Warsaw, 19 June 2026
Opinion-Nr.: FOE-PRT/583/2026 [TO/AlC]

URGENT OPINION ON THE BILL NO. 398/XVII/1 ON MEASURES TO PROTECT CHILDREN IN DIGITAL ENVIRONMENTS

PORTUGAL

This Urgent Opinion has benefited from contributions made by **Dominika Bychawska-Siniarska**, International Human Rights Law Specialist, **Nevena Krivokapic Martinovic**, Attorney at Law specialized on in online media, freedom of expression in the digital environment and information privacy; and **Tamara Otiashvili**, Senior Legal Expert in Human Rights and Democratic Governance.

The Urgent Opinion was also peer reviewed by **Antonina Cherevko**, Senior Adviser to the OSCE Representative on Freedom of the Media.

Based on an unofficial translation of the Bill provided by the requesting authority.

OSCE Office for Democratic Institutions and Human Rights

Ul. Miodowa 10, PL-00-251 Warsaw
Office: +48 22 520 06 00
www.legislationline.org

EXECUTIVE SUMMARY AND KEY RECOMMENDATIONS

Bill No. 398/XVII/1 on Measures to Protect Children in Digital Environments (the Bill) establishes a regulatory framework aimed at strengthening the protection of minors online in response to growing concerns about the impact of digital platforms and services on children's wellbeing, privacy, and development. It increases the "minimum digital age" from 13 to 16 for independent access to platforms and online services covered by the Bill, requires parental consent for younger users aged 13-16, provides for a minimum access age of 13 for covered platforms and services, with some exceptions, along with mandatory age verification and enhanced duties for digital service providers to mitigate risks.

Generally, the Bill pursues a legitimate child protection objective consistent with international human rights obligations. Indeed, risks of children's exposure to harmful content, including grooming, disinformation, manipulative design, pervasive data collection and other digital risks in today's online ecosystem, are real and well-founded and need to be addressed. In this respect, the initiative to develop the Bill is particularly timely and reflects an effort to reinforce protections for children and to mitigate risks that may affect their wellbeing, privacy, and development in digital environments. The Bill includes a number of positive features aimed at addressing platform design and addictive or harmful functionalities, and introduces default settings for children, among others, which reflect international and regional recommendations. At the same time, the Bill would benefit from a more comprehensive assessment of its potential impact on the exercise of the full range of children's rights, the evolving capacities of children and their diversity, taking into account that mandatory-age-verification measures will affect all users, and should be approached with caution. In addition, to ensure effective protection of children but also of all users, it is also important to more comprehensively target systemic issues linked to specific platform design choices and business models.

Overall, the proposed Bill could be strengthened by reflecting a more clearly rights-based and risk-based approach grounded in privacy-by-design, safety-by-design, and security-by-design principles and solutions, ensuring fair, accessible, safe and secure digital platforms and services for children and other users.

In addition, the Bill's overall structure and scope could be enhanced to ensure legal certainty, foreseeability and proportionality of the contemplated measures. The proposed framework at times includes some broad and vague wording that would deserve further elaboration to avoid ambiguity and possible arbitrary or inconsistent application, particularly with respect to the sometimes indeterminate categories of digital services covered, and risks identified, especially with respect to so-called "harmful content". A clearer differentiation of categories of digital platforms and services, taking into account the nature and level of risk they may present to children would allow for more proportionate measures tailored to the identified risks posed by a specific category of digital platform or service, also considering the distinct and potentially heightened risks posed for children by generative artificial intelligence systems and similar technologies. This would avoid the imposition of uniform obligations across types of services that differ significantly in their potential to generate or mitigate risks of potential harm, and therefore not warranting the same regulatory

response. Such differentiation would also help reducing legal uncertainty for service providers.

The differentiated age-based restrictions reflect a graduated approach based on evolving capacities of children although the minimum access age of 13 for covered platforms and services may warrant further consideration from the perspective of ensuring a proportionate balance between protection objectives and exercise of all children's rights, including the rights of access to information, freedom of expression, to education, health and development, participation and protection from violence. The proposed age verification mechanisms, if not carefully designed, may also raise concerns related to privacy, data protection, non-discrimination, and the risk of exclusion of certain user groups.

In addition, some provisions may allow potentially overly intrusive monitoring and parental control systems and could be more narrowly circumscribed, while strong de-indexing or blocking powers, in the absence of appropriate safeguards, may risk overreach and chilling effects on expression. Stronger guarantees for fundamental rights should be considered, including more proportionate, minimally intrusive, and non-discriminatory approaches to age verification, in particular to avoid an exclusive dependence on state-issued digital credentials which may risk indirect exclusion of certain groups – such as undocumented children, asylum-seekers, refugees, or individuals lacking access to digital identity infrastructure.

More specifically, and in addition to what is stated above, ODIHR makes the following recommendations to further strengthen the Bill in accordance with international standards, OSCE human dimension commitments and good practices:

A. To consider supplementing the overall approach of the Bill with a broader rights-based and risk-based approach grounded in privacy-, safety- and security-by-design principles to ensure fair, accessible and safe digital services for children as well as other users; [para. 33]

B. To include in Article 1 a general children's rights clause, which should provide that all measures under the Bill are implemented in accordance with the best interests of the child, taking into account the child's evolving capacities, development needs and participation rights, while complying with the obligation to respect, protect and fulfil all children's rights online, including the rights to non-discrimination, privacy and data protection, freedom of expression and access to information, the rights to education, health and development, participation, protection from violence as well as access to effective remedies; [para. 31]

C. To ensure that the scope of the Bill in Article 2 is more precisely defined, by clarifying key concepts such as "*harm to the physical or mental development of children*" and more clearly differentiating between categories of digital services and platforms taking into account the nature and level of risk they may present to children for the purposes of determining the applicable obligations under the Bill, including the necessity and proportionality of age verification mechanisms; [paras. 37 and 39]

D. To clarify under Article 8 the key features that age verification method should satisfy, beyond reliability, including accuracy, not easily circumventable, non-intrusiveness and non-discriminatory, in particular to avoid an exclusive dependence on state-issued digital credentials which may risk indirect exclusion of certain groups – such as undocumented children, asylum-seekers, refugees, or

individuals lacking access to digital identity infrastructure, with further elaboration as to the meaning of such requirements, while requiring compliance with principles of anonymity, decentralization, and independent oversight; [para. 44]

E. To consider revising Article 5 (3) to ensure that any restriction on access for children under 13 is narrowly tailored to specific and demonstrable risks stemming from content exposure as well as systemic and design-related features of specific categories of digital platforms and services, including those that may contribute to excessive engagement, addiction or dependency, also considering the distinct and potentially heightened risks posed for children by generative artificial intelligence systems and similar technologies, while ensuring that aged-based access restrictions are differentiated by category of digital platform and services and corresponding risks, while explicitly safeguarding children's continued access to age-appropriate digital services in accordance with their evolving capacities, and guaranteeing the exercise of their rights; [para. 56]

F. To amend Article 9 of the Bill to include clear procedural and substantive safeguards specifying that suspension or de-indexing should be a measure of last resort and decisions of the competent authorities should be reasoned, based on an assessment of their potential impact on lawful expression and access to information, made publicly available, and preceded by notice unless urgent action is strictly necessary, while ensuring that judicial authorization or prompt judicial review is available and strictly listing the types of "urgent precautionary measures" the National Communications Authority may order under Article 9 (2) (c) of the Bill; [para. 73]

G. To amend Article 10 to clarify the meaning of "non-addictive algorithmic recommendations", including by incorporating explicit requirements ensuring that recommender systems for minors (i) are not primarily optimized for engagement time; (ii) do not amplify harmful or age-inappropriate content; (iii) include a non-profiling-based recommendation option; (iv) are transparent and explainable in age-appropriate language; and (v) are subject to independent risk assessment and audit; [para. 75]

H. To ensure that human review is available in addition to automated content review and any other relevant tools for reported accounts or content that the provider suspects may pose a risk of harm to minors' privacy, safety or security, while ensuring that any automated content moderation does not promote over-blocking, and does not unduly undermine the confidentiality of interpersonal communications; [paras. 83 and 85]

I. To revise Article 12 to ensure that obligations relating to the detection, blocking and reporting of harmful content are clearly defined, strictly limited to identifiable unlawful or high-risk content, and applied in a manner consistent with the principles of legal certainty, necessity and proportionality, in particular by further specifying the notions of "violent or sexual material", "aggressive content", "cyberbullying" and "suspicious contacts"; reporting mechanisms should be accessible, simple and child-friendly; [para. 85]

J. To ensure that the development and adoption process of the Bill, as well as design of age-verification mechanisms, are subject to inclusive, extensive, effective and meaningful consultations, including with child-rights organizations and parents'

organizations, and as appropriate and relevant, children – using age-appropriate formats reflecting their evolving capacities. [paras. 68 and 93-94]

These and additional recommendations, are included throughout the text of this Urgent Opinion, highlighted in bold.

As part of its mandate to assist OSCE participating States in implementing their OSCE human dimension commitments, ODIHR reviews, upon request, draft and existing laws to assess their compliance with international human rights standards and OSCE commitments and provides concrete recommendations for improvement.

TABLE OF CONTENTS

I. INTRODUCTION

1. On 24 April 2026, the President of the Committee on Constitutional Affairs, Rights, Freedoms and Guarantees of the Assembly of the Republic of Portugal sent to the OSCE Office for Democratic Institutions and Human Rights (hereinafter "ODIHR") a request for a legal review of the Bill No. 398/XVII/1 on Measures to Protect Children in Digital Environments (hereinafter "the Bill").
2. On 8 May 2026, ODIHR responded to this request, confirming the Office's readiness to prepare a legal opinion on the Bill to assess its compliance with international human rights standards and OSCE human dimension commitments. Given the subject-matter, in line with established practice, ODIHR invited the Office of the OSCE Representative on Freedom of the Media (RFoM) to contribute to this legal opinion via peer review. The peer review does not imply endorsement by the OSCE RFoM of all views, findings and recommendations contained in the Urgent Opinion.
3. On 11 May 2026, the requester informed ODIHR that the legal analysis was required as a matter of urgency, given that the parliamentary process on the Bill had already been initiated. In light of this request, ODIHR agreed to expedite the preparation of the legal analysis and to issue an Urgent Opinion on the Bill, which does not provide a detailed analysis of all the provisions of the Bill, but primarily focuses on the most critical provisions. The absence of comments on certain provisions of the Bill should not be interpreted as an endorsement of these provisions.
4. This Urgent Opinion was prepared in response to the above request. ODIHR conducted this assessment within its general mandate to assist OSCE participating States in the implementation of their OSCE human dimension commitments.[1]

II. SCOPE OF THE URGENT OPINION

5. The scope of this Urgent Opinion covers only the Bill submitted for review. Thus limited, it does not constitute a full or comprehensive review of the entire legal and institutional framework governing online platforms and digital services, the right to freedom of expression and to receive information, access to the Internet and freedom of the media, as well as child protection in Portugal.
6. The Urgent Opinion raises key issues and highlights areas of concern. In the interest of conciseness, it focuses more on those provisions that require amendments or improvements than on the positive aspects of the Bill. The ensuing legal analysis is based on international and regional human rights standards, norms and recommendations, as well as relevant OSCE human dimension commitments. It also highlights, as appropriate,

1 See, in particular, CSCE/OSCE, Document of the Copenhagen Meeting of the Conference on the Human Dimension of the CSCE (Copenhagen Document), 29 June 1990, para. 9.1; Document of the Moscow Meeting of the Conference on the Human Dimension of the CSCE, (Moscow Document), 3 October, 1991, paras. 9.1 and 26; and CSCE Budapest Document 1994, Towards a Genuine Partnership in a New Era (Budapest Document), CSCE/OSCE, 21 December 1994, Chapter VIII, para. 36. See also OSCE Ministerial Council Decision No. 3/18, "Safety of Journalists", 12 December 2018, p. 3, which calls upon OSCE participating States to *"[b]ring their laws, policies and practices, pertaining to media freedom, fully in compliance with their international obligations and commitments and to review and, where necessary, repeal or amend them so that they do not limit the ability of journalists to perform their work independently and without undue interference (…).*" See also Copenhagen 1997 (Annex 1: Permanent Council Decision No. 193, Mandate of the OSCE Representative on Freedom of the Media).

good practices from other OSCE participating States in this field. When referring to national legislation, ODIHR and RFoM do not advocate for any specific country model but rather focus on providing clear information about applicable international standards while illustrating how they are implemented in practice in certain national laws. Any country example should be approached with caution since it cannot necessarily be replicated in another country and has always to be considered in light of the broader national institutional and legal framework, as well as country context and political culture.

7. Moreover, in accordance with the Convention on the Elimination of All Forms of Discrimination against Women[2] (hereinafter "CEDAW") and the 2004 OSCE Action Plan for the Promotion of Gender Equality[3] and commitments to mainstream gender into OSCE activities, programmes and projects, the Urgent Opinion integrates, as appropriate, a gender and diversity perspective.

8. In view of the above, ODIHR stresses that this review does not prevent ODIHR from formulating additional written or oral recommendations or comments on respective subject matters in Portugal in the future.

