
COMPARATIVE
LAW REVIEW
Vol. 16 – n. 1 – 2025
ISSN:2038 – 8993

COMPARATIVE LAW REVIEW
The Comparative Law Review is a biannual journal published by the
I. A. C. L. under the auspices and the hosting of the University of Perugia Department of Law.

Office address and contact details:
Email: complawreview@gmail.com

Comparative Law Review is registered at the Courthouse of Monza (Italy) - Nr. 1988 - May, 10th 2010.

COMPARATIVE LAW REVIEW

VOL. 16/1 - 2025

115

JACOPO FORTUNA

Minors' Digital Vulnerability in the EU and the US: A Comparison Between The Digital Services Act and The Kids Online Safety and Privacy Act

MINORS' DIGITAL VULNERABILITY IN THE EU AND THE US: A COMPARISON BETWEEN THE DIGITAL SERVICES ACT AND THE KIDS ONLINE SAFETY AND PRIVACY ACT [Ψ]

Jacopo Fortuna[*]

SUMMARY: 1. INTRODUCTION. - 2. THE DIGITAL SERVICES ACT AND ITS PROVISIONS ON THE PROTECTION OF MINORS ONLINE. - 3. THE ESSENTIAL ELEMENTS OF THE KIDS ONLINE SAFETY AND PRIVACY ACT. - 4. POINT OF CONTACT AND DIFFERENCES BETWEEN DSA AND KOSPA. - 5. CONTENT MODERATION AND DUTY OF CARE. - 6. CONCLUSIVE REMARKS.

Minors are among the most vulnerable users in the digital context and their protection online seems to be one of the greatest challenges. The need to protect minors from the risks of abuses is more and more felt as a need from a transnational point of view and this is the reason why the EU and the US have recently attempted to address this issue, albeit with different approaches. The legal comparison made in this paper between the EU's Digital Services Act (DSA) and the US Kids Online Safety and Privacy Act (KOSPA, which has not yet received a favourable vote from the US House of the Representatives of Congress) is particularly useful in order to outline a comprehensive and effective regulatory approach, combining the best features of the two analysed legislations. Indeed, while the DSA is characterised by the protection of all users of the digital environment, but with provisions that are perhaps too general and with a mainly 'reactive' form of intervention against illegal online content, KOSPA has the merit of offering a preventive approach focused specifically on minors, but it does not provide for ex post tools against such illegal content that are as precise and effective.

Keywords: Digital vulnerability – Minors – DSA – KOSPA – EU and US

I. INTRODUCTION

The fundamental rights of children are increasingly exposed to potential dangers within the digital environment. For this reason, the EU and the US have in recent years attempted to enact legislations to protect minors, who are among the most vulnerable of online users[1].

Within the European Union, there is currently no act exclusively dedicated to the digital protection of minors and their vulnerability[2]. The protection of minors online is, in fact, the result of various provisions included in different EU acts regulating different matters[3].

[Ψ] The paper was written within the framework of the project PRIN PNRR Self-assessment Network Impact Program (SNIP) – code P2022AK2HK.

[*] Assegnista di ricerca presso Scuola Universitaria Superiore Sant'Anna di Pisa (jacopo.fortuna@santannapisa.it; j.fortuna@unimc.it).

[1] On the topic of vulnerability and vulnerable users, including children, see D. Amram, *Standards to Face Children and Patients Digital Vulnerabilities*, in The New Shapes of Digital Vulnerability in European Private Law, ed. by C. Crea and A. De Franceschi, 2024, p. 439 ff.; *Id.*, *La transizione digitale delle vulnerabilità e il sistema delle responsabilità*, in Rivista italiana di medicina legale, 2023, p. 1 ff.; *Id.*, *Children (in the Digital Environment)*, in Elgar Encyclopedia of Law and Data Science, ed. by G. Comandé, 2022, p. 64 ff. On the concept of vulnerability within the EU, see G. Malgieri, *Vulnerability*, in Elgar Encyclopedia of Law and Data Science, ed. by G. Comandé, 2022, p. 363 ff.

[2] Think, for instance, of the exposure of minors to harmful or inappropriate content, commercial practices that exploit their vulnerability, or cyberbullying.

[3] The Audiovisual Media Services Directive (Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018), the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016), and Proposal for a Regulation on Child

The European legal framework is therefore fragmented, but the Digital Services Act[4] (henceforth DSA) constitutes the milestone on which the protection of all vulnerable users, including minors, is based and it provides the fundamental tracks that guide the approach to the protection of those most exposed to online dangers in the EU. Therefore, as far as the EU is concerned, the DSA will be the text analysed in relation to this issue.

The United States, on the other hand, has started a legislative process aimed at the approval of an act specifically designed to protect the safety of minors, to date called the 'Kids Online Safety and Privacy Act'[5] (henceforth KOSPA), the text of which passed the US Senate on 30 July 2024[6], pending a possible favourable vote by the House of Representatives as well.

The purpose of this work is to undertake a legal comparison between the two legal sources, being representative of the EU and US approaches to minors' digital vulnerability respectively, and to highlight the similarities and differences between them in order to understand the different tools adopted by the two legal systems to ensure children's online rights and safety, as well as to identify their respective possible shortcomings.

II. THE DIGITAL SERVICES ACT AND ITS PROVISIONS ON THE PROTECTION OF MINORS ONLINE

The DSA (Regulation (EU) 2022/2065 on a Single Market For Digital Services - Digital Services Act)[7] is a wide-ranging regulation establishing the obligations and responsibilities

Sexual Abuse (Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse {SEC(2022) 209 final} - {SWD(2022) 209 final} - {SWD(2022) 210 final}) also contain provisions on the protection of minors online, outlining a fragmented and not always coherent regulatory framework. On this point, see C. Di Francesco Maesa, *Digital platforms' private regulating and vulnerable users: the case of minors*, in Enforcing Private Regulation in the Platform Economy, ed. by F. Casarosa and M. Grochowski, 2025 (forthcoming). See, also, the compendium of EU formal texts concerning children in the digital world at https://digital-strategy.ec.europa.eu/en/library/european-strategy-better-internet-kids-bik-compendium-legislation.

[4] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[5] https://www.congress.gov/bill/118th-congress/senate-bill/2073/text.

[6] Statement on Senate Passage of the Kids Online Safety and Privacy Act, DCPD Number: DCPD202400658, July 30, 2024: "Today the Senate took a crucial bipartisan step forward to make our kids safer online. There is undeniable evidence that social media and other online platforms contribute to our youth mental health crisis. Today, our children are subjected to a wild west online, and our current laws and regulations are insufficient to prevent this. It is past time to act. […] The last time Congress took meaningful action to protect children and teenagers online was in 1998, before the ubiquity of social media and smartphones. Our kids have been waiting too long for the safety and privacy protections they deserve and which this bill would provide. This is more important than ever with the growing use of AI".

