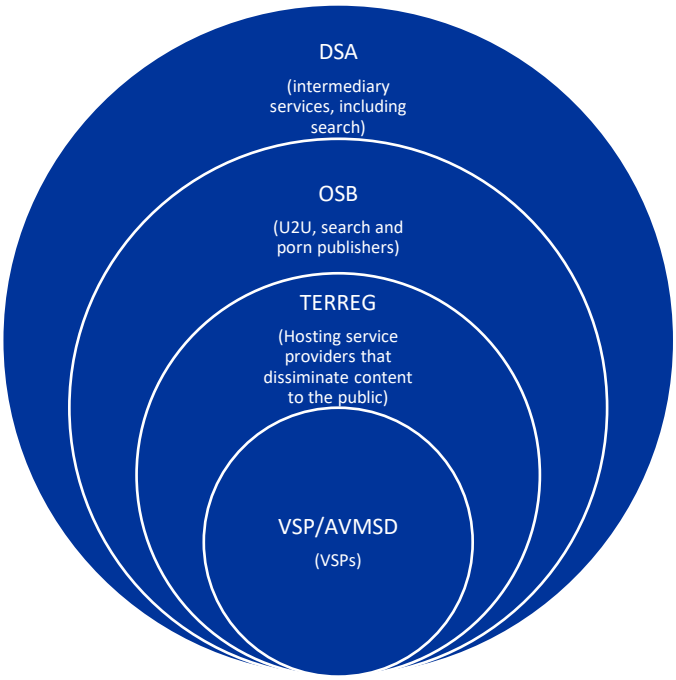

Figure 3. Scope of application of initiatives - Summary

3.1.2. Territorial application

Given the global nature of digital services, the initiatives naturally also foresee that they have an extra-territorial effect to make sure that providers comply with the rules if they have some sort of connection with their jurisdiction. The mechanisms however differ, creating an additional layer of complexity for the regulators who will need to enforce the rules and for the platforms themselves who will need to comply with them.

The **DSA[8] and the TERREG[9]** contain the same mechanism which is that the regulations apply to providers irrespective of their place of establishment, provided they **offer services in the EU, as evidenced by a substantial connection**. This substantial connection will be presumed to exist either where the service provider:

- has an establishment in the EU;
- has a significant number of recipients of the services in one or more Member States in relation to the population; or

[8] Recital 7 and 8 and articles 3 (d) (e) of the DSA
[9] Recitals 15 and 16 and articles 1.2 and article 2 (4) and (5) of the TERREG

- targets its activities towards one or more Member States. This can be determined on the basis of all relevant circumstances, including factors such as the use of a language or currency, or the possibility of ordering products or services, or using a relevant top-level domain. The fact that a website is accessible technically from the Union is not sufficient ground alone to be considered as establishing a substantial connection to the Union.

These providers will then need to designate a legal representative in one of the Member States where they offer services. That legal representative could be held liable for non-compliance with obligations under the DSA.

Rules for VSPs in the **AVMSD** are different. To be covered, a non-EU VSP will be deemed to be established in a Member State if it has a parent or subsidiary undertaking that is established in that Member State or if it is part of a group where an undertaking is established in that member state.[10] So, here the criteria is to have a **link or connection with a parent or subsidiary undertaking that has an establishment in the EU**.

Unsurprisingly, the OSB also contains rules to capture the services in scope and if they 'have links with the UK'. This will be the case if:

- the service has a significant number of users in the UK; or
- the UK is a target market; or
- if it can be used in the UK by individuals and there are reasonable grounds to believe that there is a material risk of significant harm to individuals in the UK.[11]

Therefore, **similar to the DSA and the TERREG, the OSB's criteria are based on the location of the end users and whether or not they are targeted by the service**. Unlike in the EU laws, which also include establishment criteria, or in the case of the AVMSD solely establishment, the UK law has the widest scope of application and is not concerned with the location of the service provider at all. It also reaches much wider than its user-based criteria by considering only the potential to be used and the risk of significant harm in addition to actual use.

In short, the TERREG, the DSA and the OSB are more encompassing than the AVMSD.

3.1.3. Designation of services

Another striking difference is the mechanisms foreseen in the legislation to designate the services in scope.

The **DSA does not contain any rule, except in relation to the designation procedure for the VLOPS and VLOSES**. This implies that for most services in scope they will need to comply with the rules of the DSA, without being formally identified or designated.

[10] Article 28a of AVMSD. Other details are also provided to settle which member state has jurisdiction where there are multiple establishments.
[11] Explanatory notes to the OSB, p.17.

For the VLOPS and VLOSES, the DSA foresees that the Commission will designate them among the online platforms that reach the threshold. It will need to adopt a designating decision [after having consulted the Digital Services Coordinator (DSC) of the Member State of establishment or after having noted that the DSC has informed it that the threshold is met]. A procedure is also foreseen if the Commission intends to take its decision on data not provided by the platform itself. In this case, the Commission will allow the platform to provide its views. The Commission will also need to repeal the designation decision if the number of average monthly active users falls below the threshold for an uninterrupted period of one year. A list of very large online services will be published in the Official Journal, and it will keep that list updated. The concerned platforms will have four months to comply with the rules for very large platforms.

The **TERREG does not contain general rules on the designation of services, beyond rules on jurisdiction**. However, service providers exposed to terrorist content will need to take certain specific measures to protect its services against the dissemination to the public of terrorist content. A service will be deemed to be exposed to terrorist content where the competent authority of the Member State of its main establishment has taken a decision to that effect and has notified the decision to the service provider. The decision will need to be taken on the basis of objective factors such as having received two or more final removal orders in the previous 12 months. A service provider will have three months to inform the competent authority of the specific measures it intends to take to mitigate the level of exposure of its services to terrorist content. The service provider will need to report back each year until the competent authority revokes the designation decision.

The **AVMSD contains rules on jurisdiction, i.e., to determine which Member States are responsible in theory for the oversight and enforcement of the rules in relation to VSPs, but it does not foresee that the authorities in charge must designate the services**. When implementing the AVMSD, many Member States have set up a notification or registration obligation, but this is not the case in all the Member States.[12]

In terms of publicity, however, the AVMSD foresees an interesting mechanism whereby the Member States need to establish and maintain up-to-date lists of VSP platforms established or deemed to be established on their territory and communicate the list to the European Commission. In turn, the Commission needs to make sure the list is made available in a **central database**, which will be accessible by the national regulatory authorities. The information contained in the database will also be publicly available. To date, this information has not yet been disclosed to the public.

The **OSB foresees a system whereby Ofcom will need to establish and maintain a register** with the services that fall within the different categories of regulated services (Category 1, 2A, and 2B of regulated U2U and search services). Ofcom will be required to assess the services which are likely to satisfy the thresholds (once they are set by the secretary of state).

[12] Mapping of national rules applicable to video-sharing platforms: Illegal and harmful content online, European Audiovisual Observatory, Strasbourg, 2021

3.1.4. Mechanisms in case of conflicts of jurisdiction between Member States

Surprisingly, **across all the laws, the only mechanism foreseen for resolving jurisdiction disputes between Member States is for VSPs in the AVMSD**. Where there is a conflict in the determination of which Member State has jurisdiction, the Member States concerned must bring the case to the Commission. The Commission can choose to request the help of the European Regulatory Group for Audiovisual (ERGA), which is comprised of all the EU audiovisual media regulators and plays an advisory and coordination role. ERGA would need to deliver an opinion to the Commission which decides on the case.

The **DSA** only foresees that the Member State of the 'main' establishment of the provider of intermediary services has the exclusive power for the supervision and enforcement of the DSA.[13] For VLOPS and VLOSES, the European Commission is solely responsible for the oversight of their added duties (compared to those applicable to online platforms). For intermediary services with no establishment in the EU, the member state where the legal representative resides or is located, or the Commission will have the enforcement powers. If no legal representative is designated, then all Member States or the Commission (for VLOPS and VLOSES) will have the oversight powers. Beyond the need to cooperate, nothing is specified in relation to solving possible conflicts of jurisdiction between the Member States.

In practice, this implies that if a conflict of jurisdiction arises between the Member States, the rules of the AVMSD will apply in so far as the conflict concerns the rules applicable to VSPs. If the conflict concerns the application of the rules regarding the DSA, no obvious way of solving the case comes to mind, except in an informal manner through the European Board for Digital Services (EBDS), the independent advisory group of DSCs set up among other things to contribute to the consistent application of the DSA and effective cooperation of the DSCs.[14] Because the European Commission will be supervising the VLOPS and VLOSES (at least in relation to their added obligation) conflicts of jurisdiction in relation to these services are less likely to arise in practice.

The most logical place however for clarification on these rules and potentially also on the idea of a database listing the services that are supervised at a national level would be in the E-Commerce Directive.

3.2. Review of specific types of services

In this section, we review certain categories of services in more detail, namely technical internet services, online storage and distribution services, private messaging services, search, online marketplaces, websites and platforms with pornography, gaming services, and live streaming services.

[13] The DSC of establishment means the DSC of the Member State where the main establishment of a provider is located or its legal representative resides or is established, article 3 (n) of the DSA.
[14] Article 61 of the DSA.

3.2.1. Technical internet services excluded from all initiatives, except the DSA

One of the most striking differences is that **technical internet services are only in scope of the DSA**, while none of the other legal instruments cover these types of services. This can be explained by the fact that the DSA carries over the rules on the liability of intermediaries of the ECD, which include the 'mere conduit' and 'caching' services.

It is still relatively difficult to determine which internet services are in scope and which are not. Schermer & al (2020) conducted a study on the technical and legal evolution around non-hosting intermediary services (i.e., mere conduit[15] and caching[16]) to see how the legal framework (before the adoption of the DSA) could be upgraded.

To recap briefly, mere conduit is defined as an information society service "that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network".[17] This clearly covers two activities: that of transmission and of provision of access to the internet.

Caching is described in the ECD (and in the DSA) as the automatic, intermediate, and temporary storage of information provided by a recipient of a service performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request. At the time of adoption of the ECD, this seemed to only cover proxy servers (DLA Piper, 2009).

