ISSN 2281-5147

Opinio Juris in Comparatione

Studies in Comparative and National Law

Vol. 2, n. 2/2025

TABLE OF CONTENTS

Section 1

Section 2

Special Issue on Special issue on "Towards *a multilevel and interdisciplinary assessment for a safer use of digital services and AI-based products", edited by D. Amram - C. Novara - M. Ratti*

ISSN 2281-5147

CHILDREN'S RIGHTS AND THE CINEMATIC EXPERIENCE IN THE DIGITAL AGE: ADDRESSING REGULATORY CHALLENGES *

Jacopo Fortuna and Nicoletta Patti **

Abstract

Digitization has profoundly reshaped minors' cinematic experience, transforming both their modes of participation in artistic and cultural products and their pathways of content access. Once a privileged physical space for socialization and collective sharing, cinema is now embedded in a digital ecosystem dominated by streaming platforms and social media—an environment where consumption is individual, transmedial, and shaped by algorithmic logics. This shift entails the risk of homogenized cultural choices and increasingly passive viewing behaviours among young audiences. The article explores the evolution of children's cinematic experience within the contemporary regulatory and digital landscape, analyzing the contractual terms, policies, and operational logics of major Video-on-Demand platforms.

Particular attention is devoted to algorithmic recommendation systems, behavioural profiling mechanisms, and forms of targeted advertising which – while offering personalized viewing experiences – tend to erode cultural diversity and compromise both privacy protection and the critical development of minors.

After examining the international and European legal framework on children's rights in relation to the cinematic experience, the article focuses on the role of the Digital Services Act (DSA) in regulating the relationship between cinema and minors. It highlights the persistent protection gaps affecting Video-on-Demand services, which currently fall outside the DSA's material scope. The argument advanced is that an integrated approach is required—one grounded in the principles of *privacy by design*, *age-appropriate transparency*, and the prohibition of *dark patterns*—to ensure a genuinely child-friendly audiovisual ecosystem.

Finally, the article calls for a comprehensive rethinking of public policies and digital-governance models aimed not only at safeguarding minors but also at actively

ISSN 2281-5147

promoting their rights, recognizing them as autonomous individuals and active participants in cultural and artistic life in the digital age.

Table of Contents

ISSN 2281-5147

Keywords

Child protection – Video-on-Demand (VoD) platforms – Parental control – DSA – Algorithmic recommendation systems

1. Introduction: Children and Cinema in the Digital Age.

Children and adolescents constitute a significant portion of the audience for the products of the film industry[1]. However, this quantitative centrality does not automatically translate into a qualitatively adequate approach to their rights, interests[2] and developmental needs. On the contrary, precisely because of their inherent

---

* While the authors contributed equally to the conception of this paper, and jointly wrote the introduction (par. 1), paragraphs 6 and 7.1 and the conclusions (par. 8), Jacopo Fortuna authored paragraphs 2, 5, whereas Nicoletta Patti authored paragraphs 3, 4, 7.
This contribution has been developed within the framework of the PRIN PNRR Self-assessment Network Impact Program (SNIP) – code P2022AK2HK and the REBOOT: Reviving, Boosting, Optimizing, and Transforming European Film Competitiveness project that has received funding from the Horizon Europe program of the European Union under the Grant Agreement No 101094769.
** *Research Fellows at the Scuola Superiore Sant'Anna, Pisa* (jacopo.fortuna@santannapisa.it; nicoletta.patti@santannapisa.it). Double blind peer reviewed contribution.

[1] https://www.obs.coe.int/en/web/observatoire/industry/children.

[2] On the topic of vulnerability and vulnerable users, including children, see D. Amram, *Standards to Face Children and Patients Digital Vulnerabilities*, in *The New Shapes of Digital Vulnerability in European Private Law*, ed. by C. Crea and A. De Franceschi, 2024, p. 439 ff.; Id., *La transizione digitale delle vulnerabilità e il sistema delle responsabilità*, in *Rivista italiana di medicina legale*, 2023, p. 1 ff.; Id., *Children (in the Digital Environment)*, in *Elgar Encyclopedia of Law and Data Science*, ed. by G. Comandé, 2022, p. 64 ff.; A. Pera, S. Rigazio, *Let the Children Play. Smart Toys and Child Vulnerability*, in C. Crea, A. De Franceschi (ed. by), *The New Shapes of Digital Vulnerability in European Private Law*, Elgar, 2024, pp. 413-437; N. Patti, V. Punzo, R. Romano, *Child vulnerabilities in the digital environment: comparative insights and operational guidelines*, in *Opinion Juris in Comparatione*, 2/2025, pp. 3 - 7; R. Chambers, *Editorial Introduction: Vulnerability, Coping and Policy*, in *IDS Bulletin*, vol. 20, 1989, pp. 1 ff; J. Fortuna, *Minors' digital vulnerability in the EU and the US: a comparison between the Digital Services Act and the Kids Online Safety and Privacy Act*, in *Comparative Law Review*, 2025, pp. 115 – 135; Id., *Il nuovo ruolo dei genitori nella tutela della vulnerabilità digitale dei minori: spunti di comparazione giuridica tra UE, USA, Italia e Australia*, in *Rivista di Diritti Comparati*, 2025, (forthcoming); F. Luna, *Elucidating the Concept of Vulnerability: Layers Not Labels*, in *International Journal of Feminist Approaches to Bioethics*, vol. 2, n. 1, 2009, pp. 121-139. On the concept of vulnerability within the EU, see G. Malgieri, *Vulnerability,* in *Elgar Encyclopedia of Law and Data Science*, ed. by G. Comandé, 2022, p. 363 ff.