III. LEGAL ANALYSIS AND RECOMMENDATIONS

1. RELEVANT INTERNATIONAL HUMAN RIGHTS STANDARDS AND OSCE HUMAN DIMENSION COMMITMENTS

1.1. Rights and Protection of Children

9. Children are independent holders of human rights and are entitled to the full range of rights guaranteed under international human rights law, which applies to "everyone". In accordance with the United Nations Convention on the Rights of the Child (CRC), States Parties must ensure that legislative, policy and regulatory measures pertaining to children are designed, implemented and assessed in a manner that respects, protects and fulfils children's rights, including in the digital environment.[4] While international human rights instruments establish the universal human rights framework applicable to all persons, including children, the CRC further elaborates how those rights are to be applied when the right-holder is a child, especially in light of children's evolving capacities, best interests, developmental needs and participation rights.

10. More specifically, Article 3 of the CRC requires that the best interests of the child be a primary consideration in all actions concerning children, while Article 5 recognizes the responsibilities of parents and caregivers to provide appropriate guidance consistent with the evolving capacities of the child. Article 12 of the CRC further guarantees the right of children capable of forming their own views to express those views freely on all matters affecting them, with such views being given due weight in accordance with the age and

2 See *UN Convention on the Elimination of All Forms of Discrimination against Women* (hereinafter "CEDAW"), adopted by General Assembly resolution 34/180 on 18 December 1979. Portugal deposited its instrument of ratification of this Convention on 30 July 1980.
3 See *OSCE Action Plan for the Promotion of Gender Equality, adopted by Decision No. 14/04, MC.DEC/14/04* (2004), para. 32.
4 See UN *Convention of the Rights of the Child* (CRC), adopted by General Assembly resolution 44/25 of 20 November 1989, entry into force 2 September 1990. Portugal ratified the CRC on 21 September 1990. See also UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*.

maturity of the child. In addition, the third Optional Protocol to the CRC[5] is also of relevance to this legal review to the extent that it concerns the prevention of and protection from the sexual exploitation and sexual abuse of children, including in the digital environment.[6]

11. In the General Comment No. 25 (2021), the UN Committee on the Rights of the Child elaborated further specific guidance on relevant legislative, policy and other measures to ensure full compliance with CRC and its Protocols' obligations in the light of the opportunities, risks and challenges in promoting, respecting, protecting and fulfilling all children's rights in the digital environment.[7]

12. At the Council of Europe level, beyond the rights guaranteed by the European Convention on Human Rights (ECHR) to everyone, including children, there are a number of standard-setting texts that aim to promote and protect children's rights. The European Social Charter contains specific rights relating exclusively to children, including the right of children and young persons to protection (Article 7) and the right of children and young persons to social, legal and economic protection (Article 17).[8] In addition, the CoE Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) [9] and the Convention on Preventing and Combating Violence against Women and Domestic Violence (Istanbul Convention)[10] are also of relevance. The *2018 CoE Recommendation CM/Rec(2018)7 on the Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment*[11] and 2025 *CoE Thematic Guidance on Safeguarding Children from the Risks of Accessing Online Pornographic Content*[12] also constitute useful reference materials.

13. Article 24 of the Charter of Fundamental Rights of the European Union (EU) further guarantees the "*right to such protection and care as is necessary for their well-being*", underlying that *"[t]hey may express their views freely"* and that *"[s]uch views shall be taken into consideration on matters which concern them in accordance with their age and maturity"*. Article 24 (2) further underlines that *"[i]n all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration*".[13]

14. At the OSCE level, a number of OSCE commitments relate to the protection of children from sexual exploitation, including in the digital environment, and the role of youth in contributing to peace and security efforts.[14] The OSCE Representative on Freedom of the

5 See UN *Convention of the Rights of the Child* (CRC), adopted by General Assembly resolution 44/25 of 20 November 1989, entry into force 2 September 1990, ratified by Portugal on 21 September 1990; and *Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography"*, ratified by Portugal on 16 May 2003. See also UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*.

6 See UN *Convention of the Rights of the Child* (CRC), adopted by General Assembly resolution 44/25 of 20 November 1989, entry into force 2 September 1990. Portugal ratified the CRC on 21 September 1990. See also UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*.

7 See UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*.

8 See CoE, *European Social Charter* (revised 1996), was ratified by Portugal on 30 May 2022.

9 See CoE, *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse* (Lanzarote Convention), was ratified by Portugal on 23 August 2012.

10 See CoE, *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201) (Istanbul Convention)*, was ratified by Portugal on 5 February 2013.

11 See CoE, Committee of Ministers, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment (4 July 2018), *Recommendation CM/Rec(2018)7*.

12 See CoE, *Thematic Guidance on Safeguarding Children from the Risks of Accessing Online Pornographic Content*, May 2025.

13 See Article 24 of the *Charter of Fundamental Rights of the European Union* (EU), OJ C 326, 26 October 2012.

14 See, in particular, OSCE Decision No.7/17, Strengthening Efforts to Combat All forms of Child Trafficking, Including for Sexual Exploitation, as well as Other Forms of Sexual Exploitation of Children; Decision No. 15/06 on Combating Sexual Exploitation of Children; and Decision No. 9/07 on Combating Sexual Exploitation of Children on the Internet.

Media (RFoM) together with the freedom of expression mandate holders from the UN, the African Commission on Human and Peoples' Rights (African Union) and the Organization of American States (hereinafter "International Freedom of Expression Mandate-Holders"), have recently adopted the *2026 Joint Declaration on the Right to Freedom of Expression and Access to Information of Children in the Digital Age* (hereinafter "2026 Joint Declaration"), which provides crucial recommendations regarding the broader legal and policy framework and measures necessary to ensure that the online environment is fair, accessible, safe and secure for ensuring the protection of children, but also other users, while protecting their rights.[15]

15. In light of the foregoing, measures intended to protect children online should therefore be evaluated not only in light of their protective aims, but also with regard to their impact on children's rights, including their rights to freedom of expression, including the right to seek, impart and receive information, to participation, freedoms of peaceful assembly and of association, education, health and development, non-discrimination, protection from violence but also the rights to respect for private and family life, and personal data protection.

1.2. Right to Freedom of Expression and Access to Information

16. The right to freedom of expression and to seek, receive and impart information is a fundamental right, as well as an enabler of other human rights and fundamental freedoms and a guardian of democratic values.[16] This right is enshrined in Article 19 of the Universal Declaration of Human Rights (UDHR).[17] Article 19 of the International Covenant on Civil and Political Rights (ICCPR) further provides that "*everyone shall have the right to hold opinions without interference*" and that "*everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice"*.[18] Article 19 (2) of the ICCPR establishes the principle of medium neutrality by noting that these rights can be exercised regardless of the medium used. The jurisprudence of the UN Human Rights Committee (UN HRC) as well as its General Comment No. 34 on Article 19 of the ICCPR also offer authoritative interpretation of the nature and scope of the right to freedom of expression and access to information.[19] Article 13 of the CRC guarantees the child's right to freedom of expression, including the freedom to seek, receive and impart

15 See *Joint Declaration on the Right to Freedom of Expression and Access to Information of Children in the Digital Age*, International Mandate-Holders on Freedom of Expression, 01 June 2026.

16 See UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur and the African Commission Special Rapporteur on Freedom of Expression and Access to Information (hereinafter "International Mandate-Holders on Freedom of Expression"), *Joint Declaration on Media Freedom and Democracy*, 2 May 2023.

17 See the *Universal Declaration on Human Rights* (UDHR), adopted by General Assembly resolution 217 A on 10 December 1948.

18 Article 19 of the *International Covenant on Civil and Political Rights* (ICCPR) provides that "*everyone shall have the right to hold opinions without interference*" and that *"everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."* According to Article 19 (3) of the ICCPR: *"The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals."*

19 See UN Human Rights Committee, *General Comment No. 34* on Article 19 of the ICCPR, CCPR/C/GC/34, para. 11, where the UN Human Rights Committee further elaborates that "*[f]reedom of expression is a necessary condition for the realization of the principles of transparency and accountability that are, in turn, essential for the promotion and protection of human rights*" and protects "*even expression that may be regarded as deeply offensive, although such expression may be restricted in accordance with the provisions of article 19, paragraph 3 and article 20."*

information and ideas of all kinds, regardless of frontiers, through any media of the child's choice, closely mirroring Article 19 of the ICCPR.[20]

17. With respect to restrictions to the right to access information, Article 13 (2) of the CRC, similarly to Article 19 (3) of the ICCPR, requires that they be provided by law (test of legality), pursue one of the legitimate aims listed exhaustively in the text of Article 13 (2) (and Article 19 (3) of the ICCPR) (test of legitimacy), be necessary and proportionate, and constitute the least intrusive measure among those effective enough to reach the designated objective (test of necessity and proportionality). In addition, pursuant to Article 2 of the CRC, restrictions shall not be discriminatory. The requirement that restrictions to freedom of expression need to be provided by law means not only that restrictions need to be based on a law, but such law must also be precise and foreseeable. Laws need to be formulated with sufficient precision to enable individuals to regulate their conduct accordingly.[21] Restrictions must be applied only for those purposes for which they were prescribed and must be directly related to the specific aim(s) they are pursuing. Additionally, Article 20 of the ICCPR requires states to outlaw any propaganda for war and "*any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence*".

18. Article 17 of the CRC recognizes the important function performed by the media and requires States Parties to ensure that children have access to information and material from a diversity of national and international sources, especially those aimed at promoting their social, spiritual and moral well-being and physical and mental health. Moreover, the Committee on the Rights of the Child reaffirmed the importance of access to information in General Comment No. 4 on adolescent health and development (2023),[22] underlining that *"[a]dolescents have the right to access adequate information essential for their health and development and for their ability to participate meaningfully in society"*. The Committee further emphasized that *"it is the obligation of States parties to ensure that all adolescent girls and boys, both in and out of school, are provided with, and not denied, accurate and appropriate information on how to protect their health and development and practise healthy behaviours."* In addition, it is essential that children also have access to quality and evidence-based information and education on sexual and reproductive health.[23]

19. At the Council of Europe level, Article 10 of the European Convention on Human Rights (ECHR) guarantees "*the right to freedom of expression, including the freedom to hold opinions and to seek, receive and impart information and ideas without interference by public authority and regardless of frontiers*". The protection afforded by Article 10 extends not only to information and ideas that are favorably received or regarded as inoffensive, but also to those that may offend, shock or disturb the State or any part of the population, as consistently affirmed in the jurisprudence of the European Court of

20 See *Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography"*, which was ratified by Portugal on 16 May 2003.

21 See *UN Human Rights Committee, General Comment No. 34* "on Article 19 Freedoms of Opinion and Expression of the ICCPR", CCPR/C/GC/34, 12 September 2011, para. 25, which states: "*a norm, to be characterized as a 'law', must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public. A law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution. Laws must provide sufficient guidance to those charged with their execution to enable them to ascertain what sorts of expression are properly restricted and what sorts are not.*" See also, e.g., ODIHR, *Guidelines on Democratic Lawmaking for Better Laws*, ODIHR, 16 January 2024, para. 12 and Principle 16; and Venice Commission, *Updated Rule of Law Checklist*, CDL-AD(2025)002-e, 16 December 2025.

22 See *CRC General Comment No. 4: Adolescent Health and Development in the Context of the Convention on the Rights of the Child*, adopted at the Thirty-third Session of the Committee on the Rights of the Child, on 1 July 2003.

23 See UN Human Rights Committee, *General Comment No. 36 on article 6: right to life (2019)*, CCPR/C/GC/36, para. 8.

Human Rights (ECtHR).[24] In addition, , a number of CoE Recommendations are relevant to this Urgent Opinion and may serve as examples of regional good practice, such as the Recommendations on the roles and responsibilities of internet intermediaries,[25] on the impacts of digital technologies on freedom of expression,[26] on the human rights impacts of algorithmic systems,[27] on human rights for Internet users,[28] on a new notion of media,[29] on gender equality and the media[30] and on principles for media and communication governance.[31] In addition, the 2024 Council of Europe Framework Convention on Artificial Intelligence is also of interest, though Portugal has not signed nor ratified it, since it requires States Parties to take due account of any specific needs and vulnerabilities in relation to respect for the rights, including children (Article 18) and to adopt or maintain measures for the identification, assessment, prevention and mitigation of risks posed by artificial intelligence systems by considering actual and potential impacts to human rights, democracy and the rule of law (Article 16).[32]

20. Comparable freedom of expression and access to information guarantees are provided under Article 11 (1) of the Charter of Fundamental Rights of the European Union (EU), with Article 11 (2) further emphasizing the respect for the freedom and pluralism of the media.[33] These provisions apply equally in the online environment and protect not only the dissemination of information but also the right of individuals, including children, to access and receive information through digital means.

21. At the OSCE level, a number of commitments proclaim the right of everyone to freedom of expression and to receive and impart information, as well as the right of the media to collect and disseminate information, news and opinion, underlining the essential role of independent and pluralistic media.[34] In addition, in its Decision 3/18, adopted on 7 December 2018 on the Safety of Journalists, the OSCE Ministerial Council called upon the OSCE participating States to fully implement all OSCE commitments and

---

24 See e.g., ECtHR, *Handyside v. United Kingdom*, no. 5493/72, 7 December 1976, para. 49, where the ECtHR held that Article 10 of the ECHR protects "*not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no 'democratic society'*"; and *Bodrožić v. Serbia*, no. 32550/05, 23 June 2009, paras. 46 and 56.