[7] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

of intermediary service providers that allow access to goods, services or content, including online marketplaces, with the aim of contributing to the proper functioning of the internal market for intermediary services, ensuring a secure online environment and building the digital sovereignty of the EU[8]. This Regulation is part of the European strategy of balancing respect for fundamental rights with the pursuit of economic objectives. The regulatory framework of the DSA defines obligations according to a system of concentric circles, envisaging an increasing and progressive pervasiveness depending on the services provided and the size of the provider[9].

However, despite the breadth of the subject matter, the DSA is also the legislation within EU law that still best outlines the fundamental principles relating to the protection of minors online who interface with intermediary service providers, including rules to protect them from harmful content online and obliging platforms to take measures to ensure the safety and security of minors using their services.

Firstly, the DSA stipulates that only very large online platforms (VLOPs) and very large online search engines (VLOSEs) will have to consider systemic risks related to their services, such as actual or foreseeable adverse effects in relation to the protection of minors[10] . For example, when assessing risks to minors' rights, VLOP and VLOSE

[8] On Digital Services Act see, *ex multis*, S. Del Gatto, *Il Digital Services Act: un'introduzione*, in Giornale di diritto amministrativo, 6/2023, p. 724 ff.; A. Chander, *When the Digital Services Act Goes Global, Berkeley Technology Law Journal* 38, no. 3, 2023, p. 1067 ff ; F. Casolari, *Il Digital Services Act e la costituzionalizzazione dello spazio digitale europeo*, in Giurisprudenza Italiana, 2024, p. 462 ff.; C. Irti, *Piattaforme digitali, contratti e protezione dei dati personali*, in I contratti, 1/2024, p. 5 ff.; G. Finocchiaro, *Responsabilità delle piattaforme e tutela dei consumatori*, in Giornale di diritto amministrativo, 6/2024, p. 730 ff.; G. Pascuzzi, *Il diritto dell'era digitale*, Bologna, 2024, pp. 289-302; M. Husovec, *Principles of the Digital Services Act*, 2024, Oxford; F. Hofmann, B. Raue (ed. by), *Digital Services Act: Article-by-Article Commentary*, München, 2024. Combined with the Digital Markets Act (Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828), the DSA aims at building the digital single market; cf., also, J. Quinn, *Regulating Big Tech: The Digital Markets Act and the Digital Services Act*, in Dublin Law and Politics Review 2, no. Finance Special Issue, 2021, pp. 2-4; M. L. Chiarella, *Digital Markets Act (DMA) and Digital Services Act (DSA): New Rules for the EU Digital Environment*, in Athens Journal of Law (AJL) 9, no. 1, 2023, p. 33 ff.

[9] S. Del Gatto, *Il Digital Services Act: un'introduzione*, in Giornale di diritto amministrativo, 6/2023, cit., pp. 724-725.

[10] DSA, Article 34, par. 1, let. (d): "Risk assessment. 1. Providers of very large online platforms and of very large online search engines shall diligently identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services. […] This risk assessment shall be specific to their services and proportionate to the systemic risks, taking into consideration their severity and probability, and shall include the following systemic risks: […] (d) any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being".

providers should take into account their ability to understand the structure and operation of the service, and to understand the risk of exposure to potentially harmful content[11].

VLOP and VLOSE providers must ensure that their services are organised in a way that allows minors to easily access the protection mechanisms imposed by the DSA, including notification, action and complaint mechanisms. For this reason, the DSA generically requires VLOPs and VLOSEs to take measures to protect minors from content that could harm their development and to provide tools that allow conditional access to such content[12]. VLOPs and VLOSEs should therefore provide tools that allow, for example, 'age verification' and 'parental control', and tools that allow minors to report abuse or obtain the necessary and appropriate support to deal with the specific case[13].

The DSA also stipulates generally that providers of online platforms accessible to minors shall take appropriate and proportionate measures to ensure a high level of security and protection of minors on their service[14] and clarifies that an online platform may be considered accessible to minors when its general terms and conditions allow minors to use the service, when its service is directed at or used predominantly by minors or if the provider is in any case aware that some of the recipients of its service are minors. Such knowledge may occur, for example, because the service provider already processes the user's personal data revealing their age for other purposes; in such a case, it must be specified that, in order to comply with the principle of data minimisation[15], the online platform provider may not retain, acquire or process more personal data than it already possesses to assess the recipient's age.

In any case, given the information in their possession, the Regulation prohibits online platform providers from presenting advertisements based on profiling if they are reasonably certain that the recipient of the service is a minor[16]. However, these restrictions are not applicable to, for example, apps, websites or other intermediary services that have advertisements within them. Therefore, digital service providers are free to micro-target

[11] DSA, Recital (81). Such risks may also arise from the design of online interfaces themselves, which could exploit (intentionally or unintentionally) the vulnerabilities and inexperience of minors.
[12] Cf. DSA, Recital (89).
[13] Cf. DSA, Art. 35, par. 1 (j).
[14] DSA, Art. 28, par.1.
[15] The principle of data minimisation is laid down in Regulation (UE) 2016/679 (GDPR), Art. 5, par. 1, let. c).

[16] DSA, Art. 28, par. 2. Moreover, with regard to advertisements on online platforms, the DSA requires that service recipients be provided with a set of information by the interfaces of the platform providers; on this point, see DSA, Art. 26 and in particular the list of identifiable information by service recipients in par. 1, lett. a), b), c), d).

such advertisements anywhere else on the web that does not fall within the scope of the DSA, since the prohibition in the Regulation does not cover, for instance, cookies and tracking banners that appear as advertisements on most web pages thanks to Google's ad services[17].

The control of compliance with the obligations for providers set out in the DSA, including those relating to minors, is distributed mainly between the European Commission, the Member States and the Digital Services Coordinators. Indeed, "According to this system, the EU Commission will be responsible for overseeing and enforcing the most stringent obligations for VLOPs and VLOSEs, even if VLOPs and VLOSEs shall also establish independent compliance officers to monitor the compliance with the DSA internally. Member States, in turn, have the duty to oversee all the other intermediary service providers that are established or have appointed a legal representative in their territory"[18].

A pivotal role is played by the Digital Services Coordinator (hereinafter 'DSC'), that is an authority appointed in each Member State with the task of supervising the application and enforcement of the Regulation[19]. DSC have both powers of investigation and enforcement powers to carry out their tasks[20].

Since the Commission is the main actor responsible to investigate compliance of providers of VLOPs and VLOSEs, it may decide to initiate proceedings and in the end of this the Commission shall adopt a non-compliance decision where it finds that the provider of the VLOP or VLOSE concerned does not comply[21].

III. The essential elements of the Kids Online Safety and Privacy Act

Voted by a very large majority, 91 votes in favour and 3 against, the legislation enjoyed bipartisan support in the Senate, which seems to presage possible approval in the House

[17] Art. 26 of the DSA does not cover the use of proxy data for sensitive features and while a platform is not allowed to target ads based on the sensitive category 'race', it can simply replace it with a generic proxy 'interested in African-American culture' or 'K-pop": on this point, see C. Di Francesco Maesa, *Digital platforms' private regulating and vulnerable users: the case of minors*, in Enforcing Private Regulation in the Platform Economy, ed. by F. Casarosa and M. Grochowski, 2025, cit., (forthcoming).