Schermer & al. highlight **some grey zones highlighted by such as Domain Name Systems (DNS), providers of WIFI hotspots, Content Delivery Networks (CDN), and live streaming**. The DSA does not clear up these grey zones. Since the definitions of the ECD have been carried over into the DSA, and because the DSA is a regulation, this means that the Member States will find it difficult to shed light in their legislation on the legal treatment of these services. The Court of Justice of the European Union (CJEU) will therefore have a key role to play. Alternatively, the European Commission could provide non-binding guidance.

The recitals of the DSA acknowledge that the online ecosystem is increasingly complex as new technologies have emerged to improve the availability, efficiency, speed, reliability, capacity, and security of systems for the transmission, findability, and storage of data online. Services that establish and facilitate the underlying architecture and proper functioning of the internet, including the technical auxiliary functions can also benefit from the exemptions from liability to the extent they qualify mere conduit, caching, or hosting.

The recitals also seek to clarify that such services include, and among others, online search engines, wireless local area networks, DNS services, top-level domain names registries, registrars, certificate

[15] Article 12 of the ECD
[16] Article 13 of the ECD
[17] Article 12.1 of the ECD

authorities, VPNs, cloud infrastructure services, or CDNs that enable, locate, or improve the functions of other providers of intermediary services.[18]

From this wording, there still appears to be quite a large area of legal uncertainty as to whether these technical auxiliary functions are 'intermediary services'. The specificity of the DSA – compared to the other initiatives - is that these technical intermediaries primarily seem to be mentioned in the context of being able to benefit from the rules on the exemption of liability. Indeed, they only need to comply with a small number of additional rules[19], compared to their existing obligations and one may wonder if this justified including them in the DSA[20].

The recitals provide examples of services under the categories of mere conduit, caching (and hosting) services while also clearly stating that whether a specific service constitutes a mere conduit, caching or hosting service will **depend solely on its technical functionality that may evolve over time and should be assessed on a case-by-case basis**.[21]

Table 1 – Examples of services

Service category	Examples given in recitals of the DSA
Mere conduit	-Internet exchange points -Wireless access points -Virtual private networks -DNS services and resolvers -Top-level domain name registries, registrars -Certificate authorities that issue digital certificates -Voice over IP -Other interpersonal communication services
Caching	-Sole provision of content delivery networks -Reverse proxies -Content adaptation proxies
Hosting	-Cloud computing -Web hosting -Paid referencing services or services enabling sharing

[18] Recital 28 of the DSA
[19] In particular, having a point of contact to be contacted by member state authorities, the Commission and the EBDS and by recipients of services, elements to be included in their terms and conditions of use, and transparency reporting obligations.
[20] Recital 27 of the DSA clarifies that fighting illegal content online should not only focus on the liability and responsibilities of intermediaries but -where possible, third parties affected by illegal content online should attempt to resolve conflicts without involving intermediaries – and other actors such as group moderators in closed online environments should also help to avoid the spread of illegal content. Where intermediaries need to be involved, then requests should as a general rule be directed to the specific provider that has the technical and operational ability to act against specific items of illegal content.
[21] Recital 29 of the DSA

	-Information and content online, including file storage and sharing

By way of stark contrast, as explained by the UK's impact assessment of the OSB, **network infrastructure services are exempt from the OSB** because they do not have direct control over the user-generated content. This means that network infrastructure such as ISPs, VPNs, and CDNs as well as business to business services, where the business does not have control over specific pieces of content or activity are not covered by the OSB. However, they could be called on to assist with enforcement, for instance, to block non-compliant user-to-user services.

The **TERREG** clearly states that providers of mere conduit, caching or other services provided in other layers of the internet infrastructure, which do not involve storage such as registries and registrars, providers of domain name systems, payment or distributed denial of service protection services also fall outside the scope of the regulation.[22]

3.2.2. Pure online storage and distribution services are only covered in the DSA and OSB

Online storage and distribution are described by Hoboken et al (2019) as the classic hosting category i.e., as services that allow their users to store content online. Distribution is implied as storage only makes sense if the content can also be retrieved on demand at a later stage. File storage always offers a least a sharing feature for defined users. Services such as Dropbox and OneDrive clearly fall under this category.

The **TERREG** only covers hosting services that disseminate information to the public, whereas the **DSA** covers both types of hosting services, but more obligations are imposed on the hosting service providers that disseminate information to the public compared to those that do not present this functionality. Both EU laws refer to the classic definition of hosting services i.e., a service that consists of the storage of information provided by, and at the request of a recipient of the service.[23]

The **AVMSD** only covers services to the extent that they are offered to the general public, which seems to imply that pure storage services are not covered.

The **OSB** does not explicitly refer to online storage services, so the answer to the question of whether they are included is not entirely clear. However, the OSB has introduced an exemption for services used internally by businesses. This covers a service (or a distinct part of the service), managed by an organisation, whose primary purpose is to host members' UGC and enable interactions between members within that organisation. According to the impact assessment, this covers intranets,

[22] Recital 13 of TERREG

[23] For more discussion, see Madiega, T. (2020). Reform of the EU liability regime for online intermediaries: Background on the forthcoming digital services act, European Parliamentary Research Service; European Commission, Directorate-General for Communications Networks, Content and Technology, Hoboken, J., Quintais, J., Poort, J., et al., Hosting intermediary services and illegal content online : an analysis of the scope of article 14 ECD in light of developments in the online service landscape : final report, Publications Office, 2019, https://data.europa.eu/doi/10.2759/284542

customer relationship management systems, **enterprise cloud storage**, productivity tools, and enterprise conferencing software.[24]

The mention of this exclusion seems to indicate that if these services are used in a private capacity, they would not fall within the exempted category.

3.2.3. Search is in scope of the DSA and of the OSB but remains a grey zone in EU legislation

Search is only explicitly covered in the OSB and the DSA. Search was not explicitly included in the Commission's initial proposed DSA but is clearly in scope of the final text, although its legal categorisation is not entirely clear.

Generally, search is categorised as a 'selection and referencing' service which, next to search engines such as Bing or Google, may also include review or price comparison websites. Ever since the adoption of the ECD, which covers ISS, there has been a certain amount of legal uncertainty on the legal qualification of these location tools in the context mainly of the application of the liability provisions of the ECD. As summarised by Hoboken et al. (2019), they are not clearly covered in the ECD as hosting providers (under article 14).

Their legal treatment was therefore left to the Member States and the CJEU has applied the rules of article 14 to search, but only in relation to its paid advertising links. It remains unclear whether the provision of links outside of advertising (i.e., natural, or organic links) is covered by article 14 or by article 13, as proposed by the Parliament in its position on the DSA[25]. Some also argue that it is not the case as the ECD calls for the European Commission to examine and analyse if there is a need for proposals on the liability of providers of hyperlinks, implying therefore that they are not regulated under the directive (Nordemann, 2018: 15-16).[26]

Turning now to the **DSA**, an online search engine is defined (in line with the Platform-to-Business Regulation[27]) as an intermediary service that "allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found".[28]). The qualification of search engines (that are not very large) is not settled in the DSA. They could therefore be qualified as hosting service services or as caching services (for natural/generic search results).

---

24 Impact Assessment of OSB, para 67

25 Amendment 24 of adopted by the European Parliament on 20 January 2022 on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC. A new recital was proposed - not included in the final text - to specify that for example, a search engine could act solely as a caching service as to the information included in the results of an enquiry but that elements displayed alongside those results, such s online advertisements would however still qualify as a hosting service.

26 CJEU of 23 March 2010, joined cases C-236/08 to C-238/08 para. 110 – Google and Google France

27 Article 2 (5) of 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, p. 57–79

28 Article 3 (j)

The **TERREG** covers hosting service providers (consisting of the storage of information provided by and at the request of a content provider) insofar as they disseminate information to the public.[29] Regarding whether search is in or out of scope of the regulation, the same legal uncertainty remains as in the DSA, except that caching services are clearly out of scope of the TERREG, meaning that potentially only online paid-for or sponsored search results generated by search engines could be in scope.

The **OSB** is much clearer as it defines a search engine as a service or functionality that enables a person to search more than one website or database and they are clearly therefore in scope.

3.2.4. Online marketplaces are in scope of all initiatives (except AVMSD) but are more specifically covered in the DSA

Online marketplaces like Amazon or Vinted are in the **scope of all the initiatives, except the AVMSD**.

Here the **DSA** stands out, however: online marketplaces are qualified in legal terms as online platforms or possibly as VLOPS, but special obligations also apply to them ('online platforms allowing consumers to conclude distance contracts with traders').[30]

TERREG and the **OSB** do not have specific obligations regarding online marketplaces, but they are in scope.

3.2.5. Online gaming not explicitly mentioned in any of the legislations but may be in scope

Online gaming websites are not specifically mentioned in the instruments. This may be surprising as, for instance, Epic's Fortnite is reported to have 70m gamers per month worldwide.[31]

Some gaming platforms like Fortnite provide virtual concerts, talk shows, and social interactions, meaning that they would be considered as platforms in scope of the regulatory initiatives examined in this report either because they are U2U services under the OSB, or because they are hosting service providers, online platforms, or very large online platforms under the DSA, or because they are VSPs under the AVMSD[32]. They could also be qualified as hosting providers that disseminate information to the public under the TERREG.

The UK's impact assessment on the OSB does however highlight that there is considerable innovation in the gaming industry, and it anticipates that these innovations could develop into the creation of a digital metaverse, described as a virtual experience going beyond gaming to provide an array of media experiences[33]. It classes online gaming as the mid-risk risk category.

---

29 Article 1.2 of TERREG

30 These obligations are specified in articles 29-32 of the DSA and relate to the traceability of traders, the design of their interfaces (to allow traders to comply with their legal information requirements) and on the obligation to inform consumers if the platform becomes aware of the listing of an illegal product or service.

31 Tim Sweeney: Epic will fight Apple and Google to keep the Metaverse open, by Patrick McGee, 26 May 2022, https://app.ft.com/content/e13ce526-0e33-4ca2-9699-184d0138eada

32 Twitch for instance is a notified VSP in the UK.

33 Impact assessment, the Online Safety Bill, RPC-DCMS-4347(4), 31/01/2022, para 396

3.2.6. Platforms and websites with pornography are specifically addressed in OSB but not in EU legislation

The OSB stands out as it contains provisions to make sure that children are prevented from accessing pornography content, even if it is not user-generated. It therefore also covers any service which publishes pornographic content which can be accessed by users in the UK, thereby departing from the U2U and search service categories. It must be noted also that some of these services will also be regulated as audiovisual media services under the AVMS Directive.