25 See CoE, *Recommendation CM/Rec(2018)2* of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries, adopted on 7 march 2018.

26 See CoE, *Recommendation CM/Rec(2022)13* of the Committee of Ministers to member States on the impacts of digital technologies on freedom of expression, adopted on 6 April 2022.

27 See CoE, *Recommendation CM/Rec(2020)1* of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, adopted on 8 April 2020.

28 See CoE, *Recommendation CM/Rec(2014)6* of the Committee of Ministers to member States on a Guide to human rights for Internet users, Council of Europe, Committee of Ministers, adopted on 16 April 2014.

29 See CoE, *Recommendation CM/REC(2011)7* of the Committee of Ministers to member States on a new notion of media, adopted on 21 September 2011.

30 See CoE, *Recommendation CM/Rec(2013)1* of the Committee of Ministers to member States on gender equality and media, adopted on 10 July 2013.

31 See CoE, *Recommendation CM/Rec(2022)11* of the Committee of Ministers to member States on principles for media and communication governance, adopted on 6 April 2022.

32 See CoE, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, Vilnius, 5.IX.2024 (CETS 225). While Portugal is not currently a Party to the Framework Convention, as an EU Member State, it is subject to the EU legal framework governing artificial intelligence, and the European Union has itself become a Party to the Convention.

33 See the *Charter of Fundamental Rights of the European Union* (EU), OJ C 326, 26 October 2012.

34 See in particular OSCE, *Document of the Copenhagen Meeting of the Conference on the Human Dimension of the CSCE* (the 1990 Copenhagen Document), which states that "*[t]his right will include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. The exercise of this right may be subject only to such restrictions as are prescribed by law and are consistent with international standards."* The OSCE participating States also reaffirmed "*the right to freedom of expression, including the right to communication and the right of the media to collect, report and disseminate information, news and opinion*" in OSCE, *Document of the Moscow Meeting of the Conference on the Human Dimension of the CSCE*, (the 1991 Moscow Document). Moreover, in 1994, the OSCE participating States reaffirmed that "*freedom of expression is a fundamental human right and a basic component of a democratic society*" committing to "*take as their guiding principle that they will safeguard this right*" and emphasizing in this respect, that "*independent and pluralistic media are essential to a free and open society and accountable systems of government*"; see OSCE, *CSCE Budapest Document 1994, Towards a Genuine Partnership in a New Era* (Budapest, 21 December 1994), para. 36.

international obligations related to freedom of expression and media freedom and to make their laws, policies and practices pertaining to media freedom fully compliant with their international obligations.[35] Within the OSCE, the RFoM is specifically mandated to observe relevant media developments in all OSCE participating States and to advocate and promote full compliance with OSCE principles and commitments regarding freedom of expression and media freedom.[36] The OSCE RFoM together with the International Freedom of Expression Mandate-Holders have adopted a series of thematic Joint Declarations, which offer practical guidance covering current universal challenges to freedom of expression and freedom of the media,[37] including the above-mentioned 2026 Joint Declaration.[38] In particular, the latter underlines that *"[i]t is the responsibility of the State to regulate the digital environment in line with international human rights standards relating to children's rights; to protect children's rights and ensure that the digital environment is safe and accessible to all children; and to engage in awareness raising, digital literacy and other educational efforts to empower children to use the digital environment*" and "*Legislation on definitions, agreed standards and independent regulatory oversight of technical safety measures are necessary to ensure that children, parents/guardians and digital technology companies have confidence in their use*".[39] The 2026 Joint Declaration also specifically emphasizes that *"[r]estrictions to children's freedom of expression and access to information in the digital environment are only acceptable if they meet the requirements of the tripartite test on legality, legitimacy of aim, and necessity and proportionality set out in the International Covenant on Civil and Political Rights and comply with the provisions of the UNCRC*".[40]

1.3. Principles governing privacy and data protection in digital regulation

22. The right to respect for private and family life is guaranteed under Article 17 of the ICCPR and Article 8 of the ECHR. Article 16 of the CRC also protects children against arbitrary or unlawful interference with their privacy, family, home or correspondence. The CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its Protocol, although the latter is not yet in force, are also of particular relevance.[41]

23. Within the EU framework, Articles 7 and 8 of the EU Charter of Fundamental Rights guarantee the rights to respect for private life and protection of personal data.[42] These guarantees are further developed in the secondary EU law, including Regulation (EU) 2016/679, General Data Protection Regulation (GDPR).[43] Article 8 of the GDPR permits EU Member States to establish a lower age threshold for children's consent in relation to the processing of personal data, provided that such threshold is not set below the age of

35 See OSCE Ministerial Council Decision No. 3/18, "Safety of Journalists", 12 December 2018, para. 2.
36 See Copenhagen 1997 (Annex 1: *Permanent Council Decision No. 193*, Mandate of the OSCE Representative on Freedom of the Media).
37 See *Joint Declarations*, UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur and the African Commission Special Rapporteur on Freedom of Expression and Access to Information (hereinafter "International Mandate-Holders on Freedom of Expression").
38 See *Joint Declaration on the Right to Freedom of Expression and Access to Information of Children in the Digital Age*, International Mandate-Holders on Freedom of Expression, 01 June 2026.
39 *Ibid. 2026 Joint Declaration*, paras. 1 (e) and 6 (e).
40 See *Joint Declaration on the Right to Freedom of Expression and Access to Information of Children in the Digital Age*, International Mandate-Holders on Freedom of Expression, 01 June 2026, para. 1 (d).
41 See, Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS 108), ratified by Portugal on 2 September 1993, and Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223), ratified by Portugal on 18 October 2023 (to enter into force once 38 Parties to the Convention have ratified the Protocol) and *Explanatory Report – CETS 223 – Automatic Processing of Personal Data (Amending Protocol)*, 10 October 2018.
42 See Articles 7 and 8 of the *Charter of Fundamental Rights of the EU*.
43 See *Regulation (EU) 2016/679, General Data Protection Regulation* (GDPR).

13. The European Data Protection Board (EDPB), in Statement 1/2025 on Age Assurance, has cautioned that age assurance mechanisms may pose significant risks to the rights and freedoms of users, including children, and has emphasized the need for a risk-based approach supported by a data protection impact assessment and the use of the least intrusive means available.[44]

24. More broadly, the GDPR establishes core data protection principles under Article 5 (1), including lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability, all of which are particularly relevant in the design and deployment of digital services targeting or accessible to children. In addition, Article 25 of the GDPR requires the implementation of data protection by design and by default, reinforcing the obligation to integrate privacy safeguards into the architecture of digital systems from the outset. The application of these principles must also be interpreted in light of the proportionality requirement under Article 52 (1) of the EU Charter of Fundamental Rights, which requires that any limitation on fundamental rights be necessary and genuinely meet objectives of general interest.

25. Within the EU framework, the Digital Services Act, Regulation (EU) 2022/206 (DSA) contains additional safeguards concerning the protection of minors online and freedom of expression.[45] In particular, Article 8 of the DSA prohibits the imposition of general monitoring obligations on intermediary service providers. Article 28 requires providers of online platforms accessible to minors to implement appropriate and proportionate measures to ensure a high level of privacy, safety and security for children. In July 2025, the European Commission adopted the Guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 (4) of the DSA, providing further interpretative guidance regarding compliance with these obligations.[46] These obligations must be read in conjunction with the DSA's systemic risk framework under Articles 34-35, which requires very large online platforms to assess and mitigate systemic risks to fundamental rights, including the rights of the child, privacy, and freedom of expression.[47] The interpretation of "appropriate and proportionate" measures under Article 28 DSA is therefore closely linked to a balancing exercise between competing fundamental rights, as reflected in Articles 16 and 17 of the EU Charter of Fundamental Rights, and must avoid measures that result in unjustified surveillance or excessive processing of minors' personal data.[48] On 29 April 2026, the Commission also adopted *Recommendation (EU) 2026/1035 on the establishment of a common EU framework for age verification technologies* aimed at introducing anonymous tools for the purpose of age verification.[49]

26. The 2026 Joint Declaration also underlines the need for a privacy-compliant digital environment, and the importance of "*[e]mbedding privacy by design, for example collecting the minimum necessary data, setting accounts to private by default, refraining from using data to profile children for targeted advertisements, and providing*

44 See the *European Data Protection Board* (EDPB) and EDPB Statement 1/2025 on Age Assurance.
45 The *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 or "DSA").
46 See European Commission, 2025 *Guidelines on the Protection of Minors Online pursuant to Article 28 (4) DSA*.
47 See the *Regulation (EU) 2022/2065* (DSA), Articles 34–35.
48 See the *Charter of Fundamental Rights of the European Union* (2012/C 326/02), Articles 7, 8, 16 and 17.
49 See European Commission, *Recommendation (EU) 2026/1035 of 29 April 2026 on the establishment of a common EU framework for age verification technologies*.

information about data practices in a way that is clear, accessible, and understandable to children".[50]

2. BACKGROUND

27. The Bill No. 398/XVII/1 on Measures to Protect Children in Digital Environments, was introduced in the parliament in February 2026 by the parliamentary group of the Social Democratic Party (PSD).[51] The proposal emerged amid increasing concerns regarding the effects of social media, online platforms, and digital services on children's wellbeing, privacy, and development. The Bill proposes a regulatory framework centred on an increase of the minimum digital age from 13 to 16 for independent access to platforms and online services covered by the Bill, mandatory parental consent for younger users aged 13-16 and a minimum access age of 13 for covered platforms and services – with some exceptions, age-verification requirements, and enhanced obligations on digital service providers to protect minors. The initiative was approved at first reading on 12 February 2026 and subsequently entered the committee stage for public consultation.

28. The Explanatory Memorandum to the Bill underlines that over the past two decades, the rapid expansion of digital technologies and social media platforms has fundamentally transformed the environment in which children exercise their rights, including their rights to freedom of expression, access to information, privacy and participation. International human rights bodies have increasingly recognized that while the digital environment offers significant opportunities for children for learning, communication and participation and for exercising their rights, it also presents specific risks for them, including exposure to harmful content, excessive commercial influence, manipulation through design features, cyberbullying and other forms of online harm.[52] In this context, States have positive obligations to take appropriate measures to ensure that children are effectively protected in the digital environment while respecting their autonomy and evolving capacities, including those of children with disabilities or in vulnerable situations, and complying with their obligations to respect, protect and fulfil all children's rights in the digital environment.

29. As outlined in Sub-Sections 1.1 and 1.2 *supra*, any legislation or other measures aimed at protecting children in the digital environment must reflect a proportionate balance between protection and the obligation to respect, protect and fulfil children's rights online, consistent with children's evolving capacities, best interests, developmental needs and participation rights. Against this background, the Explanatory Memorandum to the Bill underlines that international and EU policy developments increasingly encourage the adoption of measures aimed at strengthening the protection of minors online, including through platform accountability, transparency of algorithmic systems, age-appropriate design and effective safeguards against harmful content and practices. The DSA and related guidance on the protection of minors online reflect this approach by requiring

50 See *Joint Declaration on the Right to Freedom of Expression and Access to Information of Children in the Digital Age*, International Mandate-Holders on Freedom of Expression, 01 June 2026, para. 4 (b) (5).
51 See the *Bill*, submitted to the Parliament.
52 See UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*, paras. 3 and 7. See also See *Joint Declaration on the Right to Freedom of Expression and Access to Information of Children in the Digital Age*, International Mandate-Holders on Freedom of Expression, 01 June 2026.

proportionate, risk-based mitigation measures tailored to the nature and severity of risks posed by specific services.[53]

3. THE PURPOSE AND THE SCOPE OF THE BILL

30. Under Article 1, the purpose of the Bill is to establish measures to protect children in digital environments. International standards recognize that children in digital environments are not only beneficiaries of protection measures but also holders of rights that must be respected, protected and fulfilled. In particular, the UN Committee on the Rights of the Child, in General Comment No. 25 (2021) on children's rights in relation to the digital environment, affirms that the CRC applies fully in digital contexts and requires States to ensure that measures adopted to protect children do not unduly restrict their rights, including their rights to privacy, access to information, freedom of expression, participation, education, and effective remedies.[54] Similarly, the CoE Recommendation CM/Rec(2018)7 on the Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment emphasises that all measures affecting children online should be guided by the principles of the best interests of the child, evolving capacities, non-discrimination, and the child's right to be heard.[55]

31. Hence, while the Bill rightly places significant emphasis on the State's duty to protect children in digital environments, there could be a more proportionate balance between protection objectives and exercise of children's rights in digital environments. **Overall, the Bill could more clearly reflect an approach grounded in human rights by including a general children's rights clause in Article 1. Such a clause should provide that all measures under the Bill are implemented in accordance with the best interests of the child, taking into account the child's evolving capacities, development needs and participation rights, while complying with the obligation to respect, protect and fulfil all children's rights online, including the rights to non-discrimination, privacy and data protection, freedom of expression and access to information, the rights to education, health and development, participation, protection from violence as well as access to effective remedies.** In addition, the Bill would benefit from a more comprehensive assessment of its potential impact on the exercise of the full range of children's rights, the evolving capacities of children and their diversity, also taking into account that mandatory-age-verification measures will affect all users, not just children, and should be approached with caution (see Sub-Section 5.3 *infra*).