[18] DSA art 49.

[19] DSA Recitals 110-115, 118-122; Art. 3 para 1, lett n), o), art 49, para 2-4, Art. 50-53, Art. 55 concerning the duty of Digital Services Coordinators to draw up annual reports on their activities under the Regulation. The most important features of DSC should be their impartiality, transparency and rapidity in performing their tasks; See DSA Art 50 para. 1.

[20] DSA art 51 para. 1, 2.

[21] DSA arts 73-74. Furthermore, the Commission may impose on the provider of the VLOP or VLOSE concerned fines not exceeding 6% of its total worldwide annual turnover in the preceding financial year where some specific conditions listed in the Regulation are met.

of Representatives as well, although the effects on the legislative process of Donald Trump's re-election to the US presidency in November 2024 will have to be assessed. The KOSPA combines acts that had started their journey in Congress separately: the KOSA (Kids' Online Safety Act)[22] and COPPA 2 (Children Online Privacy Protection Act 2)[23], which was an update of the Children Online Privacy Protection Act of 1998[24].

As mentioned above, KOSPA is aimed at protecting the minors' digital vulnerability and preventing specific dangers and harms that the minor may suffer (e.g., anxiety, depression, bullying, etc.; on this point, see below, § 5). Sec. 103 of the Act deals precisely with safeguards for minors and provides that platforms that are aware that the person interacting with them is a minor must provide readily accessible and easy-to-use safeguards. For example, they must limit the ability of other users or visitors to communicate with the minor and prevent them from viewing personal data collected or shared on the platform, in particular by limiting public access to such data[25].

Platforms[26] are also required to limit by design features that encourage or increase the frequency, time spent and activity of minors on the platform[27], such as infinite scrolling, autoplay, rewards for time spent online, notifications and other features that incentivise compulsive use of the platform by minors[28].

Platforms are also required to control personalised recommender systems[29] or otherwise limit the types or categories of recommendations from such systems[30], and must also limit

[22] https://www.congress.gov/bill/118th-congress/senate-bill/1409/text.

[23] https://www.congress.gov/bill/118th-congress/senate-bill/1418/text.

[24] Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505 (COPPA); on COPPA and the need for its reform, see A. Parra, *Coping with COPPA: Exploring Alternatives to the Children's Online Privacy Protection Act*, in Indiana Journal of Law and Social Equality, 12, no. 2, 2024, pp. 193-208. On the inadequacy of current US regulations for the protection of children's online privacy, see S. Steinberg, *The Myth of Children's Online Privacy Protection*, in SMU Law Review, 77, no. 2, 2024, p. 441 ff. For some insights into the future of US privacy law in the digital context: E. Lampmann-Shaver, *Privacy's next Act*, in Washington Journal of Law, Technology & Arts, 19, no. 1, 2024, p. 97 ff.

[25] Cf. KOSPA, Sec 103, (a), (1). (A) e (B).

[26] KOSPA, Sec. 120, (6): "Online platform. The term 'online platform' means any public-facing website, online service, online application, or mobile application that predominantly provides a community forum for user-generated content, such as sharing videos, images, games, audio files, or other content, including a social media service, social network, or virtual reality environment".

[27] On this point, see KOSPA, Sec 3, (a), (2) which requires the platform to provide an easily accessible and user-friendly option to limit the amount of time spent by the child online.

[28] Cf. KOSPA, Sec 103, (a), (1). (C).

[29] Including the possibility for a minor to opt-out of such systems.

[30] Platforms may use a personalised recommendation system to show content to a minor if the system only uses information such as the language spoken by the minor, the city in which is located or the age; on this point see KOSPA, Sec 103 (e), (4), (C), from (i) to (iii). Moreover, KOSPA stipulates that the Secretary of Commerce, in coordination with the Federal Communications Commission and the Federal Trade Commission, shall conduct a study evaluating the most technologically feasible methods and options for developing systems to verify age at the device or operating system level. Such study shall consider the

the sharing of a minor's geolocation and provide a warning about the tracking of that geolocation[31].

KOSPA specifically addresses parental control tools to protect minors so that parents can support them in using the platform, especially with regard to the ability to manage a minor's privacy and account settings[32]. Parents must also have the ability to restrict purchases and financial transactions made by the minor, to view metrics of total time spent on the platform, and to place a limit on the time spent online by the minor[33].

With regard to reporting mechanisms, which can be activated by parents, children and schools, platforms must provide an easily accessible and user-friendly tool to allow the submission of reports of harm suffered by a minor and must therefore create a specific electronic contact point for this purpose[34]. Therefore, a platform must establish a timely and effective internal process for receiving and responding to such reports[35].

Obviously, platforms may not facilitate the advertising of products that are illegal (such as drugs) or that are illegal when provided to minors (such as, for example, tobacco, gambling and alcohol)[36].

The US act also qualifies it as illegal for any platform to design, modify or manipulate an interface in order to subvert or impair user autonomy, decision-making or choice (so-called dark pattern prohibition)[37].

The KOSPA also specifically provides that the provisions of the Act shall not be interpreted in such a way as to discourage any autonomous initiative of digital platforms to protect minors[38]. Indeed, the hermeneutics of the provisions should not be interpreted as preventing a platform from taking reasonable measures to block, detect or prohibit the

benefits of creating a device or operating system level age verification system, what information may need to be collected to create this type of age verification system and the accuracy of such systems and their impact or steps to improve accessibility, including for individuals with disabilities; on this issue, see Sec. 108 KOSPA.

31 Cf. KOSPA, Sec 103, (a), (1). (D) e (E).

32 KOSPA, Sec 103, (b), (1), (2), (A).

33 KOSPA, Sec 103, (B) e (C). Furthermore, a platform must provide a clear and visible notice when the described parental control tools are in place and information on what settings and controls are applied. The platform must provide that, in the case of a user whom the platform knows to be a child (up to 13 years of age), the tools are enabled by default; cf., Sec 3, (3) e (4).

34 KOSPA, Sec 103, (c), (1), (A) e (B); In addition, it is also necessary to provide confirmation of receipt of the report as well as a substantive reply to the submitter; cf. KOSPA, Sec 103, (c), (1), (C).

35 KOSPA, Sec 103, (c), (2). See also lett. (A), (B) and (C) for specific timeframes.

36 KOSPA, Sec 103, (d).

37 KOSPA, Sec 103, (e), (2); see, also, Art. 25 DSA on dark patterns.

38 KOSPA, Sec 103, (e), (4).

distribution of illegal, obscene or otherwise harmful material, block or filter spam, prevent criminal activity or protect the security of a platform or service[39]. In this, the Act emphasises the proactive spirit that underpins it and partially differentiates it from the DSA (on this point, see below, § following).