These publishers will only need to comply with specific provisions and will not be in scope of the other safety rules. In essence, they will need to prevent children from accessing published pornographic content. For pornography on U2U services or generated by search, the general provisions of the OSB apply.

Contrary to what had been proposed by the European Parliament during the adoption process, the DSA does not contain special rules on platforms used for the dissemination of pornographic content[34] but these websites are covered by the DSA as online platforms or as VLOPS if they meet the required threshold. It does, however, contain a general requirement for online platforms that are accessible to minors to put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors on their services.[35]

3.2.7. Live streaming covered but without explicit provisions

Live streaming is sadly associated with the Christchurch terrorist attacks in New Zealand in 2019, which were live streamed on Facebook. It is also associated with the issue of piracy of live content, especially sporting events.[36] Live streaming also exposes users to particular dangers, for instance, it may reveal their location, and could lead them to be pressured into certain harmful behaviour such as sexual abuse or self-harm.

None of the instruments contain specific provisions on live streaming, but the AVMSD clearly mentions that live steaming is covered. There had been some attempts to introduce special rules in the DSA. In particular, the Internal Market and Consumer Protection Committee of the European Parliament had proposed that live streaming platforms should be specifically brought into the scope of the DSA.[37]

A resolution of the European Parliament adopted in May 2021, called on the European Commission (among other things) to tackle the online piracy of sports events that are broadcast 'live' by asking

[34] Amendment 291 adopted by the European Parliament on 20 January 2022 on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC. A new article was proposed - not included in the final text - to introduce additional obligations for platforms primarily used for the dissemination of user-generated pornographic content (e.g. to ensure that the identity of users that share such content are verified, that added standards of content moderation are used, and that a qualified notification procedure is available to signal cases of revenge porn.
[35] Article 28 of the DSA.
[36] Aavailable at https://www.europarl.europa.eu/doceo/document/TA-9-2021-0236_EN.html
[37] According to amendment 19 of the report, adopted on 20.12.2021, live streaming services are defined as information society services of which the main or one of the main purposes is to give access to audio or video material, that is live broadcasted to its users , which it organises and promotes for profit-making purposes. Available at https://www.europarl.europa.eu/doceo/document/A-9-2021-0356_EN.html

online intermediaries to remove, or disable access to infringing live sports broadcasts immediately, or as fast as possible, and in any event, no later than within 30 minutes of the receipt of the notification from rights holders or from a certified trusted flagger (para 12).[38] The Commission responded to this call by stating that it will "*set out, in the first half of 2022, the legislative or any other concrete actions that it intends to take to address online piracy of live content, including live sport event*".[39] The Commission announced in its 2023 workplan (published on 18 October 2022) that it intends to propose a non-binding recommendation on piracy of live content.[40]

It can also be noted that the UK government published guidance on how to improve the safety of online platforms in June 2021, including for live streaming.[41]

In the absence of specific provisions, the situation is therefore that live streaming events will be covered to the extent that they are provided by the intermediaries in scope (including search engines) but the general rules of the instruments apply, and no special procedures (such as live human content moderation) need to be followed to moderate illegal or harmful content which is live-streamed. In the context of risk assessments which will need to be carried out by VLOPS and VLOSES under the DSA and by the services in scope under the OSB, it is however possible that the services will need to deploy special risk mitigation measures to deal with specific harms that could arise in the context of live streaming.

[38] Available at https://www.europarl.europa.eu/doceo/document/TA-9-2021-0236_EN.html
[39] Response available at https://oeil.secure.europarl.europa.eu/oeil/spdoc.do?i=57210&j=0&l=en#:~:text=In%20the%20first%20half%20of,sport%20events%20(paragraph%2017) .
[40] Available at https://ec.europa.eu/info/strategy-documents/commission-work-programme/commission-work-programme-2023_en
[41] , ihttps://www.gov.uk/guidance/live-streaming-improve-the-safety-of-your-online-platform#how-to-design-safer-live-streaming

3.3. Summary table

Table 2 - Services in scope - summary table

	DSA	AVMSD	TERREG	OSB
Technical Internet services	Yes but grey zones	No	No	No
Search	Yes, but grey zones	No	Grey zone	Yes
Pure online storage	Yes	No	No	Grey zone
Online market places/app stores	Yes (special rules apply)	No	Yes	Yes
Online gaming	Not mentioned	Not mentioned	Not mentioned	Not mentioned
Porn publishers	No	No	No	Yes
Live streaming	Yes	Yes	Yes	Yes

3.4. Out of scope services, companies, and other exemptions

Beyond the services mentioned above, the initiatives also reveal other differences on the services that are either completely out of scope or that do not need to respect some of the rules, usually because of their small size.

3.4.1. Private messaging services mostly out of scope

Purely private messaging/communications services are excluded from the scope of all the instruments.

The **DSA** excludes interpersonal communications services from the definition of online platforms 'as they are used for interpersonal communication between a finite number of persons, which is determined by the sender of the communication. But they may apply to services that allow the making available of information to a potentially unlimited number of recipients, not determined by the sender of the communication, such as through public groups or open channels.[42] Despite not being considered online platforms, interpersonal communications services could perhaps also potentially still indirectly fall within the definition of mere conduit services under the DSA to the extent that

[42] Recital 14 of the DSA

service also consists of the transmission of information in the communication network. This interpretation would however have inconsistent consequences: it would exclude over-the-top (OTT) or -number-independent interpersonal communications services from the scope of the DSA altogether (as they don't provide transmission) whereas the number-based interpersonal communications services would be in scope.

The DSA and the **TERREG** both specify that where access to information requires registration or admittance to a group of users, that information should be disseminated to the public only where users seeking to access the information are automatically registered or admitted without a human decision or selection of whom to grant access. Interpersonal communications services as defined in the European Electronic Communications Code (EECC) such as emails or private messaging services should fall outside of the regulation.[43]

The OSB exempts (U2U and search services) from duties if the only type of user-generated content enabled by the service is respectively, an email, SMS and/or MMS messaging and one-to-one live aural communication services.

A case-by-case analysis will of course still need to be made to assess if very large group chats, which some messenger applications allow, are covered by the exemption.

Small-size companies

The **DSA** exempts micro and small enterprises[44] (except if they have been designated as VLOPS) from the additional obligations incumbent on online platforms (except that they need to respect the rules on the design and organisation of their online interfaces as well as the rules on the traceability of traders, right to information and compliance by design if they are providing an online marketplace) and from transparency reporting obligations.

The **TERREG** and **AVMSD** do not foresee any exemption for small-sized companies. But the TERREG states that when imposing penalties, the competent authority should take into account whether the hosting service provider is a start-up or a micro-, small-, and medium-sized enterprise.[45]

The **OSB**, like the AVMSD, provides that the measures to be taken must be proportionate to the size of the company providing the service. It does not exempt small-sized companies from its scope but does take a graduated approach based on reach and functionality.

3.4.2. Limited functionality

All of the legal instruments (except the TERREG) have rules to make sure that services that are confined to minor sharing functionalities are not covered. Unsurprisingly, these are defined

[43] Recital 14 of the TERREG, referring to Directive 2028/1972 of the European Parliament and of the Council of 11 December 2018, OJ L 321, 17.12.2018, p. 36
[44] Article 19 of the DSA which refers to definition in Annex to Recommendation 2003/361/EC.
[45] Recital 45 and article 18 2.(f) of TERREG

differently but they seek to capture inherently the same thing but may pose interpretation issues in practice.

Under the **DSA**, it is clearly specified that "if the activity of dissemination to the public of information is a minor or ancillary feature that is intrinsically linked to another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation", the service will not be considered as an online platform (but a pure hosting service).[46]

A recital explains that this is to avoid imposing overly broad obligations and covers for instance the comments section of an online newspaper, but that the storage of comments in a social network should be considered an online platform service, where it is clear that it is not a minor feature of the service offered, even if it is ancillary to publishing the posts of recipients of the service.[47]

The **AVMSD** also implicitly contains a limited functionality rule as the definition of a VSP refers to the 'principle purpose' or an 'essential functionality' criterion, as interpreted by the Commission's guidelines published in 2020.[48]

The limited functionality exemption under the **OSB**[49] states that a user-to-user service is *exempt* if the only ways users can communicate on the service are: by posting comments or reviews on the provider's content (content published on the service by or on behalf of the service provider); by sharing these comments or reviews on other internet services; by expressing views on the provider's content or on comments and reviews on the provider's content through: (i) a 'like or dislike' button, (ii) applying an emoji or symbol of any kind, (iii) engaging in yes/no voting or (iv) rating or scoring content; or by displaying or producing identifying content (e.g. usernames or avatars) in connection with any of these activities.

According to the explanatory statement, "this exempts services where the only user interaction is, for example, 'below the line' content on media articles, or user reviews of directly provided goods and services". Clause 49 then defines specific categories of such below the line content, such as comments and reviews on provider content and links to or images of news publisher content.

[46] Article 3 (i) of the DSA
[47] Recital 13 of the DSA
[48] Communication from the Commission Guidelines on the practical application of the essential functionality criterion of the definition of a 'video-sharing platform service' under the Audiovisual Media Services Directive 2020/C 223/02 C/2020/4322 OJ C 223, 7.7.2020, p. 3–9
[49] Para 4 of Schedule 1.

4. TREATMENT OF CERTAIN CATEGORIES OF CONTENT SUCH AS EDITED CONTENT OR 'PUBLIC INTEREST' CONTENT

When considering the treatment of edited content or public interest content, a distinction may be drawn between 1) whether (and if so how) content should be prominently displayed on the platform and 2) whether such content should benefit from a special derogation procedure and be moderated in a different way, compared to other types of content.

4.1. Prominence options

The **AVMSD** is the only legislation covered in this report that contains a provision on prominent display. A new article was introduced during the 2018 revision of the directive which gives the power to Member States to take measures to ensure the "appropriate prominence of audiovisual media services of general interest".[50] The AVMSD leaves much to be decided at a national level: the type of content to be covered (linear, non-linear, public service media (PSM) content, commercial content, etc.), the platforms to be covered (smart TVs, pay TV platforms, open internet platforms) and how prominence should be organised. A recital does specify that there should be designated general interest objectives such as media pluralism, freedom of speech, and cultural diversity. Also, the obligations should only be imposed where they are necessary to meet these general interest objectives, and they need to be proportionate.[51]

In September 2022, European Commission proposed in its European Media Freedom Act (EMFA) that users should have the right to customise audiovisual media offers by changing the default settings on devices and user interfaces to as to customise the content in accordance with their interests or preferences. Device manufacturers and developers will therefore be obliged to add functionality to allow this.[52] This does not, however, equate to prominence requirements for public interest content.