53 See e.g., the *Regulation (EU) 2022/2065* (DSA), Articles 34–35; UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*; and *Joint Declaration on the Right to Freedom of Expression and Access to Information of Children in the Digital Age*, International Mandate-Holders on Freedom of Expression, 01 June 2026, para. 6 (g).

54 See the UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*, paras. 12–18, 24–34, 40–46 and 107–114. 21. Similarly, Article 28 of the *DSA* expressly requires providers of online platforms accessible to minors to put in place appropriate and proportionate measures to ensure a high level of privacy, safety and security for children.

55 See CoE, Committee of Ministers, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment (4 July 2018), *Recommendation CM/Rec(2018)7*, paras. 10–17 and Chapter II (Fundamental Principles).

32. The risks of children's exposure to harmful content, including grooming,[56] disinformation,[57] manipulative design, pervasive data collection and other digital risks in today's online ecosystem are real and well-founded, and need to be addressed. In this respect, the initiative to develop the Bill is particularly timely and reflects an effort to reinforce protections for children and to mitigate risks that may affect their wellbeing, privacy, and development in digital environments. In addition, to ensure effective protection of children but also of all users, it is also important to more comprehensively target systemic issues linked to specific platform design choices and business models in addition to aged-based restrictions and potential minimum age for accessing digital services.

33. Increasingly, international and regional bodies recommend considering measures or incentives to ensure that digital technology companies and other relevant actors build privacy-by-design, safety-by-design, and security-by-design features into their systems and platforms and services, as a way to protect children but also other users.[58] **Overall, the proposed Bill could be strengthened by reflecting a more rights-based and risk-based approach grounded in privacy-by-design, safety-by-design, and security-by-design principles and solutions, ensuring fair, accessible, safe and secure digital platforms and services for children and other users**.

34. Article 2 defines the material and personal scope of application of the Bill. Under Article 2.1, the Bill applies to a wide range of digital services, including social media platforms, online gambling and gaming platforms, image and video-sharing services, content-hosting services, communication applications, providers of services and content subject to age restrictions (including violent, addictive or sexual content), as well as app store services and "*any online intermediary services whose nature, characteristics, or content may harm the physical or mental development of children*". Article 2.2 provides that the Bill applies to the above-mentioned providers insofar as they make services available to children residing in Portugal. Article 2.3 excludes from the scope interpersonal electronic communications services, as defined in the Electronic Communications Act, as well as online applications and games of an informational or educational nature specifically designed for children, and platforms intended exclusively for the dissemination of content of clear public interest, particularly in the areas of education and health.

35. While the objective of protecting children online is legitimate and consistent with international human rights standards, the scope defined in Article 2 could be more

56 i.e., the intentional proposal, through information and communication technologies, of an adult to meet a child who has not reached the age of sexual consent for the purpose of committing sexual abuse or exploitation offences, where this proposal has been followed by material acts leading to such a meeting; see Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201), Article 23; see also Explanatory Report to the Lanzarote Convention, paras. 156-161.

57 i.e., verifiably false, inaccurate or misleading information deliberately created and disseminated *to cause harm* or pursue economic or political gain by deceiving the public; see Report on countering disinformation for the promotion and protection of human rights and fundamental freedoms, United Nations, Secretary General, A/77/287, 12 August 2022, para. 42. See also, as a comparison, Action Plan against Disinformation, Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, 2018.

58 See e.g., *Joint Declaration on the Right to Freedom of Expression and Access to Information of Children in the Digital Age*, International Mandate-Holders on Freedom of Expression, 01 June 2026, paras. 1 (f) and 6, which state that "*Digital technology companies and other relevant actors have the responsibility to ensure that relevant platforms and services, including content, advertising and companion services in the digital environment, as well as data mining and processing operations, are in line with international human rights standards relating to children's rights, including safety by design, privacy by design and privacy by default*" and recommends that "*States should ensure that digital technology companies and other relevant actors build safety by design and privacy by design features into their systems and platforms and services, and should diligently enforce this requirement*". See also UN Committee on the Rights of the Child, *General Comment No. 25 on children's rights in relation to the digital environment*, paras. 77, 88 and 116; and CoE, Committee of Ministers, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment (4 July 2018), *Recommendation CM/Rec(2018)7*, paras. 35 and 63; and European Commission, *Guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 (4) of Regulation (EU) 2022/2065*, para. 57 (a); see CoE, *Thematic Guidance on Safeguarding Children from the Risks of Accessing Online Pornographic Content*, May 2025, p. 16.

precisely defined and narrowly circumscribed to comply with the principles of legal certainty, necessity and proportionality.

36. In particular, the formulation in Article 2 (1) (c) of the Bill, referring to "*any online intermediary services whose nature, characteristics, or content may harm the physical or mental development of children*" is broad and imprecise. This means that private actors would need to make *ex ante* determinations as to whether their services may fall within the scope of the legislation on the basis of an undefined and unclear criteria or risk standard of being considered "*harmful to the physical or mental development of children*". For example, social networking platforms, video-sharing services, adult content services, gaming environments, app stores, and messaging services each present distinct risk profiles, which would each require tailored regulatory responses. Conversely, mere conduit services should not automatically be subject to the same obligations as platforms, which have an editorial or curatorial role including through the use of algorithms.[59] State authorities should apply an approach that is graduated and differentiated.[60] International and regional guidance documents tend to distinguish between different categories of risks of harm to children, including contact risks, content risks, conduct risks and health risks, each of which requiring distinct mitigating regulatory and/or other measures.[61] It is also worth referring to international standards that define specific harmful content for children precisely and outline detailed measures.[62]

---

59 See e.g., CoE, *Recommendation CM/Rec(2018)2* of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries, adopted on 7 march 2018, para. 1.3.9; and EU *DSA*, Recitals 19 and 21 and Article 4.

60 See e.g., CoE, *Recommendation CM/Rec(2018)2* of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries, adopted on 7 march 2018, para. 1.3.9.

61 See e.g., CoE, Committee of Ministers, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment (4 July 2018), *Recommendation CM/Rec(2018)7*, para. 50, which mentions contacts risks (including sexual exploitation and abuse, solicitation for sexual purposes (grooming), online recruitment of children for the commission of criminal offences, for participation in extremist political or religious movements or for trafficking purposes), content risks (including the degrading and stereotyped portrayal and over-sexualisation of women and children in particular; the portrayal and glorification of violence and self-harm, in particular suicides; demeaning, discriminatory or racist expressions or apologia for such conduct; advertising, adult content); conduct risks (including bullying, stalking and other forms of harassment, non-consensual dissemination of sexual images, extortion, hate speech, hacking, gambling, illegal downloading or other intellectual property infringements, commercial exploitation); and health risks (including excessive use, sleep deprivation and physical harm). See also UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*, para. 105; and EU *DSA*, Recitals 80 to 83.

62 See e.g., UN General Assembly, *Resolution 78/213 Promotion and protection of human rights in the context of digital technologies*, 22 December 2023, para. 5, the importance of combating all forms of violence in the context of digital technologies, including sexual exploitation and abuse, harassment, stalking, bullying, non-consensual sharing of personal sexually explicit content, threats and acts of sexual and gender-based violence, death threats, arbitrary or unlawful surveillance and tracking, trafficking in persons, extortion, censorship, illegal access to digital accounts, mobile telephones and other electronic devices; in addition, a number of international instruments require the criminalization of the dissemination or communication of certain forms of sexually exploitative content: Articles 2 (c) and 3 (1) (c) of the *Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography"*, ratified by Portugal on 16 May 2003, require the criminalization of "*child sexual exploitation material*"; see also, Article 20 of the *Council of Europe Convention on Protection of Children Against Sexual Exploitation and Sexual Abuse* (Lanzarote Convention) requires the criminalization of intentional conduct, amounting to *"(a) producing child pornography; (b) offering or making available child pornography; (c) distributing or transmitting child pornography; (d) procuring child pornography for oneself or for another person; (e) possessing child pornography; and (f) knowingly obtaining access, through information and communication technologies, to child pornography*" (Council of Europe Convention on Protection of Children Against Sexual Exploitation and Sexual Abuse (Lanzarote Convention), CETS No. 201, Article 20). See also e.g., the UK Online Safety Act which requires risk assessments, content moderation including takedown procedures, restrictions on harmful content (pornography, suicide encouragement, violence, bullying, dangerous stunts), and limits on addictive or manipulative features (e.g., autoplay, streaks); Sec. 61 also defines 'Priority content that is harmful to children' as a series of content such as abusive content targeting one or more protected characteristics, incites hatred against certain protected characteristics, encourages serious violence against a person, is of a bullying nature, depicts real or realistic serious violence or injury against a person, an animal or a fictional creature, encourages dangerous challenges or stunts, ingesting or inhaling harmful substances. See also the EU *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/EU DSA)*, which mandates that providers accessible to minors adopt "appropriate and proportionate measures" for privacy, safety, and security, with detailed guidance issued by the Commission in July 2025 on defaults, recommender system adjustments, and parental controls, among others (see Commission publishes guidelines on the protection of minors | Shaping Europe's digital future: the Guidelines set out key recommendations for service providers, including: making children's accounts private by default; adjusting recommender systems to reduce harmful content and give children greater control over their feeds; enabling children to block or mute others and preventing their addition to groups without consent; banning the downloading or screenshotting of minors' content to prevent the unwanted sharing of

37. In addition, the notion of "physical or mental development of children" is not further defined and may be interpreted in a very expansive manner, potentially encompassing a wide range of lawful digital services with differing functionalities, levels of user interaction, and capacities to implement protective measures. This raises issues under the principle of legal certainty, a core principle under the ICCPR and the ECHR, which requires that the scope of legal obligations be formulated with sufficient precision to enable individuals to foresee, with reasonable clarity, whether and how the law applies to them.[63] In light of the foregoing, **Article 2 (1) (c) should be revised to ensure compliance with the principle of legal certainty by providing sufficiently clear and foreseeable criteria for determining which services fall within the scope of the Bill, including by more precisely defining key concepts such as "harm to the physical or mental development of children".**

38. From the perspective of proportionality, Article 2 establishes a uniform regulatory framework for a wide and diverse categories of digital services that are not comparable in terms of types and levels of risk for children, functionality, or editorial/curatorial roles. Social networking platforms, video-sharing services, gaming environments, adult content services, messaging applications, and hosting or intermediary providers differ significantly in the nature of risks they may pose to children, as well as in their technical and operational capacity to mitigate such risks. A one-size-fits-all approach therefore risks imposing uniform obligations across types of services that differ significantly in their potential to generate or mitigate risks of potential harm, and therefore not warranting the same regulatory response. In this respect, in its Guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 (4) of the DSA, the European Commission specifically notes that the heterogeneous nature of online platforms and diversity of contexts may require distinct approaches, with certain measures being better suited to some platforms over others.[64]

39. In light of the foregoing, **a clearer differentiation of categories of digital services and platforms and corresponding types and levels of risks arising from the nature, design, functionality, scale, and user base of the category of service concerned –** also taking into account the rapidly evolving nature of risks linked to digital environment[65] – **for the purposes of determining the applicable obligations would allow for a more proportionate regulatory framework.** For that purpose, **it is also important that States set up appropriate monitoring and evaluation mechanisms to identify, assess, prevent and mitigate new and emerging risks in the digital environment**.[66]

40. Article 2 (3) specifies that certain digital services fall outside the scope of the Bill (i.e., interpersonal electronic communications services, online applications and games of an informational or educational nature specifically designed for children, and platforms intended exclusively for the dissemination of content of clear public interest, particularly

intimate material; disabling by default features that encourage excessive use, such as streaks, autoplay and push notifications; restricting manipulative commercial practices that promote spending or addictive behaviour; and strengthening moderation, reporting and parental control tools).

63 See Article 19 (3) of the ICCPR and Article 10 (2) of the ECHR; See also UN Human Rights Committee, *General Comment No. 34* on Article 19, para. 25, which provides that "*a norm, to be characterized as a 'law', must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly*".

64 See European Commission, 2025 *Guidelines on the Protection of Minors Online pursuant to Article 28 (4) DSA*, para. 18.

65 See e.g., the *DSA*, Recital 71. See also e.g., CoE, Committee of Ministers, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment (4 July 2018), *Recommendation CM/Rec(2018)7*, paras. 50-54; UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*, para. 14; *Joint Declaration on the Right to Freedom of Expression and Access to Information of Children in the Digital Age*, International Mandate-Holders on Freedom of Expression, 01 June 2026, paras. 4 (b) and 6 (j).