Before the registration by an individual whom the platform knows to be a minor, it must provide clear, conspicuous and easy-to-understand information on the platform's policies and practices in relation to minor safeguard and on access to parental protections and tools, as well as information on the possible use or provision of a product, service or functionality, including any personalised recommender system, that presents a high risk of harm to minors[40]. A platform operating a personalised recommender system must also set out in its terms and conditions how such a system is used, including how it processes personal data. Information shall also be provided on how minors (or their parents) may opt out of or manage the personalised recommender system[41].

KOSPA also focuses on the specific arrangements for the protection of the minor below the age of 13, referred to as a "child"[42]. Indeed, in such a case, the platform will have to provide additional information on the tools and parental protections required under Section 103 and obtain verifiable consent[43] from the parent prior to the child's initial use of the service[44].

SEC 105 of KOSPA addresses the transparency aspects of platforms and the resulting reporting on minor protection. Indeed, the US Act requires that at least once a year a platform must issue a public report describing the reasonably foreseeable risks of harm to minors and assessing the prevention and mitigation measures taken to address that risk based on an independent third-party audit of the platform[45]. In issuing public reports, a platform must take measures to safeguard the privacy of its users, including ensuring that

[39] KOSPA, Sec 103, (e), (4), (A), (i) e (ii).
[40] KOSPA, Sec 104 (a), (1).
[41] KOSPA, Sec 104 (b). A platform must provide minors and parents with clear, conspicuous, easy-to-understand and comprehensive information in a prominent location, which may include a link to a webpage, about its policies and practices regarding child protection required under section 103 and about how to access the safeguards and tools required under section 103; on this point, see KOSPA, Sec 104 (d).
[42] KOSPA, Sec 101, (1): "Child. The term 'child' means an individual who is under the age of 13".
[43] As defined in section 1302(9) del Children's Online Privacy Protection Act (15 USC 6501(9)).
[44] KOSPA, Sec 104 (a), (2), (A).

[45] KOSPA, Sec 105, (a).

data is presented in an aggregated and 'de-identified' format that cannot reasonably be linked to any user[46].

Finally, one of the hallmarks of the Kids Online Safety and Privacy Act is the amendment to Childern's Online Privacy Protection Act (COPPA). Indeed, KOSPA updates (in its Title II, entitled 'Children and Teen's Online Privacy')[47] the COPPA, amending various parts of the Act, especially with regard to the protection of children and teenagers (on this topic, see following §)[48].

IV. Point of contact and differences between DSA and KOSPA

Having analysed the content of the DSA in the part relating to minors and some of the most relevant parts of the KOSPA, it is now necessary to identify some points of contact and differences between the two legislations.

First of all, it should be noted that both sources aim to regulate the digital environment to ensure the safety of users, but they focus on partially different targets and aspects. While KOSPA deals exclusively and specifically with the safety of minors, protecting them from well-identified risks such as mental disorders (anxiety, depression, compulsive behaviour) and online sexual abuse[49], the DSA, not limiting itself to minors, is concerned with protecting all users from illegal and harmful content[50]. In relation to minors, the DSA only generically requires providers of online platforms accessible to minors to take appropriate and proportionate measures to ensure a high level of privacy, safety and security on their service[51].

---

46 KOSPA, Sec 105, (f). It should be specified that the term 'de-identified' means data that does not identify and is not linked or reasonably linkable to a device that is linked or reasonably linkable to an individual, regardless of whether the information is aggregated (see, KOSPA, Sec 105, (f), (3). KOSPA cannot be interpreted to prevail over the Children's Online Privacy Protection Act del 1998 – Sec. 113 (a), (2).

47 Sec 201 of KOSPA, amending and updating the Children's Online Privacy Protection Act of 1998, is entitled: "Online Collection, Use, Disclosure, and Deletion of Personal Information of Children and Teens".

48 KOSPA, Title 2, Sec. 201, in particular lett. (a) e (b).

49 KOSPA, Sec. 102, (a). KOPSA, on the other hand, is focused on protecting the vulnerability of minors and children, so much so that it specifically addresses age verification, requiring platforms to obtain verifiable parental consent before use by minors under the age of 13; cf. Sec. 104, (a), 2, (A).

50 Within the DSA see, ex multis, Art. 1. About the risk-based approach for larger online platforms in the DSA and the mitigation of the risk of sharing illicit online contents, see D. Amram, *Comparing EU initiatives on data: addressing risks and enhancing harmonisation opportunities*, in Opinio Juris in Comparatione, 1/2023, p. 13 ff.

51 Art 28, para. 1 and 2: "Online protection of minors 1. Providers of online platforms accessible to minors shall put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service. 2. Providers of online platform shall not present advertisements on their interface based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 using personal

Both Acts establish measures to make the platforms more transparent, both in terms of reporting and informing users. Although some requirements, parameters and criteria on reporting differ, KOSPA and DSA share the same need for transparency with quite similar underlying functions, with the big difference, of course, that the US Act is focused exclusively on minor (and child) protection. The DSA requires, in fact, regular reports on the actions taken to moderate content and indicating, in general, all information that favours transparency in digital service provision[52]. The Regulation also imposes for transparent reporting obligations, requiring platforms to publish information on the average monthly number of active users, disputes submitted to resolution bodies and suspensions imposed on users[53]. KOPSA also requires platforms to provide transparency and audit reports[54]; in fact, at least once a year, a platform must publish a public report describing the reasonably foreseeable risks of harm to minors and assessing the prevention and mitigation measures taken to address this risk based on an independent third-party audit, conducted through an inspection of the platform[55].

Still on the subject of transparency, Section 104 of KOSPA requires platforms to inform users about the platform's policies and practices in relation to minor safeguard, how to access parental protections and tools, and how to use personalised recommender systems, also specifying the associated risks[56], while the DSA deals with recommender systems in Art. 27, where it is established that providers of online platforms using such systems shall specify in their general terms and conditions, in clear and intelligible language, the main parameters used in providing recommendations, and indicate the options available to the recipients of the service enabling them to change or influence these parameters[57].

Both texts encourage the adoption of internal instruments to promote online safety: the DSA provides the possibility for the Commission to draw up codes of conduct in specific

data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor".

[52] On this point, see DSA, Artt. 15, 24, 42. More specifically, on the reporting activity related to content moderation, see, *infra*, §5.

[53] DSA Art. 24 and 42.

[54] Sec 105.

[55] Sec 105, (a).

[56] KOSPA, Sec. 104, (a), (A), (B), (C) e (b).

[57] see, also, DSA, Art. 38: "Recommender systems. In addition to the requirements set out in Article 27, providers of very large online platforms and of very large online search engines that use recommender systems shall provide at least one option for each of their recommender systems which is not based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679".

areas, while the KOPSA mentions the importance of developing best practices and clear technical standards[58].

With regard to the differences, as already mentioned, one should first look at the scope: DSA has a broader scope, addressing all intermediary service providers, including providers of services of "mere conduit", "catching" and "hosting" of information[59]; KOPSA focuses specifically on online platforms offering services to minors[60]. Furthermore, DSA seeks to safeguard competition in the internal market, fundamental rights enshrined in the Charter of Fundamental Rights of the European Union[61] and consumers, and it aims to counter both the dissemination of illegal content and misinformation[62].