4.2. Special derogations option

The second area is whether the instruments contain some sort of exception or derogation to ensure that certain content such as the content edited by broadcasters or news publishers should be protected from removal by platforms, or at least should be subject to specific safeguards to protect media freedoms.

The arguments in favour of such a derogation are simple: much of this content is edited upstream by a press publisher or a broadcaster (including sometimes a public service broadcaster) and is therefore already subject to control and special (self) regulatory procedures, it would therefore be excessive for platforms to exercise a supplementary control and potentially to take such content down. Procedures already exist to challenge the content. On the other side, some damaging content may also originate from news publishers, and they can also be hard to distinguish from other content creators, so the exemption could grant legal protection or at least a safe haven to those wanting to disseminate

[50] Article 7a of the AVMSD.
[51] Recital 25 of the AVMSD.
[52] Article 19 of European Commission's proposal for a regulation establishing a common framework for media services in the internal market (European Media Freedom Act) and amending Directive 2010/13/EU, 2022/0277 (COD).

harmful content. Furthermore, the contours of such an exception may be difficult to frame. Unsurprisingly therefore we see a patchwork of solutions emerging.

At the EU level, none of the instruments contain specific exemptions, except for the TERREG.

The **TERREG contains a clear exception, but some of its contours may be a bit vague and could be subject to interpretation**. What is striking is that the exception is wide, since the regulation does not apply to "material disseminated to the public for educational, journalistic, artistic or research purposes or for the purposes of preventing or countering terrorism, including material which represents an expression of polemic or controversial views in the course of public debate".[53] The regulation specifies that this content is not considered to be terrorist content. So, the exception could cover content coming from many sources. The regulation foresees that an "assessment shall determine the true purpose of that dissemination and whether material is disseminated to the public for those purposes".[54] There is however no indication as to who needs to undertake this assessment and under what control.

There were **attempts to include a specific derogation in the DSA but finally, it was not included**. In particular, the Culture and Education Committee of the European Parliament had proposed amendments to introduce a special regime for editorial content providers, that would have been defined as "a natural or legal person who has editorial responsibility for the content and services they offer, determines the manner in which the content and the services are organised, who is subject to sector specific regulation, including self-regulatory standards in the media and press sectors, and has put in place complaints-handling mechanisms to resolve content-related disputes".[55] The idea was to prohibit intermediation services from moderating (removing, disabling access, or otherwise interfering) content or services made available by these editorial content providers (or to disable their accounts).

However, the DSA does foresee two elements worth noting and which show that media content and 'public interest' content are of special importance.

First, intermediaries need to apply their terms and conditions (which need to specify their content moderation practices) "with due regard to the rights and legitimate interests of all parties involved, including the fundamental rights of the recipients of the service, such as the freedom of expression, freedom and pluralism if the media, and other fundamental rights and freedoms as enshrined in the Charter".[56] This provision gives no guidance on how platforms need to apply this provision or to the situations to which it could apply in practice.

The other provision is on the risk assessments (and risk mitigation measures) that need to be carried out by the VLOSEs and VLOPs. It obliges them to assess 4 categories of risks and two of these are

[53] Article 1.3 of the TERREG.
[54] Article 1.3 of the TERREG.
[55] Amendments 67 and 79 of the CULT Committee Opinion, 5.10.2021, available at https://www.europarl.europa.eu/doceo/document/CULT-AD-693943_EN.pdf
[56] Article 14.4 of the DSA.

related to the dissemination of certain categories of 'public interest' content: any actual or foreseeable negative effects for the exercise of fundament rights, in particular "(…) freedom of expression and information, including the freedom and pluralism of the media (….)" ; and "any actual or foreseeable negative effects on civic discourse and electoral processes, (…)".[57] If the platform identifies that such risks, linked in particular to the design of their recommender systems or other algorithms they may use, their content moderation systems or their terms and conditions exist, they will need to take risk mitigation measures, which may imply modifying any of these elements. As an example, the DSA mentions specifically the possibility to adapt their content moderation processes. Commission guidance could be adopted by the Commission in particular to present best practices and recommend possible measures.[58]

The Commission's proposed EMFA contains special rules to make sure that VLOPS (as defined in the DSA) respect the editorial integrity of media services. In particular, these very large online platforms would need to provide a statement of reason **before** they take down (delist, suspend, etc.) their content and make sure that any complaint is processed and decided with priority and without undue delay. A dialogue between media service providers that consider that their content is frequently restricted or suspended and VLOPS would also need to take place. The EMFA proposal sets criteria for determining which media services would enjoy this special treatment. The media service providers that would benefit from these rules are those that provide a media service (i.e. audiovisual, audio, press) with editorial responsibility if they are independent from Member States' and third countries' governments, and subject to regulatory requirements in at least one member state or subject to co- or self-regulatory editorial standards that are widely recognised and accepted in a member state.[59]

The OSB contains an explicit carve-out for news publishers and audiovisual media services (holder of broadcast licences or registered on-demand services). It establishes specific communications offences for users of online services related to harmful or false communications, but news publishers and audiovisual media services cannot be considered to have committed these communications offences defined in the Bill.[60] This means that ordinary users, or even small-scale publishers that do not meet the criteria to be classed as news publishers under the Bill, may be prosecuted for messages or images that can be freely disseminated by news publishers**.**

The OSB also states that Category 1 U2U services will need to put in place systems and processes to ensure the importance of the free expression of "content of democratic importance" and of "journalistic content" when making decisions about how to treat such content.

The Bill defines content of democratic importance as content from a news publisher or regulated audiovisual media service, or content that "is or appears to be specifically intended to contribute to democratic political debate". [61] According to the bill, it would be up to service providers to identify

[57] Aricle 34 of the DSA.
[58] Article 35.3 of the DSA.
[59] Articles 17 and 18 of the proposed EMFA.
[60] OSB Clauses 151(6) (harmful communication); 152(4) (false communication)
[61] OSB Clause 15(6)(b)

what content fits into the category of democratically important content. For such content, Category 1 services should ensure freedom of expression is considered when making decisions about removing content or taking actions against users uploading such content.[62] Arguably this should always be taken into account, and the Bill further specifies that the systems and processes adopted by Category 1 services for content of democratic importance should be applied to a wide diversity of political opinions. Nevertheless, the definition, on the one hand, favours well-established media and, on the other, contains significant vagaries that require the services to play what is essentially an editorial role. Services might be incentivised to identify only well-recognised speakers that clearly are engaged in political debate, such as known politicians and major civil society groups.

The definition of journalistic content in the OSB is somewhat clearer. It is content from a news publisher or regulated service, content generated for the purpose of journalism **«**and linked to the UK**».**[63] Linkage to the UK can be determined based on the content being of interest to a significant number of UK users, which means that arguably most international content would still qualify, but Category 1 service providers will need to include in their terms their methods for determining what qualifies. Category 1 services will need to ensure that freedom of expression is taken into account in decisions about removal of content or action against uploaders of journalistic content. They will also have to put in place a « dedicated and expedited complaints procedure » to ensure that content moderation decisions about a particular piece of journalistic content can be challenged.[64]

Although according to the explanatory notes, journalistic content includes that created by freelance journalists and citizen journalists, these would have to be based in the UK or working for British media to take advantage of the privilege. With the determination of who qualifies reliant on not only determining the purpose of the content and the location or affiliation of the source, but it could also become difficult for those not easily identifiable as news publishers to access this privilege. Overall, as has been argued consistently by Article 19 and others (Harbinja & Leiser, 2022), the definition of news publishers and treatment of them in the OSB in the ways the journalistic privileges have been constructed risk entrenching the power of large media that are already established news publishers at the expense of media pluralism.

[62] OSB Clause 15(2)
[63] OSB Clause 16(8)
[64] OSB Clause 16(3)

5. HARMS IN SCOPE

This section is divided into different categories of harms to ease the comparison between the texts. The first category of harms covers those that occur because of the production and dissemination of illegal content online. Illegal content refers to content, activities, and products that do not comply with the law and or which may constitute a criminal offence. Content can be illegal itself, such as a - hate-inciting message, or can be illegal due to the illegality of the behaviour of its creation or dissemination. As discussed below, the OSB would create new criminal offences related to the behaviour and intention of its dissemination. For example, an image of female breasts may not be illegal ordinarily but if such an image is shared without consent in a jurisdiction where the sharing of intimate images without consent is a criminal offence, then such an image is illegal. As this section will show, this is not a straightforward category.

The harms that belong to the second category stem from content that is legal, therefore their creation and dissemination do not constitute an offence. For example, violent content or falsehoods are generally not illegal, but can be harmful to certain audiences, groups, or contexts. It is in this category where the balancing of the potential harm from the dissemination of the content with any harm that might arise from the prohibition or removal of content is arguably most delicate. These harms may be to individual speakers or receivers or to wider society. In this category, we see significant differences in approaches across the pieces of legislation.

5.1. Illegal content

The next point of comparison is on the types of illegal harms addressed by each piece of legislation. Here again, we see important differences which – at least for the DSA, OSB, and AVMSD – add a layer of complexity.