66 See e.g., *Joint Declaration on the Right to Freedom of Expression and Access to Information of Children in the Digital Age*, International Mandate-Holders on Freedom of Expression, 01 June 2026, para. 6 (j).

in the areas of education and health), the wording of such provision is vague and potentially subject to diverging or arbitrary interpretation. In addition, the exception may not adequately capture the variety of potential use of digital services by children to exercise their rights. As noted above, children should not only be protected from illegal or harmful content, and systemic and design-related features that may contribute to excessive engagement, addiction or dependency, but are also the holders of rights, including the rights to freedom of expression, access to information, participation, freedoms of peaceful assembly and of association, education, health and development, non-discrimination, and privacy in the digital environment. Excessively broad or restrictive regulatory measures may therefore risk limiting children's exercise of all of their rights in the digital environment, including lawful access to a wide diversity of information and viewpoints, participation in public discourse, right to leisure and play, and ability to engage in social, educational and cultural life online, among others.[67] International and regional bodies expressly recognize the digital environment as a space in which children exercise their rights and freedoms, and not merely as an environment from which they must be shielded from risk.[68] **It is recommended to review and clarify Article 2 (3) to ensure that the exclusions from the scope of the Bill are sufficiently precise, foreseeable and consistently applicable, and assess whether the current exemptions adequately reflect the diverse ways in which children exercise their rights in the digital environment and associated risks.**

4. DEFINITIONS

41. Article 4 sets out the key definitions, which determine the personal and material scope of the obligations imposed under the Bill. While the use of defined terms is generally welcomed to ensure a structured regulatory framework, several definitions are broad and vague, thereby undermining legal certainty.

42. The definition of "platform accessible to children" appears especially broad. By referring to any online service that, "by its nature, features, or target audience, can be used by children", the definition may potentially encompass a very large category of online services, including services not specifically directed at children and services primarily intended for general audiences. Given that many digital services are technically accessible to minors, the absence of more precise criteria may create uncertainty as to which providers fall within the scope of the Bill and which obligations apply to them.

43. Similarly, the definition of "social networking platform" may capture a broad range of online services beyond traditional social media platforms. Functionalities such as user interaction, communication between users and the ability to post content are common features across numerous digital services, including educational platforms, collaborative tools, gaming environments, discussion forums and certain productivity applications. In

67 See e.g., UN Committee on the Rights of the Child, *General Comment No. 25 on children's rights in relation to the digital environment*, which notes in particular that children should have access to a wide diversity of information, including information held by public bodies, about culture, sports, the arts, health, civil and political affairs and children's rights (para. 51), and that they have the right to culture, leisure and play, as this is essential for their well-being and development (para. 106).

68 See e.g., UN Committee on the Rights of the Child, *General Comment No. 25 on children's rights in relation to the digital environment*; CoE, Committee of Ministers, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment (4 July 2018), *Recommendation CM/Rec(2018)7*, para. 25, which emphasizes that measures aimed at protecting children online should not result in unnecessary or disproportionate restrictions on their rights, including their rights to access information, express views, participate in society and seek support online; *Joint Declaration on the Right to Freedom of Expression and Access to Information of Children in the Digital Age*, International Mandate-Holders on Freedom of Expression, 01 June 2026, para. 2 (d).

the absence of additional limiting criteria, the definition may therefore extend to services that do not present the same types or levels of risk that the Bill is covering.

44. The definition of "age verification" refers to a technical process designed to "reliably determine" whether a user meets the required age criteria. However, the provision does not clarify the level of reliability required, the applicable safeguards, or the relationship between age verification and data protection obligations. The absence of clearer safeguards may create risks for privacy and personal data protection, particularly where age verification systems involve the processing of sensitive or identity-related information.[69] Although Article 4 (g) introduces the concept of a "*privacy-preserving age verification system*", this definition similarly does not specify the technical or legal standards required to ensure effective privacy protection nor **the key features that age verification method should satisfy, beyond reliability, including accuracy, not easily circumventable, non-intrusiveness and non-discriminatory, with further elaboration as to the meaning of such requirements**.[70] In addition, the Bill does not clarify whether such systems **must comply with principles of anonymity, decentralization, or independent oversight**, nor does it specify whether less intrusive forms of age assurance should be prioritized where appropriate, and should be supplemented in this respect.[71] The *Recommendation (EU) 2026/1035 on the establishment of a common EU framework for age verification technologies* aimed at introducing anonymous tools for the purpose of age verification, may serve as a useful reference in this respect.[72]

45. The definition of "addictive design" covers a broad range of interface techniques and algorithmic features, including autoplay functions, continuous information flows, infinite scroll mechanisms, compulsive notifications and digital reward mechanisms such as loot boxes. While such features contribute to compulsive or excessive use patterns, some of them approached in the context of accessibility by persons with disability and inclusive design may also contribute to reducing barriers when accessing digital content online,[73] for instance automated content progression or structured content feeds, although appropriate safeguards such as user control, transparency and the ability to pause or adjust the features should be ensured. The definition does not sufficiently distinguish between accessibility-related functionalities intended to facilitate usability, navigation or user engagement by persons with disabilities, from engagement mechanisms contributing to addictive or compulsive usage patterns.

46. Finally, the definition of "cyberbullying" as "*sending of messages, comments, or other types of aggressive, false, or repeated behaviour, or behaviour carried out with the intent to intimidate or humiliate, when occurring in the digital space*" (Article 4 (j)) appears broad especially as it includes references to "aggressive", "false" or "repeated" behaviour. At the outset, it is important to underline that there is no universally agreed legal definition of cyberbullying in international or regional human rights instruments. In its 2026 Action Plan against Cyberbullying as part of its broader strategy to improve

69 See Article 17 of the *ICCPR*; Article 8 of the *ECHR*, and *UN Human Rights Committee, General Comment No. 16* (Right to Privacy), para. 3.

70 See European Commission, *Guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 (4) of Regulation (EU) 2022/2065*, para. 49.

71 See the *Council of Europe Convention 108+*, Articles 5-7; See also Articles 5 and 25 of the *GDPR*.

72 See European Commission, *Recommendation (EU) 2026/1035 of 29 April 2026 on the establishment of a common EU framework for age verification technologies*.

73 See United Nations *Convention on the Rights of Persons with Disabilities*, Articles 9 (Accessibility) and 21 (Access to information), which require States Parties to ensure that persons with disabilities have equal access to information and communications technologies, including through accessible digital design. See also UN Committee on the Rights of Persons with Disabilities, *General Comment No. 2*; *European Accessibility Act* (Directive (EU) 2019/882).

the protection of minors online, the European Commission defined "Cyberbullying" as referring to "*behaviour carried out through digital technologies, with the primary intention or effect of repeatedly or continuously humiliating, socially excluding, abusing, harassing or harming in particular children or young people*", underlying that repetition is seen as a key feature of bullying and cyberbullying.[74] Where definitional elements are used in domestic legislation or soft-law instruments, cyberbullying is generally understood as referring to aggressive or hostile behaviour carried out through digital means, often involving an intent to cause harm and occurring in a context of real or perceived power imbalance, the impact of which may be amplified by factors such as anonymity, repeated conduct, and the continuous, permanent and potentially wide dissemination of content.[75]

47. First, the term "aggressive" may be considered inherently subjective and open to varying interpretation, potentially affecting legal certainty and the consistent application of the definition. In addition, the definition in the Bill may be understood as implying that the mere transmission of "false" content in a digital environment could fall within the scope of "cyberbullying". It is important to underline that not all false or inaccurate information is harmful and requires legal regulation, and state intervention should could be warranted to prevent the dissemination of disinformation e.g., false information disseminated with the intent to cause harm.[76] The wording of Article 4 (j) may therefore risk encompassing lawful forms of expression, including disputed factual claims, repeated criticism, satire, public debate or persistent but legitimate communication. Furthermore, insofar as the "*intent to intimidate or humiliate*" is not necessarily required and is formulated as an alternative definitional element, this may further broaden the scope of the provision and increase the risk of overreach. **Article 4 (j) of the Bill should be revised to reflect a clearer and more circumscribed definition of "cyberbullying", requiring a behaviour along with the primary intention or effect to repeatedly or continuously humiliate, socially exclude, abuse, harass or harm in particular children or young people**.

5. DIGITAL AGE OF CONSENT

48. Article 5 of the Bill introduces a "minimum digital age" of 16 for independent access to online services covered by the Bill, and requires children's informed acceptance and express and verified parental consent for younger users aged 13-16 (Article 5 (1)-(2)). Article 5 (3) provides that children under the age of 13 may not access the digital services covered by the Bill.

49. The EU applicable framework leaves the determination of the digital age of consent largely to EU Member States, within the framework of Article 8 of the GDPR, which sets a general threshold of 16 years, while allowing national legislation to establish a lower age between 13 and 16.[77] At the same time, EU-level policy developments and political

74 See European Commission, *Action plan against cyberbullying*, COM(2026) 71 final, 10 February 2026.
75 See European Commission's Joint Research Centre, *2025 Report on Cyberbullying: Insights from science, policy and legislation*, Section 5.2.1.
76 See Report on countering disinformation for the promotion and protection of human rights and fundamental freedoms, United Nations, Secretary General, A/77/287, 12 August 2022, para. 42. See also, as a comparison, Action Plan against Disinformation, Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, 2018.
77 See Article 8 of the *GDPR*: conditions applicable to child's consent in relation to information society services. The flexibility offered by the GDPR has resulted in divergent national approaches, including higher thresholds such as 16 in Germany, intermediate models such as France's "digital maturity" age of 15, and lower thresholds such as 13 in several EU Member States, including Portugal, Belgium

initiatives appear to increasingly converge towards strengthening and harmonizing the protection of minors online and a number of regional or domestic initiatives have called for the introduction of common minimum digital age for access to certain digital services, such as social media, and provide further guidance as to age assurance measures, among others.[78]

50. At the same time, as noted above, any restrictions to children's freedom of expression and access to information in the digital environment are only acceptable if they meet the requirements of legality, legitimacy, necessity and proportionality, and non-discrimination set out in international and regionals standards.[79] In addition, when designing measures aimed at protecting children in the digital environment, the State should be guided by the principles of the best interests of the child, children's evolving capacities, non-discrimination, right to development and the child's right to be heard.[80]

5.1. Minimum Digital Age

51. Article 3 of the Bill raises the national age for children's consent to data processing from 13 to 16 pursuant to Article 8 of the GDPR, which is also reflected in Article 5 (1). Article 5 (2) allows children aged 13 or older to access digital services covered by the Bill subject to informed acceptance and verified parental consent, while Article 5 (3) provides that children under the age of 13 may not access covered services.

52. The raising of the age of a children's consent to the processing of their personal data in relation to information society services from 13 to 16 is in line with Article 8 of the GDPR, which allows EU Member States to choose an age between 13 and 16 for such consent. But any such age-based regulatory model must also be assessed against established international children's rights standards, which require that children's rights be protected in a manner that is both enabling and proportionate, rather than purely restrictive. Article 12 of the CRC guarantees the right of children capable of forming their own views to express those views freely on all matters affecting them, while Article 13 of the CRC guarantees children's right to freedom of expression, including the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, through any media of the child's choice.[81] This right is complemented by Article 17 of the CRC, which obliges States Parties to ensure children's access to information and material from a diversity of national and international sources, especially those aimed at the promotion of his or her social, spiritual and moral well-being and

and the Netherlands, alongside ongoing legislative initiatives such as Spain's proposed increase to 16 years with mandatory parental controls and age verification systems.

78 See e.g., European Parliament, *Briefing - Protecting children online Selected EU, national and regional laws and initiatives* (2025); European Parliament, Resolution on the protection of minors online adopted on 26 November 2025 (2025/2060(INI), para. 28, which calls for "*the establishment of a harmonised European digital age limit of 16 as the default threshold under which access to online social media platforms should not be allowed unless parents or guardians have authorised their children otherwise; calls for the same age limit to apply to video-sharing platforms and AI companions that present risks to minors; calls, furthermore, for a harmonised European digital age limit of 13, under which no minor can access social media platforms*." See also the *Jutland Declaration on Better Protection of Children from Harmful Content Online* (2025), signed by 25 EU Member States, including Portugal, calling for strengthened age-assurance and age-verification measures and enhanced co-operation to ensure a safer digital environment for children; and the *G7 Common Set of Principles defining a safer and more secure digital space for minors*, adopted in May 2026. See also European Commission, 2025 *Guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 (4) of Regulation (EU) 2022/2065 (DSA),* which provide further guidance to establish a framework of due diligence obligations for platforms accessible to minors, including risk assessment, design safeguards, and age assurance measures aimed at ensuring a high level of safety, privacy and protection online.

79 See *Joint Declaration on the Right to Freedom of Expression and Access to Information of Children in the Digital Age*, International Mandate-Holders on Freedom of Expression, 01 June 2026, para. 1 (d).

80 See e.g., UN Committee on the Rights of the Child, *General Comment No. 25 on children's rights in relation to the digital environment*, paras. 8-21; and CoE, Committee of Ministers, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment (4 July 2018), *Recommendation CM/Rec(2018)7*, paras. 10–17 and Chapter II (Fundamental Principles).