Another of the most relevant differences between the two regulations concerns the fact that, while the DSA establishes abstract and generic obligations of diligence for intermediary service providers, requiring them, however, to take measures to remove illegal content online *ex post*[63], the KOSPA focuses on the specific forms of prevention to be adopted to avoid harm to minors, requiring platforms to mitigate *ex ante* risks identified in a very specific way (on this point, see following §)[64]. It is true, however, that despite the different approaches (since KOSPA is more focused on preventive forms of protection[65]), both EU and US legislation require digital platforms to act responsibly.

58 Art. 45 e 46 DSA e Sec 109 KOSPA.

59 On this topic, see DSA, Artt. 4, 5 and 6.

60 Art. 2 e 3 DSA e KOSPA, Sec. 101: "(3) Covered platform. (A) In general. The term 'covered platform' means an online platform, online video game, messaging application, or video streaming service that connects to the internet and that is used, or is reasonably likely to be used, by a minor" e Sec. 102.

61 Charter of Fundamental Rights of the European Union, hereinafter "the Charter", available at https://eur-lex.europa.eu/eli/treaty/char_2012/oj/eng.

62 DSA, Art. 1., Recital (9). On this topic, see V. Zeno-Zencovich, *The EU's Regulation of Speech: A Critical View*, in University of the Pacific Law Review, 2024, p. 175 ff.

63 DSA, Recital (40): "In order to achieve the objectives of this Regulation, and in particular to improve the functioning of the internal market and ensure a safe and transparent online environment, it is necessary to establish a clear, effective, predictable and balanced set of harmonised due diligence obligations for providers of intermediary services. Those obligations should aim in particular to guarantee different public policy objectives such as the safety and trust of the recipients of the service, including consumers, minors and users at particular risk of being subject to hate speech, sexual harassment or other discriminatory actions, the protection of relevant fundamental rights enshrined in the Charter, the meaningful accountability of those providers and the empowerment of recipients and other affected parties, whilst facilitating the necessary oversight by competent authorities." (41) "In that regard, it is important that the due diligence obligations are adapted to the type, size and nature of the intermediary service concerned. This Regulation therefore sets out basic obligations applicable to all providers of intermediary services, as well as additional obligations for providers of hosting services and, more specifically, providers of online platforms and of very large online platforms and of very large online search engines". See, also, l'Art.1 and Chapter III of DSA.

64 KOSPA, Sec 102 and 103.

65 However, even in relation to COPPA alone, there were suggestions for reform with a view to intervening to protect minors *ex ante* rather than ex post: "The two greatest challenges that must be addressed by the

Furthermore, while both regulations oppose design features that have the potential to promote harmful behaviour, some differences can be found on the subject. While KOSPA imposes pointed restrictions on features such as 'infinite scrolling' and 'auto-play'[66], which incentivise the compulsive use of the tool, the DSA in Articles 34 and 35 generically obliges VLOPs and VLSEs to identify and mitigate systemic risks, also deriving from their design features. It is evident, therefore, that in the US Act the preventive measures to be adopted must ensure that the platforms' algorithms are not limited to the generic identification of risks[67], but must be programmed in such a way as not to encourage an increase in the amount of time the minor spends on the platform.

One of the most obvious differences between the EU Act and the US Act is then the aspect of the processing of personal data: KOSPA contains specific provisions to update COPPA, which implement the protection of children's privacy in the digital context[68]. Thus, while the KOSPA provides detailed rules for the collection, use and deletion of children's personal data[69], in line with and updating the US COPPA, the DSA tends to rely on the GDPR for the processing of personal data, making only a few limited specific mentions of minors[70].

FTC as they work to reform COPPA are to make sure that the regulations are acting in a proactive rather than reactive manner, and to provide incentives to both corporations and parents to make sure that COPPA is self-enforcing": A. Parra, *Coping with COPPA: Exploring Alternatives to the Children's Online Privacy Protection Act*, in Indiana Journal of Law and Social Equality, 12, no. 2, cit., 2024, p. 207.

66 KOSPA, Sec 103 (a) (C).

67 Differently, in DSA Art. 34, para. 1, it is generically stated that the risk assessment must include any current or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors, and negative consequences for the physical and mental well-being of the person.

68 KOSPA, Title II, Children and Teen's Online Privacy, SEC. 201, Online Collection, Use, Disclosure, and Deletion of Personal Information of Children and Teens; v, altresì, KOSPA, SEC. 113. Rules of Construction and Other Matters: "(a) Relationship to Other Laws. Nothing in this subtitle shall be construed to […] (2) preempt the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.) or any rule or regulation promulgated under such Act".

69 KOSPA, Sec. 201.

70 DSA, Recital (10) "[…] The protection of individuals with regard to the processing of personal data is governed solely by the rules of Union law on that subject, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC […]" e (71): "[…] Providers of online platforms should not present advertisements based on profiling using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor. In accordance with Regulation (EU) 2016/679, notably the principle of data minimisation as provided for in Article 5(1), point (c), thereof, this prohibition should not lead the provider of the online platform to maintain, acquire or process more personal data than it already has in order to assess if the recipient of the service is a minor. Thus, this obligation should not incentivize providers of online platforms to collect the age of the recipient of the service prior to their use. It should be without prejudice to Union law on protection of personal data" and Art. 2, par. 4 "This Regulation is without prejudice to the rules laid down by other Union legal acts regulating other aspects of the provision of intermediary services in the internal market or specifying and complementing this Regulation, in particular, the following: […] g) Union law on the protection of personal data, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC". However, for a mapping of the recent EU legislative initiatives on data, see D. Amram, *Comparing EU initiatives on data: addressing risks and enhancing harmonisation opportunities*, in Opinio Juris in Comparatione, 1/2023, cit., p. 1 ff.

A further element of differentiation between KOSPA and DSA concerns the role of parents and the tools available to them in the protection of minors. In fact, the KOSPA specifically regulates the functions and tools available to parents for monitoring and controlling the online activities of minors, as well as for accessing the data collected on the platforms[71]. The DSA, on the other hand, does not include detailed provisions for the involvement of parents nor a direct role for parents in regulating the safety of minors online[72].

With regard to sanctions, KOSPA does not identify very detailed sanctions, focusing, as already noted, on preventive and advisory mechanisms, while the DSA provides for stricter enforcement with significant specific economic sanctions of up to 6% of the global turnover of platforms[73] in the event of violation of the rules of the Regulation[74].

Finally, it should be noted that the DSA provides for a limited exemption for certain categories of Internet service providers from liability for the unlawful conduct of users. In fact, the Regulation states that service providers who play a 'passive' role with regard to the specific information hosted are exempted from liability for information provided by a

71 KOSPA, Sec. 103 (b).

72 Even on this aspect, the DSA generically provides that VLOPs and VLOSEs must set up useful tools for the protection of minors that allow, for example, 'age verification' and 'parental control' as well as set up tools that allow minors to report abuse or obtain the necessary and adequate support to cope with the specific case: cf. DSA, Art. 35, para. 1 (j).