It is very clear that the **DSA stands out as having the widest scope**. It covers illegal content, defined as any information that does not comply with Union law or the national law of any member state, irrespective of the precise subject matter or nature of the law. It covers information itself, as well as any activity such as the sale of a product or the provision of a service.[65]

A recital provides some guidance that shows the true breadth of what is covered: what is illegal offline is illegal online, as the notion should "should broadly reflect the existing rules in the offline environment".[66] Recital 12 further clarifies that the concept should be understood to refer to information, irrespective of its form, that under the applicable law is either itself illegal (like illegal hate speech or terrorist content), or that the applicable rules make illegal because it relates to activities that are illegal. Illustrative examples include the sharing of images depicting child sexual abuse, unlawful non-consensual sharing of private images, online stalking, the sale of non-compliant or counterfeit products, the sale of products or the provision of services in infringement of consumer

[65] Article 3 (h) of the DSA.
[66] Recital 63 of the DSA

protection law, the non-authorised use of copyright-protected material, the illegal offer of accommodation services or illegal sale of live animals.[67]

Of crucial importance, the DSA alludes to an element that will no doubt lead to debate: if the illegality of the information or activity results from national law, that national law should comply with Union law. This element that only the breaches of national laws, which themselves comply with European Union law should be upheld by the DSA, was also debated during the adoption process of the DSA. It is quite possible that some national laws are not aligned with EU law, including with the EU Charter on Fundamental Rights. No doubt also that this element will put platforms, citizens, and courts in an uncomfortable position as there is no indication as to how to assess whether the national laws comply with EU laws. Should this be done by the platforms themselves? Would this be a matter for courts to decide? For example, if a Member State criminalises speech related to LGBTQ+ rights, would the platform need to take measures appropriate to illegal content? Could it decide that this was not in line with EU law, or would it need to comply until a citizen or group established the conflict with EU law at the CJEU?

In short, the DSA puts criminal offences such as child sexual abuse or failure to provide pre-contractual information to protect consumers into the same category. Of course, increasingly European law makers are adopting specific legal instruments to deal more specifically and sometimes more rapidly with the online spread of particularly damaging forms of offences such as terrorist content or child sexual abuse. Nevertheless, because the scope of application of the DSA is so wide, this could pose application problems. Platforms could receive huge numbers of notices and they will all require a follow-up. This could potentially undermine or slow up the treatment of more serious cases involving criminal offences, which should perhaps be treated with priority.

Having said that, the DSA does refer to the concept of "manifestly illegal content" – which is "where it is evident to a layperson, without any substantive analysis, that the content is illegal" – in the context of allowing online platforms to suspend the accounts of those that frequently post such content. [68]

Lastly, the DSA also provides that hosting service providers (and hence also all online platforms, VLOPS, and possibly VLOSEs) need to report suspicions of serious criminal offences to law enforcement or judicial authorities. This should be done when the service providers become aware of any information giving rise to a suspicion that a criminal offence, involving a threat to the life or safety of a person or persons has taken place, is taking place, or is likely to take place.[69] A recital gives a few examples of the types of offences such as incitement to terrorism.[70]

The **AVMSD has a much narrower scope of application**. VSPs need to take appropriate measures to protect the general public from content that contains a) incitement to violence or hatred directed against a group of persons or a member of a group, based on any of the grounds referred to in article

[67] Recital 12 of the DSA.
[68] Article 23 and recital 63 of the DSA.
[69] Article 18 of the DSA.
[70] Recital 56Terr of the DSA.

21 of the EU Charter on Fundamental rights[71]; b) content which if it is disseminated constitutes an activity which is a criminal offence under Union law (i.e. the public provocation to commit a terrorist offence, offences concerning child pornography, and offences concerning racism and xenophobia.[72] The AVMSD also requires VSPs to protect minors from content that could impair their physical, mental or moral development. Most of this will not be illegal content per se if viewed by adults, however, in some jurisdictions, certain content can be illegal when accessed by minors. An important limiting factor to the AVMSD is that only video content is covered.

T**he TERREG has the narrowest scope of application since it 'only' aims to address the dissemination to the public of terrorist content online**. The TERREG refers to the definitions of terrorist offences defined in Directive 2017/541 on combating terrorism, and which obliges the Member States to criminalise these offences**.**[73]

All types of content are covered (text, image, video, etc.) so long as it:

- incites the commission of one of the offences linked to terrorism where it directly or indirectly advocates the commission of terrorist offences, thereby causing a danger that one or more such offences may be committed;
- solicits a person or a group of persons to commit or contribute to the commission of one of the offences;
- solicits a person or a group of persons to participate in the activities of a terrorist group;
- provides instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific methods or techniques for the purpose of committing or contributing to the commission of one of the terrorists offences;
- constitutes a threat to commit one of the terrorist offences.

The **OSB distinguishes between priority illegal content and other illegal content.** The illegality of any content is based on its association with a criminal offence, however, the OSB specifically excludes offences related to infringement of intellectual property, product safety, and other offences related to consumer protection as being relevant to its definition of illegal content.[74] Its definition of illegal content includes three categories of priority illegal content and content linked to an offence not within the priority categories "of which the victim or intended victim is an individual (or individuals)".[75] For this non-priority illegal the duty of user-to-user services is to include it in their risk assessments and to take "proportionate measures to effectively mitigate the risk of harm to individuals".[76] For priority

[71] Article 21 of the EU Charter on Fundamental Rights refers to any ground such as such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation

[72] All of these criminal offences are foreseen in EU legislation: respectively in Article 5 of Directive (EU) 2017/541, Article 5(4) of Directive 2011/93/EU, Article 1 of Framework Decision 2008/913/JHA.

[73] Article 3 of Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA *OJ L 88, 31.3.2017, p. 6–21*

[74] OSB cl. 52(8)

[75] OSB cl. 52(4)

[76] OSB cl. 9(2)

illegal content, their duty is to use proportionate systems and processes to prevent users from encountering it, minimise its presence and take it down swiftly.[77]

As defined in the OSB, priority illegal content mostly derives its illegality from criminal offences in existing legislations. The definition[78] includes terrorist content, based on criminal offences in terrorism and serious crimes laws set out in schedule 5, and child sexual exploitation and abuse content, based on a number of laws on sexual offences and child protection set out in schedule 6. The category of priority illegal content also includes content related to a list of "priority offences" listed in schedule 7:

- Assisting suicide
- Threats to kill
- Public order – harassment, stalking, fear of provocation of violence
- Supplying of drugs
- Dealing in firearms
- Assisting illegal immigration
- Sexual exploitation
- Extreme or private sexual content
- Concealing or acquiring criminal property
- Fraud
- Unauthorised or false financial services

A government-proposed amendment would add foreign interference, understood as "covert attempts by foreign state actors to manipulate our information environment" to this list.[79] These priority offences indicate several acts that can result in harm to individuals as well as indirect consequences for society more widely, for example to public health or safety. Only the foreign interference one, if added as proposed, would address wider societal harm to democratic processes like those addressed in the DSA, where such is treated under legal harms (see below).

The OSB also establishes three new communications offences for harmful, false, and threatening communication, and introduces an offence into the Sexual Offences Act for the sending of photographs or films of genitals for the purpose of causing harm (cyberflashing). These provisions in the OSB are in line with the recommendation of The Law Commission (2021), which was concerned about harm from over-criminalisation of communication that exists in current UK law and the need to include certain behaviour that has emerged with recent online services.

As Lorna Woods, one of the two architects of the duty of care approach taken by the OSB has argued, the harmful communications offence is not entirely new, but shifts the focus of the offence from the content to the harm that is caused.[80] Whereas the 2003 Communications Act establishes an offence

[77] OSB cl. 9(3)
[78] OSB cl. 52(7)
[79] See statement of Secretary of State 07 July 2022 https://questions-statements.parliament.uk/written-statements/detail/2022-07-07/hcws193
[80] https://essexlawresearch.blog/2022/07/15/the-new-harmful-communications-offence-and-the-online-safety-bill/

based on whether the message is "grossly offensive or of an indecent, obscene or menacing character"[81], the OSB bases the offence on whether there was a risk of harm, defined as "psychological harm amounting to at least serious distress"[82]. The false communication offence essentially rewords an offence already present in the Communications Act[83] and is based on knowledge that the information is false and the intention to cause "non-trivial physical or psychological harm to a likely audience"[84]. Threatening communication offences are defined in the OSB as the sending of messages conveying a threat of death or serious harm, including grievous bodily harm, rape, penetrative assault, or serious financial loss[85]. As was recommended by the Law Commission, the offences do not require establishing what constitutes indecent or offensive content but whether serious harm, a category defined in other law, was a risk or threats of specific categories of harm were made. All these communications offences aim to prevent harm to individual users, or members of a likely audience for the content disseminated by an offender.

The OSB imposes a duty of care on all services in scope to conduct illegal content risk assessments and then to use proportionate systems to prevent users from encountering and limit the presence of priority illegal content. Unlike the EU laws, which all maintain a ban on monitoring, the OSB essentially requires this in relation to illegal content and places the onus on service providers to determine whether the content is illegal and remove it, including through proactive technology (see Coe, 2022).

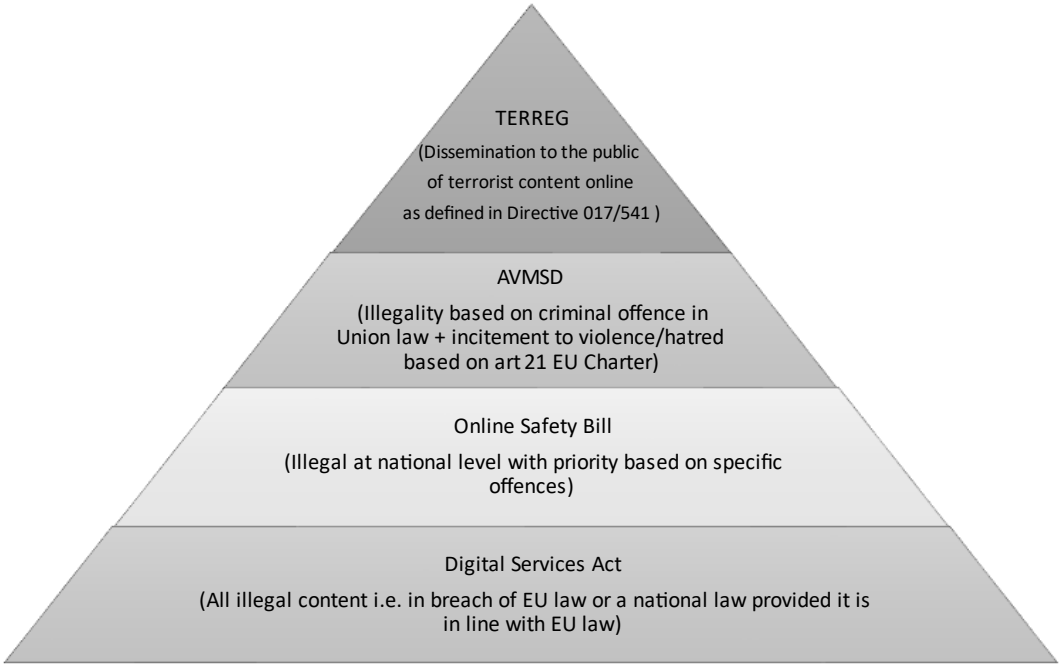

Figure 4. Relative breadth of illegal content in scope in each piece of legislation

[81] 2003 Communications Act cl. 127
[82] OSB cl. 151(4)
[83] 2003 Communications Act cl. 127(2)
[84] OSB cl. 152(1)
[85] OSB cl. 153

The DSA covers the widest scope of illegal content. This reflects its EU level and horizontal nature, but also results in a need to clarify the process, and associated responsibilities, dealing with situations when a Member State's law may conflict with EU law. Though the UK is no longer an EU Member State, the OSB provides an example of how a state can establish illegal content. The OSB defines illegal content with reference to specific offence and introduces new offences. The list covers a diversity of offences and can be added to, giving it still a broader scope than the AVMSD. The OSB can therefore be seen as an example of the type of detailed legislation that might be expected at the national level among some EU Member States as well and would then constitute illegality under the DSA.