81 See Article 13 of the *CRC*, read together with Article 19 of the *ICCPR*.

physical and mental health. These obligations apply fully in digital environments, as confirmed by the UN Committee on the Rights of the Child.[82]

53. International standards do not exclude age-based protection measures, but they require that such measures be based on an assessment of the specific risks sought to be addressed and proportionate to such risks, take into consideration the best interests and evolving capacities of the child, and ensure that any resulting restrictions on children's rights remain necessary, proportionate and do not unduly restrict the exercise of other rights.[83]

54. States should protect children against harmful or illegal content, including gender-stereotyped, discriminatory, racist, violent, pornographic and exploitative information, disinformation and information encouraging children to engage in unlawful or harmful activities, which may come from multiple sources; children should also be protected against exposure to the promotion of unhealthy or illegal products.[84] At the same time, any protective measures should be balanced with children's rights to information and freedom of expression and their other rights, while protecting them in accordance with their evolving capacities. Regulations relating to the digital environment should be compatible and keep pace with regulations in the offline environment, while aiming to formulate them in a technology-neutral manner, leaving room for the emergence of new technologies.[85]

55. From a proportionality standpoint, the wide scope of the access restrictions and minimum age for accessing digital services gives rise to concerns. Restrictions on access to information must be strictly limited to what is necessary to achieve a legitimate aim, must be appropriate to achieve their protective function; and must represent the least intrusive means available amongst those which might achieve their protective function.[86] In this respect, Article 5 could be revised to introduce a more differentiated, risk-based and proportionate regulatory approach to children's access to digital services. This would ensure that restrictions are not applied in a uniform manner across all platforms, services and applications, but are instead tailored to the specific characteristics, functionalities, and specific risks posed by them.

56. Conversely, Article 5 (3) provides a minimum access age of 13 for all platforms and services covered by the Bill, safe for the digital services excluded from the scope of the Bill as per Article 2 (3) (see para. 40 *supra*). Even if they would still be able to use inter-personal communication services, and other platforms and tools of an informational or educational nature or disseminating content of clear public interest, this may not necessarily reflect the wide range of children's legitimate use of the digital environment to exercise their rights, including but not limited to lawful access to a wide diversity of information and viewpoints, participation in public discourse, right to leisure and play, and ability to engage in social, educational and cultural life online, among others. In addition, it is noted that access to key resources, such as helplines or other preventive or

82 See the *UN Committee on the Rights of the Child, General Comment No. 25 (2021)* on children's rights in relation to the digital environment, paras. 24-26.

83 See UN Committee on the Rights of the Child, *General Comment No. 25 on children's rights in relation to the digital environment*, paras. 19-21, 54 and 97; UN Committee on the Rights of the Child, *General Comment No. 20 (2016) on the rights of adolescents*, para. 9; and CoE, Committee of Ministers, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment (4 July 2018), *Recommendation CM/Rec(2018)7*, paras. 48 and 74.

84 See UN Committee on the Rights of the Child, *General Comment No. 25 on children's rights in relation to the digital environment*, paras. 12-16, 18, 82, 95-97; and CoE, Committee of Ministers, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment (4 July 2018), *Recommendation CM/Rec(2018)7*, Sections 1, 2.1, 2.2 and 3.6.

85 See UN Committee on the Rights of the Child, *General Comment No. 25 on children's rights in relation to the digital environment*, para. 97; and CoE, Committee of Ministers, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment (4 July 2018), *Recommendation CM/Rec(2018)7*, para. 74.

86 See e.g., *UN Human Rights Committee, General Comment No. 34* "on Article 19 Freedoms of Opinion and Expression of the ICCPR", CCPR/C/GC/34, 12 September 2011, para. 34; and ECtHR, *Handyside v. United Kingdom*, no. 5493/72.

counselling services to children, should in any case be exempt from any requirement for a child user to obtain parental consent in order to access such services.[87] **It is recommended to revise Article 5 (3) to ensure that any restriction on access for children under 13 is narrowly tailored to specific and demonstrable risks stemming from content exposure as well as systemic and design-related features of specific categories of digital platforms and services, including those that may contribute to excessive engagement, addiction or dependency, also considering the distinct and potentially heightened risks posed for children by generative artificial intelligence systems and similar technologies, ensuring that aged-based access restrictions are differentiated by category of digital platforms and services and corresponding risks.,**

57. With respect to access by children aged 13 to 16, it is noted that Articles 3 and 5 of the Bill are not fully consistent in that Article 5 refers to the importance of also ensuring the child's informed acceptance in addition to the express and verified consent of the holders of parental responsibility for the child. Article 5 tends to better reflect the child's agency and evolving capacities, and is more consistent with Articles 12 and 5 of the CRC than a framework based solely on parental consent.

5.2. Parental Consent and Control Mechanisms

58. Article 6 pursues a legitimate child-protection aim by requiring verified parental consent and by enabling holders of parental responsibility to manage children's use of digital services through a dashboard. The tools listed in Article 6 (3), including time limits, privacy settings, usage-time controls and regular usage reports, may support a safer digital environment for children and are not problematic as such.

59. At the same time, parental consent and control mechanisms should be developed and deployed taking into account the principle that children are autonomous rights-holders with evolving capacities and gradual autonomy.[88] Any system of parental consent or control should not infringe children's right to privacy or undermine children's right to freedom of expression and to access a variety of information, in accordance with their age and maturity.[89] **It should also be emphasized that there are also circumstances where parental consent should not be required, such as to access preventive or counselling services to children, which should be exempt from any requirement for a child user to obtain parental consent in order to access such services and this should be reflected in the Bill**.[90]

60. Article 6 (3) (b) refers to the possibility of monitoring "*contacts and interactions flagged as risky for the child*". This wording is narrower than general parental access to private

87 See UN Committee on the Rights of the Child, *General Comment No. 25 on children's rights in relation to the digital environment*, para. 78.

88 See the UN Committee on the Rights of the Child, *General Comment No. 20* on the implementation of the rights of the child during adolescence (evolving capacities and gradual autonomy).

89 See e.g., CoE, Committee of Ministers, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment (4 July 2018), *Recommendation CM/Rec(2018)7*, para. 54. The CoE's Handbook for policy makers on the rights of the child in the digital environment indicates, with regard to parental controls tools, recommends that member states, while designing their own legislation, if such controls are developed and deployed, should pay attention to the questions of taking into account children's evolving capacities without reinforcing discriminatory attitudes, of whether parental control tools infringe children's right to privacy and data protection or deny children the right to information, take into account their age and maturity. See CoE *Handbook for policy makers on the rights of the child in the digital environment to support the implementation of Recommendation CM/Rec(2018)7 of the Committee of Ministers of the Council of Europe on Guidelines to respect, protect and fulfil the rights of the child in the digital environment*, Council of Europe, S. Livingstone, E. Lievens, J. Carr, 2020, p. 58.

90 See UN Committee on the Rights of the Child, *General Comment No. 25 on children's rights in relation to the digital environment*, para. 78.

communications and should not be interpreted as allowing unrestricted reading or surveillance of a child's online exchanges. A system of monitoring or surveillance of children's online activities risks interfering with the child's right to privacy, which protects children against arbitrary or unlawful interference with their privacy, family, and correspondence, and should not be conducted routinely, indiscriminately or without the child's knowledge.[91] Broad or continuous surveillance would also undermine the proportionality requirements, which require that any interference with privacy be necessary and the least intrusive means available.[92] To avoid such an interpretation, **Article 6 could specify that any monitoring must be limited to safety-related alerts, proportionate to the child's age and maturity, made with the child's knowledge, and subject to safeguards where parental access could expose the child to harm, including to ensure that no parental consent or control measures apply when children are accessing preventive or counselling services.** Such clarification would preserve the legitimate role of the holders of parental responsibility while better reflecting children's evolving capacities and their rights to privacy, freedom of expression and access to information, particularly for older children seeking confidential support on sensitive issues.

5.3. Age Verification with Privacy Considerations

61. Article 5 (4) permits age verification through the Digital Mobile Key system or another comparable mechanism, using simple or enhanced authentication in accordance with technical guidelines. Under Article 7, service providers offering services accessible to children are required to implement a mandatory age verification mechanism compatible with the Digital Mobile Key system or another equivalent approved system, in accordance with technical guidelines, while explicitly prohibiting the use of self-declaration or user self-identification for age verification. Article 8 further provides that the age verification system must ensure a high level of reliability and resistance to fraud, minimize the collection of personal data, support compatibility with national and EU digital identity frameworks (including anonymized attributes where available), and incorporate privacy-preserving technologies such as zero-knowledge proofs. It also establishes detailed technical governance requirements for the National Technical Reference Framework, including interoperability with EU digital identity systems, rules on certification, auditing and anonymization, and provisions relating to data security and the child's right to be forgotten. Lastly, under Article 20, the Digital Mobile Key system is designated as the national age-verification mechanism and is required to ensure interoperability with the European digital identity card or other equivalent European digital identity systems.

62. Articles 7 and 8, read together with Article 5, and the broad and vague scope of services covered under Article 2 (see Sub-Section III.3 *supra*), establish a generalized obligation for service providers to implement age verification for access to services covered by the Bill, while prohibiting self-declaration mechanisms and requiring identity-linked verification methods. While this reflects a clear policy objective of strengthening child protection online, it also raises questions regarding the systemic nature of the obligation, particularly when assessed against established human rights standards. Indeed, the broad age-verification requirements applying to a wide range of digital services have implications that extend well beyond the category of children whom the legislation seeks

91 Article 16 of the CRC; and UN Committee on the Rights of the Child, *General Comment No. 25 on children's rights in relation to the digital environment*, para. 75.

92 See Article 17 of the *ICCPR*; See also UN Human Rights Committee, *General Comment No. 16* on the right to privacy.

to protect. Even if the applicable framework seeks to incorporate privacy-preserving tools and to minimize personal data collection, such measures may require all or most users to be subject to some age-verification mechanism that may still risk to disclose, generate or otherwise involve the processing of age-related credentials or personal data as a condition for accessing all the digital services covered by the Bill. Consequently, the scope of individuals affected by the Bill may be considerably wider than the group intended to benefit from its protection, thereby raising important questions regarding data minimization, necessity, proportionality and the potential chilling effect associated with generalized identity or age verification in the digital environment for all users.

63. While the protection of children from harmful content and digital risks constitutes a legitimate and important public interest objective, the chosen regulatory model, namely, universal or near-universal age verification for access to covered services, may not sufficiently reflect the requirement that is strictly necessary and based on a risk-sensitive assessment. The EDPB has emphasized that age assurance must be implemented in a risk-based and proportionate manner, taking into account the nature of the service and the actual risks to children, and that less intrusive alternatives must be prioritized where available; it has further clarified that systematic age verification across all users and all services, including low-risk or non-risk environments, may fail the necessity and proportionality test and may require a prior Data Protection Impact Assessment under Article 35 of the GDPR.[93] The EDPB also stresses that age assurance systems must not enable unnecessary identification, tracking, profiling, or inference of user behaviour beyond what is strictly required for the intended purpose.[94] In addition, such broad verification obligations may generate a chilling effect on the exercise of the rights to freedom of expression and privacy, if access to digital services becomes systematically dependent on the disclosure of identity credentials or biometric data.[95] Hence, as elaborated in Sub-Section III.3 *supra*, a clearer differentiation of categories of digital services and corresponding risk profiles for the purposes of determining the applicable obligations, including potential requirement for age verification is recommended, to ensure a more proportionate regulatory framework.

64. The European Commission's Guidelines on Article 28 (4) of the DSA emphasizes that age-assurance measures should be accurate, reliable, robust, non-intrusive, and non-discriminatory.[96] The EU is also seeking to advance privacy-preserving age assurance solutions within the framework of the European Digital Identity Wallet, including selective disclosure mechanisms and attribute-based verification models.[97] These provisions of the Bill, taken together, appear to seek to reflect such efforts to develop secure, interoperable and privacy-preserving age assurance. However, further safeguards should be considered in relation to Articles 7, 8 and 20 to ensure that the contemplated measures are necessary, proportionate and non-discriminatory and do not undermine the exercise of children's rights online.

65. First, while reliance on systems such as Chave Móvel Digital or EU digital identity credentials may enhance security and reliability, an exclusive dependence on state-issued

93 See EDPB, *Statement 1/2025 on Age Assurance*, paras. 13 and 14.
94 *Ibid*, para 15 and 16.
95 See the *European Digital Rights (EDRi)*, policy papers on age verification and fundamental rights impacts of identity-based access systems.
96 See European Commission, 2025 *Guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 (4) of Regulation (EU) 2022/2065 (DSA)*, para. 4(b) and 49(e). The guidelines also recommend the use of effective age assurance methods provided that they are accurate, reliable, robust, non-intrusive, and non-discriminatory.
97 See the *European Digital Identity Framework / eIDAS 2.0 proposal and Digital Identity Wallet pilot initiatives*. Trust Services, introduced in the *2014 eIDAS Regulation ((EU) 910/2014)*, are regulated digital services, like qualified signatures, designed to ensure the security, authenticity, and integrity of electronic transactions.

digital credentials may risk indirect exclusion of certain groups, including undocumented children, asylum-seekers, refugees, or individuals lacking access to digital identity infrastructure.[98] **In this respect, the framework should explicitly require that alternative, non-discriminatory and accessible age-verification methods be made available, ensuring that access to essential digital services is not conditioned on possession of a specific form of state-issued digital identity.**

66. Second, the requirement of a "*high degree of reliability and resistance to fraud*" should be carefully defined to avoid disproportionate reliance on biometric-based age estimation technologies. Under the GDPR, biometric data constitute special category data subject to heightened safeguards, including strict necessity requirements.[99] The National Technical Reference Framework should therefore clarify that reliability should be achieved primarily through privacy-preserving cryptographic and federated identity solutions, rather than through intrusive biometric inference methods, except where strictly necessary and fully compliant with data protection law.