73 Cf. DSA, Art. 52.

74 It is also useful to briefly dwell on enforcement mechanisms of the two regulations: while the DSA provides for a system of supervision and enforcement that mainly entrusts the Digital Services Coordinators and the European Commission with the task of monitoring the correct application of the Regulation, the KOSPA envisages important roles for the Federal Trade Commission (see, for instance Federal Trade Commission, *A Record of Results for American Consumers*, WL 4254252, September 16, 2024, in particular at p. 4 about "Protecting Privacy and Safety Online") and the Kids Online Safety Council to guarantee the effectiveness and correctness of the measures adopted. On this topic see DSA, Chapter IV, Sec 1, Art. 49 ff. and Sec. 4, art. 64 ff. Moreover, Section 3 establishes the European Board for Digital Services, which consists of an independent advisory group of digital service coordinators to supervise intermediary service providers; Art. 61, para. 2: "The Board shall advise the Digital Services Coordinators and the Commission in accordance with this Regulation to achieve the following objectives: (a) contributing to the consistent application of this Regulation and effective cooperation of the Digital Services Coordinators and the Commission with regard to matters covered by this Regulation; (b) coordinating and contributing to guidelines and analysis of the Commission and Digital Services Coordinators and other competent authorities on emerging issues across the internal market with regard to matters covered by this Regulation; (c) assisting the Digital Services Coordinators and the Commission in the supervision of very large online platforms". About KOSPA, see Sec 110 for enforcement of KOSPA by the Federal Trade Commission, which is a US government agency, established in 1914 by the Federal Trade Commission Act, whose main task is to promote consumer protection and prevent or eliminate anti-competitive commercial practices (see https://www.ftc.gov/) and Sec 111 establishing the Kids Online Safety Council, which has mainly advisory functions.

recipient of the service[75]. It should also be noted that Article 8 of the DSA, concerning the absence of general obligations to monitor or actively seek facts, states that 'No general obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers'[76]. The lack of preventive obligations for the dissemination of illegal DSA content is however counterbalanced by the tendency of digital platforms to operate a collateral censorship, aimed at censoring (over-blocking) legal content for fear of incurring penalties, thus risking the restriction of fundamental rights such as those of

[75] See DSA, Art. 4, 5. 6: Article 4, 'Mere conduit' "1. Where an information society service is provided 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, the service provider shall not be liable for the information transmitted or accessed, on condition that the provider: (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission. 2. The acts of transmission and of provision of access referred to in paragraph 1 shall include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission. […]" Article 5, 'Caching' "1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, the service provider shall not be liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient or more secure the information's onward transmission to other recipients of the service upon their request, on condition that the provider: (a) does not modify the information; (b) complies with conditions on access to the information; (c) complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry; […]" Article 6, Hosting "1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, the service provider shall not be liable for the information stored at the request of a recipient of the service, on condition that the provider: (a) does not have actual knowledge of illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or (b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content". However, on the exemption from liability for intermediaries acting as facilitators of communication and the concept of passivity, see also G. Sartor, *Providers Liability: From the eCommerce Directive to the future'. In-Depth Analysis for the IMCO Committee*, 2017, available at https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf, p. 24 e 26: […] we must abandon the view that only "passive" intermediaries should be protected, i.e., the view that intermediaries that take a "non-passive", or active role" – by indexing user-generated content, or linking advertising to it, or determining what results will be provided to user queries – should lose their protection from secondary liability. What justifies the exemption from secondary liability is not the passivity of intermediaries, but rather their function as communication enablers. This function would be incompatible with initiating the communications at issue, but may allow or even require playing an active role in creating an environment in which users' communications can be delivered and made accessible".

[76] See G. Pascuzzi, *Il diritto dell'era digitale*, Bologna, 2024, cit., pp. 295-296. However, the DSA provides that Internet intermediaries may be ordered by a competent authority to put an end to, or otherwise prevent, any violations of the Regulation, and in such an eventuality providers will have to respect and comply with the order issued by the competent authority. On this point, cf. DSA Art 4 para. 3, Art. 5 para. 2, and Art. 6 para. 4.

expression and information (see the Charter, Art. 11[77]) by platform users[78]. A similar issue was raised by civil society in relation to KOSPA and the First Amendment in the US, where emphasis was placed on the difficulty of striking a balance between the protection of minors and freedom of speech, especially in the face of the markedly preventive forms of protection that characterise the US Act[79].

V. CONTENT MODERATION AND DUTY OF CARE

Within a comparison between DSA and KOSPA, it is useful to focus on two of the main aspects addressed by these regulations, namely respectively "content moderation" and "duty of care", both aimed at protecting vulnerable users against possible harm that may occur in the digital environment.

The DSA regulation on content moderation is essential for the protection of minors online. Article 3 of the Regulation defines content moderation as 'the activities, whether automated or not, undertaken by providers of intermediary services, that are aimed, in particular, at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service [...]' [80].

[77] Charter of Fundamental Rights of the European Union, Article 11: "Freedom of expression and information 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. 2. The freedom and pluralism of the media shall be respected". On this topic, see V. Zeno-Zencovich, *The EU's Regulation of Speech: A Critical View*, in University of the Pacific Law Review, 2024, cit., p. 175 ff.

[78] See G. Sartor, *Providers Liability: From the eCommerce Directive to the future'. In-Depth Analysis for the IMCO Committee*, 2017, cit., available at https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf, p. 11 and C. Di Francesco Maesa, *Digital platforms' private regulating and vulnerable users: the case of minors*, in Enforcing Private Regulation in the Platform Economy, ed. by F. Casarosa and M. Grochowski, 2025, cit., (forthcoming).

[79] Constitution of the United States, First Amendment: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances"; https://constitution.congress.gov/constitution/amendment-1/#amendment-1. For some examples of the criticism raised by civil society regarding KOSPA and respect for freedom of speech, protection of minorities (especially the LGBTQ+ community) and the freedom of minors online, see https://www.eff.org/deeplinks/2023/05/kids-online-safety-act-still-huge-danger-our-rights-online; https://www.eff.org/deeplinks/2024/02/dont-fall-latest-changes-dangerous-kids-online-safety-act; https://www.fightforthefuture.org/news/2022-11-28-letter-90-lgbtq-and-human-rights-organizations-oppose-kosa; https://reason.com/2024/07/29/kosa-moves-forward-in-congress-threatening-free-speech-and-encryption/; https://www.cnbc.com/2023/05/02/updated-kids-online-safety-act-aims-to-fix-unintended-consequences.html.

[80] Art. 3 del DSA continues as follows : "[…] including measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, demonetisation, disabling of access to, or removal thereof, or that affect the ability of the recipients of the service to provide that information, such as the termination or suspension of a recipient's account".

In the activity of content moderation, digital platforms can only be held liable if they have 'actual knowledge' of the illegality of the content[81], which, moreover, can only be objected to if it is manifestly illegal, i.e. when the invalidity is clear to a layman[82].