The AVMSD requires protection from content that is illegal because disseminating it constitutes a crime at the Union level. This means its scope is narrowed to specific very serious crimes. According to Article 83 of the TFEU, the EU can adopt what would essentially be criminal law only in ten specific areas, among which are terrorism and sexual exploitation of women and children. Speech that amounts to incitement to violence or hatred is also unprotected, or illegal, as discussed above. TERREG is exactly the kind of EU law that clarifies the criminality of specific types of content based on the EU's competence in combatting that type of crime. The proposed regulation to prevent and combat child sexual abuse would play a similar role.[86] Therefore, although the DSA does not indicate a hierarchy of illegal harms, the EU-level priorities can be seen in the AVMSD, TERREG, and the expected regulation covering CSAM, as well as the 2008 Framework Decision on Combatting Certain Forms of Expressions of Racism and Xenophobia[87] and other acts.

5.2. Harmful but legal content

In addition to addressing illegal content and behaviour, **all but the TERREG also aim to prevent a variety of harms that can occur from content and behaviour that is legal**. In this section, we first cover the overall approach to what for brevity's sake we will refer to as legal harms. The AVMSD, DSA, and OSB all directly aim to prevent legal harms, while the TERREG addresses harm to fundamental rights as something that must be avoided in the implementation of measures it imposes to prevent the legal harms. We will take in turn each of the main areas of legal harms.

Only the OSB defines harm explicitly, and it does so in a manner that seems to understand harm as being in relation only to individual service users. Clause 190 states that "'Harm' means physical or psychological harm" and then elaborates on the possible causes and circumstances in which harm might occur. Harm can arise from the nature of the content; the fact of its dissemination; or the manner of its dissemination. Dissemination to the public is not a necessary condition for this understanding of harm. It can be from "content repeatedly sent to an individual by one person or by different people".[88] The circumstances for harm given in the OSB make it even clearer that the Bill is

[86] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse COM/2022/209 final: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN
[87] Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33178
[88] OSB, cl. 190(3)

concerned with harm to individuals. Clause 190 (4) states that references to harm include ones that arise:

> *(a) where, as a result of the content, individuals act in a way that results in harm to themselves or that increases the likelihood of harm to themselves;*
>
> *(b) where, because of the content, individuals do or say something to another individual that results in harm to that other individual or that increases the likelihood of such harm*

Although the harm to an individual can be related to that individual's membership in a group, the OSB does not appear to address collective harms to groups, such as the silencing of minority voices due to persistent use of derogatory language or abuse, or harm to a political party and arguably a wider constituency, from a disinformation campaign in an election.

Though it does not explicitly define harm or circumstances in which it can take place, the AVMSD is similarly concerned with harm to individuals from content. The AVMSD has long been concerned with harm to minors from content. The Directive defines this as impairment of "the physical, mental or moral development of minors"[89] . The recitals of the most recent amending Directive (2018/1808), which expanded its scope to include video-sharing platforms, refer to protecting minors and "all citizens"[90] or "the general public"[91]. Although in one reference to protecting minors and the general public on video-sharing platforms, both harmful content and hate speech are lumped together[92], in other references and in the articles the general public is to be protected from illegal content while minors are to be protected from wider legal harms. The one exception to this is in relation to commercial communication, which will be elaborated on below.

The DSA takes the broadest approach to harm. The DSA is designed to prevent harm to individuals as fundamental rights and consumer protection are mentioned in the aim statement in Article 1. However, it is only in relation to VLOPs and VLOSEs that these are really incorporated. For VLOPs and VLOSEs the Act is also concerned with "economic and societal harms"[93]. It openly addresses the potential for collective harm from digital services, for example through discriminatory or manipulative advertising that "can negatively impact entire groups and amplify societal harms"[94]. For VLOPs and VLOSEs, the DSA requires assessments of the systemic risk of an extensive list of potential harms[95], some of which relate to individuals or groups (even when they are not users of a service) and others of which are *public harms*. As discussed in a previous CERRE report, (Broughton Micova, 2021) public harms are ones to public institutions or processes, such as elections or service delivery.

The DSA's systemic risk approach is revolutionary as it requires the large platforms and search engines to consider not just harm from content but also harm that can stem from their functionalities and

[89] Art. 6a, AVMSD (Directive 2010/13 as amended by 2018/1808)
[90] Recital 4 of Directive 2018/1808 amending the AVMSD
[91] Recitals 18&44 of Directive 2018/1808
[92] Recital 45 of Directive 2018/1808
[93] Recital 79 of the DSA
[94] Recital 69 of the DSA
[95] Art. 34 of the DSA

arguably even their ways of doing business. Most of the harms to be covered in systemic risk assessment by VLOPs and VOSEs under the DSA are legal harms, but fundamental rights are at stake and mitigation could require significant measures, such as age-appropriate design or changes to approaches to targeted advertising.

5.2.1. Harms to minors

The AVMSD, the DSA, and the OSB all deal with the protection of minors from legal harms in addition to their protection from the illegal content and behaviour discussed above. The approach of the AVMSD is the oldest as it dates to its predecessor, the 1989 Television without Frontiers Directive. Across all three of them, there is an assumption that certain content that is fine for adults can be harmful to children and that the regulated services must take action to limit the chances of minors encountering such content. There is an emphasis in all three on design features and functionalities as means for achieving this.

The AVMSD requires Member States to ensure that audiovisual media services that might be harmful to minors take measures such as broadcast timing, age verification, or other technical measures[96]. For example, technical measures might include placement in the electronic programme guide, signal encoding, or other deterrents. Audiovisual media services that carry any programmes that might be harmful to minors must provide information to viewers on these[97]. An example of this would be a standardised rating system and symbols that indicate the presence of violence, nudity, and adult language. The AVMSD also requires Member States to ensure that video-sharing platforms take measures to protect minors from programmes, user-generated content, and commercial communications that might harm them[98]. The Directive lists several measures, of which rating functionalities and age verification are like those expected for audiovisual media services and parental controls are specific to video-sharing platforms.

The DSA takes a similar approach to the AVMSD. Following a considerable amount of debate, the **DSA only places a general obligation on online platforms to ensure a high level of privacy, safety, and security of minors**.[99] The DSA additionally requires providers to make sure that their terms and conditions are understandable for minors if their service is widely used by them. In particular, the lead committee in the European Parliament had adopted an amendment specifying additional technical and organisational obligations to be taken by platforms "primarily used for the dissemination of user-generated pornographic content".[100]

The protection of minors is also covered in the systemic risk assessments that must be conducted by VLOPs and VLOSEs. The areas of risk for which must conduct assessments, listed in Article 34 of the DSA includes "any actual or foreseeable negative effects on…the rights of the child". This is a broad-brush obligation that has the potential to cover not only the protection from exposure to harmful

[96] Art 6a(1)) of the AVMSD
[97] Art. 6a(3) of the AVMSD
[98] Art. 28b(1)
[99] Article 28 of the DSA.
[100] Amendment 291, report of the Committee on the Internal market and Consumer Protection, adopted on 20.12.2021, available at: https://www.europarl.europa.eu/doceo/document/A-9-2021-0356_EN.html

content, but also any harm that could come from constraining or impinging on the rights of children to create and express, as well as their rights to digital literacy and education (Livingstone et al., 2020). The DSA also requires these large services to undertake measures to mitigate the risks identified. Among those measures suggested are generic adaptations to design, terms of conditions, and content moderation that can certainly be done in the service of mitigating risks to minors. Also included are the more specific age verification, parental controls, and tools for minors to signal abuse or access help.[101] The UN's interpretation of the Convention on the Rights of the Child in relation to online services[102] identifies the need to address design features, prevent discrimination in terms of access, enable specific spaces for expression, and other elements that could be considered relevant to a systemic risk assessment. Therefore, the scope of legal harms to minors covered by the DSA could be interpreted as being quite broad and the expected measures to be taken to mitigate risk of those harms quite wide-reaching.

The **OSB would require a children's risk assessment of all services that are likely to be accessed by children[103]**. Ofcom will have to prepare a risk profile for this type of harm providing more detail on the scope. However, the details already present in the Bill indicate that the concern is primarily about exposure to harmful content, but also potentially harmful behaviour. The assessments are supposed to consider the extent of dissemination of content, the level of harm posed by the content, and the extent to which design or functionalities can limit exposure to content. They should also cover whether adults can contact each other or minors and the ways the service is used. The Bill would require all the considerations of risk to be broken down by age group. In line with its "duty of care" approach, the OSB would then institute safety duties to protect children from the risks identified in the assessments. Providers of online platforms would have to take "proportionate measures" to mitigate the risks and impact of harm and "proportionate systems" to prevent children from encountering harmful content. The list of suggested systems resembles the measures suggested by the AVMSD and the DSA. It includes age verification, parental controls, terms, content moderation, design features, and user support measures. The OSB also would require that any providers of pornographic content ensure that it cannot be accessed by children by using age verification and other tools[104].