67. In addition, age verification systems should be designed in a way to collect as little data as possible and to enable only selective disclosure of information, ensuring that only the minimum necessary attribute, such as a binary confirmation of age threshold compliance, is communicated to the service provider, without disclosure of additional identity-related data.[100]

68. Further, it is relevant to note that international standards caution against regulatory approaches that treat children as a homogeneous group without sufficient consideration of their evolving capacities,[101] and their diversity, specific needs and personal circumstances.[102] In this context, the absence of dedicated child rights and data protection impact assessment, in the Explanatory Memorandum or elsewhere, focused on age verification measures, may be viewed as a gap in the regulatory framework.[103] Furthermore, discussions on the Bill and design of age verification mechanisms should be subject to meaningful consultations, including with child-rights organizations and parents' organizations, and as appropriate and relevant, children – using age-appropriate formats reflecting their evolving capacities.[104]

69. **It is recommended to reconsider the systematic application of age verification for all services covered by the Bill and instead provide a clearer differentiation of categories of digital services and corresponding types and levels of risks arising from the nature, design, functionality, scale, and user base of the service concerned** – also taking into account the rapidly evolving nature of risks linked to digital environment – **for the purposes of determining whether age verification is a**

98 See the *Council of Europe Convention 108+*; UNHCR *guidance* on digital identity and inclusion of displaced persons.
99 See *GDPR*, Article 9.
100 See *GDPR*, Article 5 (1) (c) (data minimization) and Article 5 (1) (e) (storage limitation). See also EDPD, Statement 1/2025 on Age Assurance, which provides that "*Age assurance should be designed, implemented and evaluated taking into account the most privacy-preserving available methods and technologies in order to meet the requirements of the GDPR and effectively protect the rights of data subjects.*" The EDPB also recommends that "*based on the state of the art in age assurance at the time this document was prepared, due consideration is given to technologies and architectures favouring user-held data and secure local processing (device-based), allowing properties such as unlinkability (from different parties' point of view and even in the case of collusions or data breaches) and selective disclosure of personal data under the control of the data subject*"; see EDPD, Statement 1/2025 on Age Assurance, Section 2.8, para. 34.
101 See UN Committee on the Rights of the Child, *General Comment No. 25*, para. 52.
102 See UN Committee on the Rights of the Child, *General Comment No. 25*, para. 25.
103 See e.g., EDPB Statement 1/2025 on Age Assurance, where the EDPB cautioned that age assurance mechanisms may pose significant risks to the rights and freedoms of users, including children, and has emphasized the need for a risk-based approach supported by a data protection impact assessment and the use of the least intrusive means available.
104 See Article 12 of the *CRC*; and UN Committee on the Rights of the Child, *General Comment No. 12 (2009) on the right of the child to be heard*, para. 122.

necessary and proportionate measure. Any age verification tool should be accurate, reliable, robust, non-intrusive, and non-discriminatory.

70. Finally, when age verification systems are implemented, it is essential that **any user has access to an effective internal complaint-handling system that enables them to lodge complaints, electronically and free of charge, against an assessment by the provider of the user's age.**[105] **The Bill should be supplemented in this respect.**

6. PLATFORM OBLIGATIONS AND CONTENT GOVERNANCE

71. Article 9 requires online service providers that offer age-restricted or potentially harmful content, namely content that may "*harm the physical or mental development of children, including violent, sexual, or addictive content*", to implement appropriate safeguards to prevent children's access to such material. This is a legitimate objective supported by EU audiovisual and platform regulation, which contains specific rules protecting minors from harmful audiovisual media and extends obligations to video-sharing platforms.[106]

72. However, Article 9 (2) raises concerns from a freedom of expression perspective. In cases of non-compliance, the National Communications Authority is empowered to impose far-reaching enforcement measures, including de-indexing the service from search engines, suspending access to the service within the national territory, and adopting urgent precautionary measures where there is a risk to children. At the same time, **it is not clear what such "urgent precautionary measures" consist of and they should be strictly listed in the Bill.** In addition, as mentioned above, the terminology "*harm the physical or mental development of children"* is broad and imprecise.[107] In that respect, international standards define specific content harmful for children precisely and outline detailed measures.[108]

105 See European Commission, *Action plan against cyberbullying*, COM(2026) 71 final, 10 February 2026, para. 77.

106 See e.g., *Directive 2010/13/EU* (Audiovisual Media Services Directive), as amended by Directive (EU) 2018/1808, which states that *"[t]he availability of harmful content in audiovisual media services is a concern for legislators, the media industry and parents. There will also be new challenges, especially in connection with new platforms and new products. Rules protecting the physical, mental and moral development of minors as well as human dignity in all audiovisual media services, including audiovisual commercial communications, are therefore necessary."*

107 The ECtHR has consistently held that restrictions on access to the internet must be subject to a particularly strict legal framework, and that wholesale blocking or suspension of access to an online service risks violating Article 10 ECHR where it is overbroad and not limited to targeted illegal or harmful content, arbitrary, or insufficiently subject to judicial control; see e.g., ECtHR, *Ahmet Yıldırım v. Turkey*, no. 3111/10, 18 December 2012, which concerned a court decision to block access to Google Sites, which hosted an Internet site whose owner was facing criminal proceedings for insulting the memory of Atatürk; the Court emphasized that the measure extended beyond the allegedly unlawful content, thereby producing disproportionate collateral effects. See also e.g., ECtHR, *Cengiz and Others v Turkey*, nos. 48226/10 and 14027/11, where the Court found in particular that the applicants, all academics in different universities, had been prevented from accessing YouTube for a lengthy period of time and that, as active users, and having regard to the circumstances of the case, they could legitimately claim that the blocking order in question had affected their right to receive and impart information and ideas. The Court also observed that YouTube was a single platform which enabled information of specific interest, particularly on political and social matters, to be broadcast and citizen journalism to emerge. The Court further stated that "*a legal framework is required, ensuring both tight control over the scope of bans and effective judicial review to prevent any abuse of power*".

108 See e.g., UN General Assembly, *Resolution 78/213 Promotion and protection of human rights in the context of digital technologies*, 22 December 2023, para. 5, the importance of combating all forms of violence in the context of digital technologies, including sexual exploitation and abuse, harassment, stalking, bullying, non-consensual sharing of personal sexually explicit content, threats and acts of sexual and gender-based violence, death threats, arbitrary or unlawful surveillance and tracking, trafficking in persons, extortion, censorship, illegal access to digital accounts, mobile telephones and other electronic devices; in addition, a number of international instruments require the criminalization of the dissemination or communication of certain forms of sexually exploitative content: Articles 2 (c) and 3 (1) (c) of the *Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography"*, ratified by Portugal on 16 May 2003, require the criminalization of "*child sexual exploitation material*"; see also, Article 20 of the *Council of Europe Convention on Protection of Children Against Sexual Exploitation and Sexual Abuse* (Lanzarote Convention) requires the criminalization of intentional conduct, amounting to *"(a) producing child pornography; (b) offering or making available child pornography; (c) distributing or transmitting child pornography; (d) procuring child pornography for oneself or for another person; (e) possessing child pornography; and (f) knowingly obtaining access, through information and communication technologies, to child pornography*" (Council of Europe Convention on Protection of Children Against Sexual Exploitation and Sexual

73. **It is recommended that Article 9 be amended to include clear procedural and substantive safeguards. In particular, it should specify that suspension or de-indexing should be a measure of last resort. Decisions should be reasoned and based on an assessment of the potential impact on lawful expression and access to information, publicly available, and preceded by notice unless urgent action is strictly necessary. The Bill should also strictly list the types of "urgent precautionary measures" that may be used. Judicial authorization or rapid judicial review should be required.**

74. Article 10 requires platforms to apply secure default settings for users under 16, ensuring their accounts are automatically private, profiles cannot be searched, algorithmic recommendations are restricted to non-addictive and age-appropriate content, and social metrics (such as likes or follower counts) are hidden to better protect children online. Default safety settings are, in principle, consistent with UN CRC Committee General Comment No. 25 and with the Commission's Guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 (4) of the DSA. The European Parliament has also called for stronger safeguards, including restrictions on engagement-based recommender systems and addictive practices targeting minors.[109]

75. However, Article 10 would benefit from further precision, particularly regarding the concept of "non-addictive algorithmic recommendations" (as referenced alongside "addictive design" in Article 4 (h)). In its current wording, the provision risks interpretive uncertainty. A more precise formulation would require that recommender systems for minors **(i) are not primarily optimized for engagement time; (ii) do not amplify harmful or age-inappropriate content; (iii) include a non-profiling-based recommendation option; (iv) are transparent and explainable in age-appropriate language; and (v) are subject to independent risk assessment and audit**, and Article 10 should be supplemented in this respect to clarify what is meant by "non-addictive algorithmic recommendations".[110] Read in conjunction with the age threshold, as provided in Article 5 and the broader design prohibitions in Article 11, Article 10 may also raise questions of proportionality in light of children's autonomy and evolving capacities, as reflected in international standards.[111] While default-settings are generally recommended, they should be framed in a way that children are not completely deprived of the ability to make own informed choices in line with their evolving capacities and hence, in line with Article 12 of the CRC.

Abuse (Lanzarote Convention), CETS No. 201, Article 20). See also e.g., the UK Online Safety Act which requires risk assessments, content moderation including takedown procedures, restrictions on harmful content (pornography, suicide encouragement, violence, bullying, dangerous stunts), and limits on addictive or manipulative features (e.g., autoplay, streaks); Sec. 61 also defines 'Priority content that is harmful to children' as a series of content such as abusive content targeting one or more protected characteristics, incites hatred against certain protected characteristics, encourages serious violence against a person, is of a bullying nature, depicts real or realistic serious violence or injury against a person, an animal or a fictional creature, encourages dangerous challenges or stunts, ingesting or inhaling harmful substances.

109 See European Parliament, *Report on the protection of minors online* (2025/2060(INI)).

110 See e.g., Regulation (EU) 2022/2065 (Digital Services Act), in particular Articles 14, 28, 34-38 and recitals 71, 79-83; Regulation (EU) 2016/679 (GDPR), Articles 5, 12-14 and 22 and Recital 58; CoE, Committee of Ministers, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment (4 July 2018), *Recommendation CM/Rec(2018)7*, especially paras. 61 and 65; UN Committee on the Rights of the Child, *General Comment No. 25*, paras. 12, 18, 23, 62-63; and the principle of platform regulation harmonisation under Article 3 of *Directive 2000/31/EC*.

111 See UN Committee on the Rights of the Child, *General Comment No. 25*, paras. 17-20; and the principle of platform regulation harmonisation under Article 3 of *Directive 2000/31/EC*.

7. CONTENT MODERATION AND CYBERBULLYING

76. Article 11 prohibits autoplay, infinite scroll, gamification designed to prolong use, non-essential notifications at night, fake-image or video systems, and loot boxes or equivalent mechanisms on accounts belonging to children under 16. Article 11 (2) specifies that essential features are permitted, provided they are configured to minimize access to inappropriate content and the risks of digital addiction.