The DSA requires intermediary service providers to make available to the public, in a machine-readable format and in an easily accessible manner, at least once a year, clear and easily comprehensible reports on the content moderation activities carried out during the reference period[83]. It is also established that intermediary service providers draw up reports containing meaningful and comprehensible information on the content moderation activities undertaken on their own initiative by the same providers, the possible use of automated tools, the measures taken to provide training and assistance to persons in charge of content moderation, the number and type of measures taken that affect the availability, visibility and accessibility of information provided by recipients of the service and the ability of recipients to provide information through the service[84].

[81] V. DSA, Recital (22): "In order to benefit from the exemption from liability for hosting services, the provider should, upon obtaining actual knowledge or awareness of illegal activities or illegal content, act expeditiously to remove or to disable access to that content. […] The provider can obtain such actual knowledge or awareness of the illegal nature of the content, inter alia through its own-initiative investigations or through notices submitted to it by individuals or entities in accordance with this Regulation in so far as such notices are sufficiently precise and adequately substantiated to allow a diligent economic operator to reasonably identify, assess and, where appropriate, act against the allegedly illegal content. However, such actual knowledge or awareness cannot be considered to be obtained solely on the ground that that provider is aware, in a general sense, of the fact that its service is also used to store illegal content. Furthermore, the fact that the provider automatically indexes information uploaded to its service, that it has a search function or that it recommends information on the basis of the profiles or preferences of the recipients of the service is not a sufficient ground for considering that provider to have 'specific' knowledge of illegal activities carried out on that platform or of illegal content stored on it"; Article 6, Hosting: "1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, the service provider shall not be liable for the information stored at the request of a recipient of the service, on condition that the provider: (a) does not have actual knowledge of illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or (b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content".

[82] On the criteria for identifying manifestly illegal content, see DSA, Recital (63), last sentence.

[83] In 2025, the Implementing Regulation laying down templates concerning the transparency reporting obligations of providers of online platforms (https://digital-strategy.ec.europa.eu/en/library/implementing-regulation-laying-down-templates-concerning-transparency-reporting-obligations) will produce its first effects. This implementing regulation will standardise the format, content and reporting periods for transparency reporting under the DSA, specify the content moderation practices of platforms, and establish uniform templates and reporting periods. Service providers will therefore have to start collecting data in accordance with the Implementing Regulation as of 01/07/2025, with the first harmonised reports expected in early 2026. The reporting periods for VLOP and VLOSE providers will then need to be aligned, depending on their designation dates. This is necessitated by the current lack of homogeneity on the part of platforms in reporting and categorising DSA violations and applying remedies towards them.

[84] See Art 15, par.1, let. c) del DSA, that continues as follows: "the information reported shall be categorised by the type of illegal content or violation of the terms and conditions of the service provider, by the detection method and by the type of restriction applied".

The reports should also contain information on any use of automated tools for content moderation purposes, including qualitative aspects, description of the precise purposes, accuracy indicators and possible error rate of the automated tools used in pursuit of these purposes, as well as any safeguards applied[85]. Where the intermediation service is primarily aimed at minors, service providers must also explain the conditions and restrictions on the use of their service in a clear and comprehensible manner for such vulnerable persons[86].
The DSA also provides for reporting mechanisms that enable the information storage service provider to make an informed and diligent decision regarding the content to which the report refers, in particular whether such content should be considered illegal and should be removed or access to it should be disabled[87]. The DSA has also provided for a mechanism to enable the removal of illegal content expeditiously by creating so-called 'trusted flaggers'[88] who submit alerts on illegal content or activities to online platform providers, who in turn must take all necessary technical and organisational measures to ensure that such alerts are prioritised and processed and decided upon without undue delay[89]. Trusted flaggers are also obliged to submit detailed reports that they must publish once a year on the flagged content during the reporting period[90]. Cyber-violence, including non-consensual sharing of intimate content, is an example of content that requires rapid processing if flagged by users, including minors, and appropriate adaptation of the content

[85] V. art 15, par.1, let. e).
[86] C. Di Francesco Maesa, *Digital platforms' private regulating and vulnerable users: the case of minors*, in Enforcing Private Regulation in the Platform Economy, ed. by F. Casarosa and M. Grochowski, 2025, cit., (forthcoming).
[87] DSA, Art. 16 (Notice and action mechanisms) "1. Providers of hosting services shall put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content. Those mechanisms shall be easy to access and user-friendly, and shall allow for the submission of notices exclusively by electronic means. 2. The mechanisms referred to in paragraph 1 shall be such as to facilitate the submission of sufficiently precise and adequately substantiated notices […]".
[88] F. Casarosa, *Internal mechanisms of enforcement – what role do trusted flaggers play?*, in Enforcing Private Regulation in the Platform Economy, ed. by F. Casarosa and M. Grochowski, 2025, (forthcoming).
[89] V. DSA, art. 22 (Trusted flaggers), par. 1: "Providers of online platforms shall take the necessary technical and organisational measures to ensure that notices submitted by trusted flaggers, acting within their designated area of expertise, through the mechanisms referred to in Article 16, are given priority and are processed and decided upon without undue delay" e par. 2 "The status of 'trusted flagger' under this Regulation shall be awarded, upon application by any entity, by the Digital Services Coordinator of the Member State in which the applicant is established, to an applicant that has demonstrated that it meets all of the following conditions: (a) it has particular expertise and competence for the purposes of detecting, identifying and notifying illegal content; (b) it is independent from any provider of online platforms; (c) it carries out its activities for the purposes of submitting notices diligently, accurately and objectively".
[90] See DSA, art. 22, para. 3.

moderation practices[91]. The DSA also provides for the possibility of lodging complaints against the inaction of digital platforms[92].

However, if the rules of the EU regulation on content moderation seem at first reading to be abstractly adequate for the protection of minors, it must be pointed out that there are no concrete, specific and uniform rules on content moderation in relation to minors and, as a result, each digital platform implements the EU provisions on the matter differently, with the result that minors are not effectively protected from harmful content online nor are they protected in a standardised manner, with the risk that even completely inadequate measures are adopted[93]. Furthermore, in order to ensure respect for fundamental rights, it has been argued that the internet service provider should be held liable when it has contributed to the unlawful conduct of its user "by failing to exercise due care, namely, to adopt reasonable measures that could have prevented that behaviour or mitigated its effects"[94].

It is precisely on a preventive approach aimed at protecting minors online that the duty of care under KOSPA focuses, which requires that everything possible be done to prevent potential harm, also by means of monitoring by external authorities, who may assess whether the proactive effort is adequate and sufficient[95].

The 'duty of care' in the KOSPA, unlike the DSA, is therefore more focused on forms of prevention aimed at protecting minors, especially in order to avoid harm that they may suffer from specific risks[96]. In fact, Sec 102 regulates that a platform shall exercise reasonable care in the creation and implementation of any design feature to prevent and mitigate the harms to minors. Such harms may relate to mental health disorders (like

---

91 DSA, Recital (87). "Providers of very large online platforms, in particular those primarily used for the dissemination to the public of pornographic content, should diligently meet all their obligations under this Regulation in respect of illegal content constituting cyber violence, including illegal pornographic content, especially with regard to ensuring that victims can effectively exercise their rights in relation to content representing non-consensual sharing of intimate or manipulated material through the rapid processing of notices and removal of such content without undue delay. Other types of illegal content may require longer or shorter timelines for processing of notices, which will depend on the facts, circumstances and types of illegal content at hand. Those providers may also initiate or increase operation with trusted flaggers and organise training sessions and exchanges with trusted flagger organisations".