5.2.2. Minors and commercial communications

The two pieces of EU legislation also recognise that minors may be at particular risk from some forms of commercial communication. The **AVMSD specifically bans commercial communication that may directly target minors** by "exploiting their inexperience or credulity" or, "directly encourage them to persuade their parents or others to purchase the goods or services being advertised, exploit the special trust minors place in parents, teachers or other persons, or unreasonably show minors in

[101] Article 35 (j) of the DSA.
[102] General comment No. 25 (2021) on children's rights in relation to the digital environment adopted on 02.03.2021 available at : https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/053/43/PDF/G2105343.pdf?OpenElement
[103] OSB cl. 10
[104] OSB cl. 69

dangerous situations".[105] It also prohibits advertising alcoholic beverages to minors or in a way that encourages immoderate consumption.[106]

Minors in the EU cannot be the objects of targeted advertising based on profiling or behavioural advertising. The AVMSD explicitly bans the use of the personal data of minors for commercial purposes including direct marketing, profiling, or behavioural advertising. This applies to both audiovisual media services and video-sharing platforms.[107] The **DSA** bans advertising based on profiling or the use of personal data if there is an indication that the user of an online is a minor.[108] Online platform providers are not allowed to process additional personal data in order to determine this, however.

The **OSB does not specifically address commercial communications towards minors, profiling of minors for commercial purposes, or the use of minors' personal data**. Its clause on safety duties to protect children refers to the duties regarding freedom of expression and privacy, which require providers to have the rule of law concerning privacy including on the processing of personal data[109]. Since the UK's data protection rules are still in line with GDPR and the UK has transposed the AVMSD in full, this means that those limits on the processing of minors' personal data for commercial purposes would be included, for the VSPs at least.

5.2.3. Harm to others from commercial communications

The three pieces of legislation that cover legal harms all address commercial communications, but they do so in very different ways.

The **AVMSD requires commercial communication to be identifiable and sets out qualitative standards for advertising content**. These standards include prohibitions on promoting discrimination and on prejudicing human dignity, public health, and the natural environment. They also include bans on the advertising of tobacco products, prescription medicines, and limits on advertising alcoholic beverages.[110] Audiovisual media services and VSPs must ensure that all commercial communications that they sell comply with these rules, and therefore bear direct responsibility for that commercial communication. VSPs also must also take measures to ensure that the commercial communications sold by others using their platform comply.[111] Such measures could be explicit terms and conditions, functionalities enabling self-declaration of sponsorship or other commercial communication, user flagging tools, and others. VSPs are held responsible by regulators for the appropriateness of the measures. The rules in the AVMSD are rooted in long-standing assumptions about the power of advertising, especially on broadcast media, to influence the public. Most of the rules have been in place since earlier versions of the Directive when they only applied to television.

[105] Article 9(1)(g) of AVMSD.
[106] Article 9(1)(e) of AVMSD.
[107] Article 6a(2) &28b(3) of AVMSD.
[108] Article 28 (2) of the DSA.
[109] OSB cl. 19
[110] Article 9(1) of AVMSD.
[111] Article 28b of AVMSD.

The **DSA is primarily concerned with the transparency of commercial communications and the ability of users and regulators to access usable information on the source of an advertising**, i.e., to know on whose behalf it is presented. The understanding of the potential harm the transparency measures aim to address is given in Recital 68 "online advertising can contribute to significant risks, ranging from advertisements that are themselves illegal content, to contributing to financial incentives for the publication or amplification of illegal or otherwise harmful content and activities online, or the discriminatory presentation of advertising with an impact on the equal treatment and opportunities of citizens". The DSA also makes it clear that the advertising systems of VLOPs and VOSEs can contribute to the systemic risks posed by these services and therefore the nature and design of these systems should be considered in risk assessments.[112] All online platforms that carry advertising must provide real-time information to recipients of the advertising on who paid for it, on whose behalf it is placed, the basis upon which they are receiving it (e.g. context, targeting parameters).[113] None of the targeting of ads can be based on sensitive personal information.

The **OSB recognises consumer harm from fraudulent advertising but does not deal with other issues related to commercial communication**. It requires services to take proportionate measures to prevent users from encountering fraudulent advertising and to remove it swiftly when reported[114]. It encourages technical means for achieving this while requiring some transparency about the technologies used. It takes a content-based approach to a limited type of harm from commercial communication, which is very different from the approach of the DSA which recognises the risks of harm from commercial functionalities such as those related to the targeting or trading of online advertising.

5.2.4. Freedom of expression

Threats to freedom of expression and to freedom and pluralism of the media are legal harms dealt with by the TERREG, which otherwise is focused on preventing harm from illegal terrorist content. Its Recital 10 argues that "Effective online measures to address terrorist content online and the protection of freedom of expression and information are not conflicting but complementary and mutually reinforcing goals". The provisions however seem to be directed at ensuring that the latter is not collateral damage to the former. Other Recitals acknowledge the importance of freedom of expression to open and democratic society and the role that hosting services play in facilitating public debate. The TERREG seems to be concerned more about societal harm from cumulative or systematic impingement on freedom of expression than about harm to any one individual's rights but does recognise the need for individuals to have recourse. The provisions of the regulation treats harm to expression as something that must be balanced with the Regulation's aim of preventing harm from illegal content and something to be considered in measures such as identifying and removing terrorist content.[115] Complaints mechanisms are required as a protection against harm to individuals' freedom

[112] Recitals 88 & 95 of DSA.
[113] Article 26 of DSA.
[114] OSB cl. 34 & 35
[115] Articles 1 & 5 of TERREG.

of expression[116], and these must be reported by the service providers on and monitored by the competent authority[117].

The 2018 Directive that amended the **AVMSD** to include VSPs also explicitly states that **the measures taken by platform providers to prevent harms to minors and to all from illegal content must be balanced with fundamental rights**, including freedom of expression and privacy.[118] It further refers to freedom of expression in combination with media pluralism and linguistic diversity as things that Member States must ensure are not impinged by any measures taken.[119] Although its articles do not mention freedom of expression directly, the AVMSD requires VSP providers to ensure there are «transparent, easy-to-use and effective procedures for the handling and resolution of users' complaints».[120] The appropriateness of these must be assessed by national regulatory authorities.

The **DSA takes wide reaching approach to freedom of expression**. In line with the other two pieces of EU legislation, it also requires measures taken to prevent other types of harm to avoid impinging on recipients' freedom of expression. Providers are instructed to take care not to impinge on recipients' fundamental rights and they are especially called upon to consider freedom of expression in the implementation of measure such as content removal and in the assessment of risk.[121] The DSA also addresses the potential for wider societal harm related to constraints on freedom of expression. When designing restrictions, providers, especially VLOPs "should in particular pay due regard to freedom of expression and information, including media freedom and pluralism".[122] VLOPs and VLOSEs must conduct assessments on their systemic risk to freedom of expression and information, including freedom and pluralism of the media, and on potential negative effects on civic discourse and electoral processes.[123] There is a clear recognition that there can be collective harm related to freedom of expression conceived as a positive right, not just about avoiding constraints on speech but also about ensuring access to diverse information and platforms for exchange (Kenyon, 2021a; Kenyon & Scott, 2020). How these obligations will be interpreted in the implementation of risk assessments will further determine the extent of the understanding of harm VLOPs and VLOSEs are supposed to prevent in relation to expression and information.

The **OSB imposes cross-cutting duties on user-to-user services about freedom of expression and privacy** in Clause 19. Here the understanding of harm as impingement on an individual user's freedom of expression is evident. It states that all services have "when deciding on, and implementing, safety measures and policies, a duty to have regard to the importance of protecting users' right to freedom of expression within the law". Similar cross-cutting duties are imposed on search services[124]. Category 1 services also have a duty to carry out specific risk assessments in relation to users' freedom of expression and right to privacy and to report publicly on the steps taken to protect these rights. Similar

[116] Art. 10 of TERREG
[117] Art. 21 of TERREG
[118] Recital 51 of AVMSD.
[119] Recital 61 of AVMSD.
[120] Article 28b (3)(i) of AVMSD.
[121] Recital 31 and 86 and Article 14(4) of DSA.
[122] Rec 47 of DSA.
[123] Art. 34 of the DSA.
[124] OSB cl. 29

to the EU legislation, the OSB requires all services to put in place complaints procedures for users who feel their rights have been unduly limited[125]. Where concern for the potential for wider societal harm related to freedom of expression is evident in the OSB is in the duties it places on Category 1 services to content of democratic importance and content of journalistic importance through the special treatment and exceptions discussed above.

5.2.5. Well-being

Another group of legal harms can be loosely classified as relating to well-being. This can be understood as referring to the physical and mental health of individuals and, as has been argued by van Dijck, Nieborg and Poell (2019) in their development of the concept of *citizen well-being*, can encompass the role citizens in collectives and the public. **The AVMSD addresses them in its rules on commercial communication**, which must be adhered to by both audiovisual media services and VSPs. Its Article 9(1) prohibits commercial communication from prejudicing human dignity, health and safety, and the environment. As discussed above these prohibitions are accompanied by specific provisions related to tobacco products, prescription medicines, alcohol, and high fat and sugar food and beverage. Well-being harms are treated more broadly in the DSA and the OSB, though in different ways.

The **DSA aims to prevent harms in this category from VLOPs and VLOSEs. It requires them to conduct assessments for systemic risk of negative effects** on human dignity and public security as well as "any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health, minors and serious negative consequences to the person's physical and mental well-being".[126] These expectations for the scope of risk assessments by VLOPs and VLOSEs reflect concern for both societal well-being in the form of public health and security and the well-being of individual users. Systemic risk assessments in this area will therefore need to address potential harm to public institutions as well as harm to individual users, but also foresee the cumulative effects on public institutions and systems from the accumulation of individual harms (Broughton Micova, 2021). For example, this could include the burden on public health or social services from increases in eating disorders or other mental health problems.

As discussed above, the **OSB introduces new criminal offences for the creation and dissemination of several types of content that are otherwise often legal but can impact users' well-being**, namely false information, threats, and messages that cause psychological harm or serious distress. In the Bill Category 1 user-to-user and search platforms and those accessed by children are also to be held responsible for assessing risks from legal but harmful content. Services accessible to children will have to also take measures to protect children from encountering such content that is harmful to children, while Category 1 services will have to provide tools for adults to protect themselves from such content that is harmful to adults.

[125] OSB cl. 18 & 28
[126] Art 34(1) of the DSA.