77. The European Commission's Guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 (4) of the DSA identify excessive-use features, harmful design practices and specifically recommend that provision of online services should ensure that minors are not exposed to persuasive design features that are aimed predominantly at engagement and that may lead to extensive use or overuse of the platform or problematic or compulsive behavioural habits.[112] The European Parliament has likewise called for stronger regulatory action against addictive design practices in digital services, including techniques such as infinite scrolling, autoplay functions and persistent notifications, and has advocated the development of digital services based on "ethical design" principles rather than engagement-maximization strategies.[113]

78. In addition, as noted above, in February 2026, the European Commission adopted its Action Plan against Cyberbullying as part of its broader strategy to improve the protection of minors online.[114] The Action Plan sets out co-ordinated measures to prevent and respond to cyberbullying, including improved and simplified child-friendly reporting and complaint tools, as well as victim support mechanisms for children and families, along with awareness-raising activities which are empowering, inclusive and accessible.[115] It also encourages online platforms to strengthen safeguards and improve moderation practices to reduce harmful interactions. The initiative promotes co-operation between Member States, schools, and digital services to ensure a more consistent and effective response across the EU.[116]

79. While Article 11 of the Bill sets out important safeguards, several aspects would benefit from greater precision in order to enhance legal certainty and ensure effective and consistent implementation. In particular, it may be helpful to clarify what qualifies as a "fake image" or "fake video", which are not permitted on accounts belonging to children under 16 as per Article 11 (1). In past opinions, ODIHR and the OSCE RFoM have cautioned against general prohibitions on the dissemination of "false" or "fake" information given the fact that not all false or inaccurate information reaches the threshold of harm that would require a regulatory intervention, and there is a credible risk of encompassing protected forms of expression under such a vague and broad terminology.[117] As currently worded, the provision could potentially be interpreted broadly enough to encompass harmless and widely used functionalities, such as photo filters, background blurring, or basic image-editing tools. The provision could specify that, for instance, the ban targets Generative AI systems capable of creating synthetic or

112 See European Commission, 2025 *Guidelines on the Protection of Minors Online pursuant to Article 28 (4) DSA*, para. 61 (b).
113 See e.g., European Parliament, Resolution on Addictive Design of Online Services and Consumer Protection in the EU Single Market (2023/2043(INI)), paras. 7-8 and 11.
114 See European Commission, *Action plan against cyberbullying*, COM(2026) 71 final, 10 February 2026.
115 See European Commission, *Action plan against cyberbullying*, COM(2026) 71 final, 10 February 2026, Sections 3.1-3.2.
116 See European Commission, *Action plan against cyberbullying*, COM(2026) 71 final, 10 February 2026, Section 4 on multi-stakeholders engagement.
117 See e.g., ODIHR-OSCE RFoM, *Joint Opinion on the Draft Law of Uzbekistan on the Protection of Users' Rights on Online Platforms and Websites*, 5 December 2025, Section 4.1.

deeply manipulated media (like deepfakes) that are likely to deceive or cause harm, rather than banning all basic image-modification tools. Similarly, the definition of "essential features", which are excluded from the scope of the prohibition, should be clarified. Without further guidance, platforms may argue that features designed to increase engagement are essential to the provision of their services. At the same time, **it may be unclear whether genuinely necessary functions, such as messages from parents or account security notifications, would fall under the scope of such "essential features".**

80. In light of the foregoing, **it is recommended that Article 11 be retained as an important child-protection measure, while clarifying the scope of the prohibitions relating to "fake images or videos" and "essential features".**

81. Article 12 of the Bill requires platforms to detect and limit suspicious contacts, automatically block violent or sexual material, block aggressive or false content that may constitute cyberbullying, and provide fast reporting channels. Article 12 (3) extends these duties, with adaptations, to interpersonal electronic communications services used by children under 16. It also mandates that reports involving children be treated urgently with a response within 24 hours (Article 12 (2)), and extends these protections to interpersonal communication services "*with the necessary adaptations*" used by children under 16. In line with the 2026 EU Action Plan against Cyberbullying, these obligations reflect a broader policy shift towards early detection, user reporting tools, and preventive safeguards within platform design to reduce exposure to cyberbullying risks.

82. The protective objective is legitimate and in line with the ECtHR caselaw and other regional soft-law documents, which have recognized positive obligations to protect children from serious online harm, including by ensuring that the applicable legal framework allows effective, early identification of the offender.[118] In addition, several reports on the protection of children in the digital environment indicate that online harm is not gender-neutral, with girls and young women experiencing disproportionately high levels of cyberbullying, sexual harassment, image-based abuse or revenge pornography (online public dissemination without consent of intimate photographs of the victim by her former intimate partner), and grooming-related targeting.[119]

83. At the same time, Article 12 of the Bill is sensitive because it may imply proactive monitoring of private communications. Specifically, Article 12 (1) (b) requires services and platforms to "*automatically block messages containing violent or sexual material, including aggressive or false content that may constitute cyberbullying*". Such requirement is vague, since as noted above, the definition of "cyberbullying" is not clear and strictly circumscribed, and "false" content is not necessarily unlawful; aggressive speech may be offensive or disturbing without crossing the threshold of unlawful expression. Automatic blocking based on such broad categories risks suppressing lawful speech, including political expression, satire, interpersonal conflict, peer support, news reporting or counter-speech. It is also uncertain whether automated AI filtering tools are

118 See e.g., ECtHR, *K.U. v Finland*, no. 2872/02, 2 December 2008, paras. 49-50, where the ECtHR found a violation of Article 8 where the domestic legal framework did not allow effective identification of a person who had posted a sexualized online advertisement concerning a child; see also the CoE, Convention on Protection of Children Against Sexual Exploitation and Sexual Abuse (Lanzarote Convention), CETS No. 201; and European Commission, *Action plan against cyberbullying*, COM(2026) 71 final, 10 February 2026, which emphasizes strengthening reporting and support mechanisms for victims of cyberbullying, including accessible complaint pathways and co-ordinated responses involving schools, platforms, and national authorities.

119 See UN *Intensification of efforts to eliminate all forms of violence against women and girls*: Technology-facilitated violence against women and girls: Report of the Secretary-General (2024). See also *Report of the Special Rapporteur* on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective (2018), A/HRC/38/47. See also ECtHR, M.Ş.D. v. Romania, 2024, para. 125, where the Court has also considered that, in the case of revenge pornography, the protection of Article 8 required a criminal-law response.

capable of reliably evaluating contextual indicators, linguistic nuance, satire, irony, or consent, and they cannot consistently distinguish between peer-to-peer adolescent interaction and malicious cyberbullying, nor separate explicit content from legitimate educational, medical, or human rights discourse, including LGBTI youth support networks.[120] **It is therefore essential that human review is available in addition to automated content review and any other relevant tools for reporting accounts or content that the provider suspects may pose a risk of harm to minors' privacy, safety or security**.[121]

84. Article 12 (1) (c) refers to the provision of fast and secure reporting channels, which is welcome in principle although it could be further specified that the **reporting mechanisms shall be simple, visible, child-friendly and easily accessible**.[122]

85. **It is recommended to revise Article 12 to ensure that obligations relating to the detection, blocking and reporting of harmful content are clearly defined, strictly limited to identifiable unlawful or high-risk content, and applied in a manner consistent with the principles of necessity and proportionality. In particular, the notions of "violent or sexual material", "aggressive content" and "suspicious contacts" should be further specified to avoid encompassing lawful forms of expression, and safeguards should be introduced to ensure that any automated content moderation is, as mentioned above, subject to human review, does not promote over-blocking, and does not unduly undermine the confidentiality of interpersonal communications. The provision should also specify that reporting mechanisms should be accessible, simple and child-friendly.**

8. SUPERVISORY AUTHORITIES AND REPORTING

86. Article 13 of the Bill designates the National Communications Authority and the National Data Protection Commission as the authorities responsible for overseeing compliance with the law within their respective areas of competence. This approach is broadly consistent with the EU regulatory model, which increasingly relies on multi-authority enforcement in the digital space.[123] In that sense, the dual structure envisaged in this provision is not inconsistent with EU law, but **the Bill would benefit from further clarification of its relationship with the EU Digital Services Act enforcement architecture in Portugal, including the role of the Portuguese Digital Services Coordinator, the European Board for Digital Services, and the European Commission in relation to very large online platforms and search engines**.

87. With respect to Article 13 (4), which provides that the authority conducting the investigation (either the National Communications Authority and the National Data Protection Commission) holds the power to impose administrative fines, it should be noted that the GDPR confers primary responsibility for the enforcement of data protection rules, including the imposition of administrative fines for data processing infringements, on the competent data protection supervisory authority. Against this background, where enforcement actions relate to measures such as age verification failures involving potential breaches of data minimisation or other GDPR principles,

120 See UNICEF, *A youth-led roadmap to realize the best interests of children in the digital environment*.
121 See European Commission, *Guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28 (4) of Regulation (EU) 2022/2065*, para. 49.
122 See European Commission, *Action plan against cyberbullying*, COM(2026) 71 final, 10 February 2026, Sections 3.1-3.2.
123 Under the DSA, Member States must designate a Digital Services Coordinator (DSC) responsible for ensuring the effective application of the Regulation at national level, including co-ordination with other competent authorities where sectoral competences overlap; see *Regulation (EU) No. 2022/2065* (DSA), Articles 49-51.

consistency with the GDPR enforcement framework should be ensured to avoid any overlap or conflict of competences. It is therefore advisable **to clarify the allocation of enforcement powers within the Bill, for example by specifying that infringements primarily concerning data protection and privacy obligations (such as items a, b, e and f) fall within the competence of the National Data Protection Commission, whereas infringements relating to structural content distribution or platform governance obligations (such as items c, g and i) fall within the competence of National Communications Authority.**

88. Article 14 of the Bill introduces reporting and transparency obligations requiring service providers and platforms covered by the Bill, upon request by the National Communications Authority, to submit within 60 days a report on compliance with the law, risks to children, preventive measures implemented, and results achieved. It also provides that such reports shall be made public, unless confidentiality grounds are duly justified and accepted by the National Communications Authority.

89. This is welcomed as it generally aligns with the DSA requirement for transparency and accountability obligations for online intermediaries, including systematic reporting on content moderation practices, systemic risks, and mitigation measures.[124] **Article 14 could be supplemented to ensure that transparency reporting also requires (at least aggregated) disclosure of content removals, content blocking and restrictions, account suspensions or age-gating, reports involving children, the extent of automated decision-making, appeals and reversal rates, and the safeguards applied to protect lawful expression**.

10. OTHER PROVISIONS

90. The Bill introduces public information campaigns (Article 17), a "Safe Platform for Children" certification scheme (Article 18), and a requirement for an evaluation of the law one year after its entry into force (Article 19). These are positive measures, which reflect the understanding that child online safety cannot be ensured solely through regulatory prohibitions and enforcement mechanisms, but also requires awareness-raising, digital literacy and education, parental support, professional training, and continuous assessment of regulatory effectiveness over time.[125] In particular, public campaigns and certification schemes may help guide users' choices and incentivize higher safety standards among service providers, while periodic evaluation supports evidence-based policymaking and allows for adjustments based on implementation outcomes and technological developments.[126]

91. More generally, it is important to assess the Bill not only in light of the restrictions and obligations it imposes, but also against the positive obligations that international human rights standards place upon the State, including in terms of promoting awareness-raising and digital literacy.[127] In the present Bill, the main expression of these positive obligations appears in Article 17 of the Bill, which provides for regular information, prevention, data

124 See *Regulation (EU) No. 2022/2065*, Articles 64-68. In particular, the DSA requires providers, especially very large online platforms and search engines, to publish regular transparency reports and disclose information on moderation actions and risk management systems (Articles 15, 24, 42 and 43).

125 See UN Committee on the Rights of the Child, *General Comment No. 25 on children's rights in relation to the digital environment*, paras. 18-22. See also See CoE, Committee of Ministers, Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment (4 July 2018), *Recommendation CM/Rec(2018)7*.

126 See UNESCO, *Media and Information Literacy: Policy and Strategy Guidelines*.

127 See e.g., UN Committee on the Rights of the Child, *General Comment No. 25 on children's rights in relation to the digital environment*, paras. 32-33.

protection, digital literacy and child safety campaigns to be carried out by the National Communications Authority and the National Data Protection Commission.

11. PROCESS OF DEVELOPING AND ADOPTING THE BILL

92. The importance of open, transparent and inclusive lawmaking process throughout the development and adoption of the Bill should be highlighted. In paragraph 5.8 of the 1990 OSCE Copenhagen Document, OSCE participating States have committed to ensure that legislation will be adopted at the end of a public procedure.[128] Moreover, key commitments specify that *"[l]egislation will be formulated and adopted as the result of an open process reflecting the will of the people, either directly or through their elected representatives*".[129] The ODIHR Guidelines on Democratic Lawmaking for Better Laws (2024) underline the importance of evidence-based, open, transparent, participatory and inclusive lawmaking process, offering meaningful opportunities to all interested stakeholders to provide input at all its stages.[130] Respect for the views of children when developing legislation that concern them, such as the Bill under review, is essential in accordance with their age and maturity, and states are encouraged to utilize the digital environment to consult with children in formats appropriate to their age and capacities and ensure that their views are considered seriously throughout the development and adoption of the Bill.[131]

93. Effective consultations in the drafting of laws, as outlined in the relevant OSCE commitments, need to be inclusive, involving both the general public and stakeholders with a particular interest in the subject matter of the draft legislation, in this case children of different age groups in accordance with their age and maturity, child-rights organizations, parents and care-givers, and others. Sufficient time should also be provided to ensure that the consultation process is meaningful, allowing adequate time to stakeholders to prepare and submit recommendations on draft legislation throughout the legislative process.[132]

94. In light of the above, **the public authorities are encouraged to ensure that a proper impact assessment is conducted, and the legislative process leading to the adoption of the Bill is subjected to inclusive, extensive, effective and meaningful consultations with relevant stakeholders including child-rights organizations, parents' organizations, and children, in formats appropriate to their age and capacities, which should enable equal opportunities for women and men, girls and boys, to participate**. According to the principles stated above, such consultations should take place in a timely manner, at all stages of the lawmaking process, including before parliament.

[END OF TEXT]

128 See *1990 OSCE Copenhagen Document*, para. 5.8.
129 See *1991 OSCE Moscow Document*, para. 18.1.
130 See *ODIHR Guidelines on Democratic Lawmaking for Better Laws* (January 2024), in particular Principles 5, 6, 7 and 12. See also Venice Commission, *Updated Rule of Law Checklist*, CDL-AD(2025)002-e, 16 December 2025 Part II.A.6.
131 See the UN Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*, para. 18. See also See *ODIHR Guidelines on Democratic Lawmaking for Better Laws* (January 2024), paras. 178 and 210.
132 See *ODIHR Guidelines on Democratic Lawmaking for Better Laws* (January 2024), paras. 169-170.