92 DSA Art. 20, para 1, lett. a) - d). This is also established in article 20 para 4.

93 C. Di Francesco Maesa, *Digital platforms' private regulating and vulnerable users: the case of minors*, in Enforcing Private Regulation in the Platform Economy, ed. by F. Casarosa and M. Grochowski, 2025, cit., (forthcoming).

94 G. Sartor, *Providers Liability: From the eCommerce Directive to the future. In-Depth Analysis for the IMCO Committee*, 2017, cit., available at https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf, p. 29.

95 On this point see, *supra*, §§ 3 and 4.

96 KOSPA, SEC. 102. Duty of care.

anxiety, depression, eating disorders, substance use disorders, and suicidal behaviours), patterns of use that indicate or encourage addiction-like behaviours by minors, physical violence, online bullying, and harassment. Harm may also be caused by sexual exploitation and abuse of minors, promotion and marketing of narcotic drugs, tobacco products, gambling, or alcohol and predatory, unfair, or deceptive marketing practices. KOSPA's duty of care is also intended to limit financial harms against minors[97]. Sec 102 specifies, however, that the protection of minors by prescribing platforms cannot in any case prevent or preclude them from independently searching for content or accessing resources and information relating to the prevention or mitigation of harm[98].

Therefore, although KOSPA's duty of care is more concise than the content moderation of the DSA, it is more effectively tailored to the peculiarities and risks run by minors, and it is also designed in proactive terms[99] and not with a view to *ex post* intervention on illegal content, as is the case for content moderation under the DSA.

VI. CONCLUSIVE REMARKS

At a time, such as the present, when the protection of minors online is a major transnational need, the EU Digital Services Act and the US Kids Online Safety and Privacy Act constitute important attempts to safeguard some of the most vulnerable users in a digital environment that is constantly evolving and presents increasingly pervasive risks.

The legislations analysed are therefore inspired by the same purpose and present both points of contact and relevant differences that reveal a different approach to the subject on the part of the two legal systems.

First of all, while the DSA aims to create a safer and more transparent digital environment, protecting the fundamental rights of all users, including minors, KOSPA is a regulatory source specifically aimed at protecting minors and taking into account the peculiar risks and harms they may incur.

Both regulations are aimed at increasing the transparency of providers of digital services and online platforms and to this end provide for analytical reporting activities (in the DSA especially related to content moderation) and mechanisms to facilitate the receipt of

97 KOSPA, SEC. 102. Duty of care, (a), no. (1)-(6).
98 KOSPA, SEC. 102. Duty of care, (b).
99 For concrete forms of minor protection see, *supra*, §3; in particular, Sec. 103 KOSPA.

information by minors, especially related to the characteristics of the digital tools used, risks and accessible remedies.

Furthermore, both KOSPA and DSA favour the introduction of internal tools to promote online safety: the EU Regulation provides for the possibility for the Commission to draw up codes of conduct in specific areas, whereas KOPSA mentions the importance of developing best practices and clear technical standards for the protection of minors.

In addition to the aforementioned difference in scope, which is also due to the fact that the DSA aims to protect competition in the internal market and the fundamental rights of all users (and is aimed at combating both disinformation and the dissemination of illegal content online), it is possible to find further elements of discontinuity between the two sources.

In fact, KOSPA and DSA seem to have a different approach with regard to 'design features', since the US act provides that the platforms' algorithms are not limited to the generic identification of risks but are programmed in such a way as not to encourage an increase in the amount of time the child spends on the platform, imposing precise restrictions on features such as "infinite scrolling" and "auto-play", which stimulate the compulsive use of the tool; the DSA, on the other hand, only obliges VLOPs and VLSEs to identify and mitigate systemic risks, also arising from their design features.

The European Regulation and the US Act also differ with regard to the processing of personal data. The KOSPA provides specific rules on the collection and handling of minors' data, in line with the Children's Online Privacy Protection Act (COPPA), and it contains specific provisions aimed at updating it, which implement the protection of minors' privacy in the digital context. It amends the COPPA especially with regard to aspects related to the online collection, use, disclosure and deletion of children's and adolescents' personal information; the DSA, on the contrary, does not focus specifically on children's data but refers to the General Data Protection Regulation (GDPR) for the processing of their personal data, and does not contains effective provisions taking into account the peculiarities and vulnerabilities of minors.

Finally, in addition to the differences on the role played by parents and the characteristics of sanctions[100] (see § 4 above), one of the most evident differences between the two acts concerns the preventive or reactive nature of online minor protection adopted by KOSPA

[100] For a brief focus on enforcement mechanisms, see supra footnote no. 75.

and DSA respectively. In fact, while the latter establishes generic and abstract obligations of due diligence for intermediary service providers, but at the same time requires them to take measures to report or remove illegal content ex post, the former focuses on the specific forms of prevention to be adopted to avoid harm to minors, requiring platforms to mitigate very specifically identified risks (on this point, see §4 above).

This different approach is reflected in the content moderation regulated by the DSA and the duty of care under the KOSPA. As noted, however (see, supra §5), *ex post* removal of illegal content is not very helpful in preventing harm to minors and the rules on content moderation are not yet sufficiently specific and uniform, with the consequence that each platform implements the relevant EU provisions in a different and non-standardised way, potentially affecting minors. In contrast, as anticipated, the duty of care under KOSPA is based on a proactive approach aimed at the protection of these vulnerable individuals, which requires that all necessary measures be taken to prevent potential harm to minors and children that could result from specifically identified risks and causes (see §5 above).

It should also be recalled that while the DSA was already enacted in 2022, KOSPA is still within the legislative process in Congress, since to date it has only passed the Senate, albeit with both Democratic and Republican support (see, supra, §3). The possible changes to the final version of the text and the effects on the issue of Donald Trump's re-election to the Presidency of the United States of America will therefore have to be assessed.

In conclusion, if the DSA would have benefited from the provision of preventive instruments aimed at the specific protection of minors, in the United States it would perhaps have been desirable to have legislation aimed at the protection of the entire digital ecosystem on the model of the European one, including protection for minors. Moreover, KOSPA does not appear to have a reactive discipline as abstractly structured as that of the DSA, potentially useful for the removal of illegal or dangerous content.

Ultimately, both DSA and KOSPA represent significant advances towards the protection of vulnerable individuals, especially in the face of new technological challenges and the transnationality of digital phenomena that require continuous adaptation of regulations. However, it is through a legislative evolution that combines the preventive and punctual vision of the KOSPA with the systemic and reactive approach of the DSA that the emergence of a safe and transparent digital environment for new generations could be more effective.