Two categories of designation are to be defined by regulations made by the Secretary of State: primary priority content and priority content[127]. These will be different for adults and for children with some overlaps. In its fact sheet on the Bill, the government lists self-harm and eating disorder related content as examples of content that would likely be designated for both children and adults.[128] Providers of Category 1 services and those accessible to children must also consider in their risk assessments non-designated content, which is content that "presents a material risk of significant harm to an appreciable number" of children or adults, but is not captured in one of the illegal categories (primary priority and priority)[129]. The Secretary of State's designations will be done once the Bill is adopted and Ofcom will be developing initial risk profiles following that, so the full scope of legal content that can be harmful to well-being will only be seen once these steps have been taken; however, the Bill seems to be open to any kind of content that could harm individual users.

[127] OSB cl. 53 & 54
[128] https://www.gov.uk/government/publications/online-safety-bill-supporting-documents/online-safety-bill-factsheet
[129] OSB cls. 53(6) & 54(3)

6. CONCLUSIONS

Each of the four initiatives covered has laudable objectives. The **DSA and the OSB have very broad objectives while the AVMSD and TERREG are more targeted** legal instruments. This report shows that the services in scope and the list of harms covered vary significantly, creating a great deal of complexity.

The DSA and the OSB cover the largest number of services, but they still only cover a subset of information society services (for the DSA) and of internet services (for the OSB). The DSA has the broadest scope of application because it covers the technical internet services, but it also maintains some grey zones, in particular on which technical internet services are covered and on the legal treatment of search engines (except for the rules that apply to VLOSEs). It may prove to have been misguided to have included these technical internet services in the scope of the DSA, given the small number of rules they will need to comply with in addition to the rules of the European Electronic Communications Code and of the e-Commerce Directive. In any case, **because the DSA is a regulation, there is very little leeway for the Member States to fill the grey zones.** Any clarifications will therefore need to be brought at the EU level, through the mechanisms foreseen in the DSA (guidance, delegated acts, and standardisation).

Despite being a very fast-growing and innovative market, **online gaming is not mentioned** – not even as examples of services in scope of the legislations, while these could convey many forms and types of illegal and harmful content. **Live streaming** seems in scope of all pieces of legislation, and is very clearly covered by the AVMSD, but no specific provisions addressing the particular dangers that might arise from live streaming are in any of them.

It is already not entirely clear if the more holistic pieces of legislation (the DSA and OSB) cover the 'metaverse' or future developments, despite recent statements by the UK government that the OSB will be sufficient.[130] The question is unsettled both at EU and UK levels.[131]

The report also shows that **the DSA does not have a process to designate services** (except for VLOSEs and VLOPs) **or to solve conflicts of jurisdiction**. It also shows that all initiatives seek to capture non-established providers, but the mechanisms foreseen are not identical. This may lead to complexities in practice.

As this report describes there have been debates about whether the regulated services should be required to treat **journalistic or edited content differently from other content, essentially whether there should be a journalistic or media exemption.** Such special treatment is included in the OSB, whereas at the EU level, there is only a timid reference to such content in TERREG and attempts to add an exception in the DSA through amendments failed. This question is now addressed in the

[130] https://hansard.parliament.uk//commons/2022-04-19/debates/F88B42D3-BFC4-4612-B166-8D2C15FA3E4E/OnlineSafetyBill#contribution-3C57F4AE-7D20-44E4-AF75-BB0AF8E4503E

[131] European Parliament Briefing – Metaverse, Opportunities, risks and policy implications, June 2020, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733557/EPRS_BRI(2022)733557_EN.pdf ; Lorna Woods, Regulating the future: the Online Safety Bill and the metaverse, 4 February 2022, https://www.carnegieuktrust.org.uk/blog-posts/regulating-the-future-the-online-safety-bill-and-the-metaverse/

proposed European Media Freedom Act, which does include some criteria, but policy makers formulating any provisions in this direction might consider some of the serious concerns raised about the approach taken in the OSB.

The **DSA has an extremely wide scope of application on the illegal harms in scope** whereas all the other initiatives have a much narrower scope. This could present challenges in implementation. Firstly, there could be significant variation among Member States in terms of offences and conflicts between a Member State and EU law. Appeal mechanisms may end up being used extensively by users to challenge national laws' compliance with EU laws or treaties. **An independent and transparent process to settle potential conflicts between national and EU legislation may need to be established by the Commission or in subsequent legislation.**

Secondly, **the DSA does not create a hierarchy of illegal harms or content**. Except for allowing that "manifestly illegal content" could justify the suspension of accounts on platforms, the DSA treats all illegal content essentially the same. This is distinctly different from the OSB, which addresses a defined set of priority criminal offences, and the other EU laws, which deal with specific, arguably severely harmful, types of illegal content.

The DSA requires service providers to act in a proportionate and diligent manner, and a kind of prioritisation of illegal harms in the EU context can be seen in the adoption of harm-specific legislation such as the TERREG and the proposed CSAM regulation, among others, as well as those chosen to be included in the AVMSD. Nevertheless, **given the DSA's broad scope, some further guidance as to how to distinguish between illegal content that risks significant harm to individual users or wider society and illegal content that is relatively benign or poses a risk only to a very limited number of users would likely help platforms avoid over-reacting**. More specific guidance on illegal harms and content related to criminal offences could also encourage standardisation across Member States and prevent the conflicts mentioned in the preceding point.

The DSA has the widest scope of legal harms for VLOPs and VLOSEs in that it requires assessment of systemic risk, and mitigation, of a broad list of harms to individual users and to wider society, including risks to fundamental rights. This kind of wider acknowledgment of collective and societal harms is in line with the recent Council of Europe recommendation (CM/Recc(2022)11) and can imply positive obligations or requirements on design or business practices. These are not covered by content and user-behaviour-focused measures such as notice and action or terms and conditions. For example, mitigating risks to freedom and pluralism of the media or preventing negative effects on civic discourse **may call for obligations to invest in journalism or public interest content prominence requirements.** The Media Freedom Act presents an opportunity for following up on some of these, however, such measures were not included in the draft Act. In other areas, such risks to public health or of gender-based violence follow-up policy may be needed.

Across all three pieces of legislation that deal with legal harms, **the protection of minors** is a core concern, but there are differences in scope. The AVMSD aims to prevent harms from content and the measures that it suggests VSPs make are ones that should limit the chances of exposure to harmful

content. Both the OSB and the DSA require risk assessments in this area. The children's risk assessment required by the OSB focuses on exposure to harmful content and recognises children as a vulnerable group of users, with its individual user-focused approach. The DSA's broader approach for VLOPs and VLOSEs requires systemic risk assessment of harm to the rights of the child. The DSA is therefore not as specific as the OSB or the AVMSD in relation to the protection of minors from content that may be harmful. Overemphasis on protective measures can lead to impingement of other aspects of children's rights online.[132] By recognising the rights of children, and not just their need for protection, the DSA likely provides an opportunity for more balanced and wholistic mitigation of the risks to children but ensuring this is opportunity is not missed will require careful attention to the systemic risk assessments and feedback loops that involve child rights organisations and experts. It must be noted also that the DSA has introduced for all online platforms an obligation for them to put in place appropriate measures to ensure a high level of privacy, safety, and security of minors and to protect them against being targeted for advertising purposes. These are very general requirements so it will be key for the Commission to adopt guidelines to help platforms to comply with these general requirements.

Lastly, **the DSA has placed more emphasis on the protection of consumers, an area already extensively covered by consumer protection legislation**. The new rules on online marketplaces are most probably justified, but they could have instead been added to the existing body of consumer protection directives.

[132] The UK already has an Age Appropriate Design Code (https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/), which mitigates some of these risk.

REFERENCES

Baker, C. E. (1989). *Human liberty and freedom of speech*. New York : Oxford University Press.

Broughton Micova, S. (2020). The Collective Speech Rights of Minorities. In *Positive Free Speech: Rationales, Methods and Implications*. Hart Publishhing.

Broughton Micova, S. (2021). *What's the Harm in Size? Very Large Online Platforms in the Digital Services Act*. Centre on Regulation in Europe asbl (CERRE). https://cerre.eu/wp-content/uploads/2021/10/211019_CERRE_IP_What-is-the-harm-in-size_FINAL.pdf

Bychawska-Siniarska, D. (2017). *Protecting the Right to Freedom of Expression under the European Convention on Human Rights*. Council of Europe. https://rm.coe.int/handbook-freedom-of-expression-eng/1680732814

Coe, P. (2022). The Draft Online Safety Bill and the regulation of hate speech: Have we opened Pandora's box? *Journal of Media Law*, 1–26.

DLA Piper (2009). EU study on the legal analysis of a single market for the information society: new rules for a new age? https://op.europa.eu/en/publication-detail/-/publication/a856513e-ddd9-45e2-b3f1-6c9a0ea6c722

Hoboken, J., Quintais, J., Poort, J., et al., (2019) Hosting intermediary services and illegal content online: an analysis of the scope of article 14 ECD in light of developments in the online service landscape: final report. European Commission Publications Office

Kenyon, A. T. (2021a). *Democracy of Expression: Positive Free Speech and Law*. Cambridge University Press.

Kenyon, A. T. (2021b). *Democracy of Expression: Positive Free Speech and the Law*. Cambridge University Press.

Kenyon, A. T., & Scott, A. (2020). *Positive Free Speech: Rationales, Methods and Implications*. Bloomsbury Publishing.

Lichtenberg, J. (1990). Foundations and limits of freedom of the press. In J. Lichtenberg (Ed.), *Democracy and the Mass Media: A Collection of Essays* (pp. 102–135). Cambridge University Press.

Livingstone, S., Lievens, E., & Carr, J. (2020). *Handbook for policy makers on the rights of the child in the digital environment*.

McGonagle, T., & Frosio, G. (2020). Free Expression and Internet Intermediaries: The Changing Geometry of European Regulation. *Oxford Handbooks in Law*, 467–485.

J. Nordemann, (2018) Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed?, Study prepared for the European Parliament http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_IDA%282017%29614207

Schwemer, S., Mahler, T. & Styri, H. (2020). Legal analysis of the intermediary service providers of non-hosting nature. Final report prepared for European Commission

van Dijck, J., Nieborg, D., & Poell, T. (2019). Reframing platform power. *Internet Policy Review*, *8*(2). https://doi.org/10.14763/2019.2.1414

cerre Centre on Regulation in Europe

Avenue Louise 475 (box 10)
1050 Brussels, Belgium
+32 2 230 83 60
info@cerre.eu
www.cerre.eu
@CERRE_ThinkTank
Centre on Regulation in Europe (CERRE)
CERRE Think Tank