ISSN 2281-5147

condition of vulnerability, minors are exposed to specific risks within an audiovisual ecosystem undergoing profound transformation[3], an ecosystem increasingly shaped by algorithmic logics, individualized consumption models, and opaque market dynamics. In this context, it becomes particularly urgent to examine the normative, technological, and cultural conditions that may enable the development of a truly *child-friendly* cinematic environment, in the fullest and most substantive sense of the term.

The digitalisation of media has profoundly redefined the cinematic experience of minors, altering not only the modalities of access to content but also the forms of interaction and meaning-making[4]. Cinemas, once privileged spaces for cultural socialisation and collective viewing, have been progressively complemented, and in part supplanted, by domestic, mobile and individualised viewing experiences, facilitated by streaming platforms and the widespread availability of audiovisual content through social media. In such a scenario, the aesthetic dimension becomes intertwined with the digital, the boundaries between entertainment and art are blurred and the curation of content shifts from human programmers to algorithmic recommendation systems.

This transformation acquires even greater significance when read through a historical lens. The 2011 report *Audiovisual Media for Children in Europe*, published by the European Audiovisual Observatory[5], offered a portrayal of the sector that was still strongly anchored in traditional television and film. It emphasised key concerns such as the limited cross-border circulation of European productions, the market dominance of U.S. content, and the marginal presence of nationally produced animation in children's programming. At that time, the main regulatory challenges revolved around public support policies, territorial distribution, and programming quotas.

---

[3] Cf. M. Guštin, *Challenges of Protecting Children's Rights in the Digital Environment*, in *ECLIC*, 2022, p. 453 ff.; S. P. Hammond, G. Polizzi, C. Duddy, Y. Bennett-Grant, K. Bartholomew, *Children's, parents' and educators' understandings and experiences of digital resilience: A systematic review and meta-ethnography*, in *New Media & Society*, 2024.

[4] On this topic, see the following paragraphs.

[5] Available at https://rm.coe.int/audiovisual-media-for-children-in-europe/168078996f.

ISSN 2281-5147

Today, by contrast, the core issue is no longer content *availability*, but rather its *visibility*, *selection*, and *mediation*. Content aimed at children is now proposed within opaque and highly personalised digital environments, through recommendation systems which, despite offering tailored experiences, tend to reinforce cultural standardisation, polarisation and repetitiveness[6]. This gives rise to a concrete risk of narrowing the narrative and imaginative spectrum accessible to minors, with significant implications for their cultural literacy, aesthetic development and critical understanding of mediated representations.

At the same time, a profound hybridisation is taking place between audiovisual consumption and social media practices. Video-on-demand platforms are no longer merely passive archives of cinematographic works, as they are immersed in interactive ecosystems where viewing is intertwined with the participatory dynamics typical of social media: likes, comments, shares, remixes, short-form reactions, and viral diffusion. The cinematic experience becomes fragmented and reassembled through transmedia logics, where meaning is generated through fast, often ephemeral and performative interactions. This marks a significant departure from the dialogic, reflective, and collective nature of traditional cinematic consumption.

In parallel, the regulatory framework has also evolved. While public debate and legal regulation once focused primarily on tools such as national quotas, public funding and media pluralism, today's concerns have shifted toward algorithmic transparency, data-driven personalisation, behavioural profiling, and commercial surveillance[7]. The digitalisation of cinema thus does not simply entail a technological transition, but a deep reconfiguration of the relationship between children, culture, and technology. This demands the development of new regulatory and governance models capable of

[6] See par. 4.

[7] Cf. https://www.obs.coe.int/en/web/observatoire/-/algorithmic-transparency-and-accountability-of-digital-services ; V. Verdoodt, E. Lievens, A. Chatzinikolaou, *The EU Approach to Safeguard Children's Rights on Video-Sharing Platforms: Jigsaw or Maze?*, In *Media and Communication*, Vol. 11, Issue 4, 2023, pp. 151–163 available at https://doi.org/10.17645/mac.v11i4.7059; E. Leijten, S. van der Hof, *Dissecting the Commercial Profiling of Children: A Proposed Taxonomy and Assessment of the GDPR, DSA and AI Act in Light of the Precautionary Principle*. Available at SSRN: https://ssrn.com/abstract=5055046 or http://dx.doi.org/10.2139/ssrn.5055046.

ISSN 2281-5147

reconciling protection with empowerment, and safeguarding with cultural participation, ensuring both freedom of access and the right to cultural diversity.

From a legal standpoint, the primary normative reference on the relationship between children and artistic products (including, therefore, cinematographic products) is Article 31 of the United Nations Convention on the Rights of the Child (CRC)[8], which enshrines every child's right to rest and leisure, to engage in play and recreational activities appropriate to their age, and to participate freely in cultural and artistic life[9]. This recognition entails that children must have access to cultural, artistic and audiovisual content that is age-appropriate and responsive to their needs and interests: the quality of such content must align with the objectives outlined in international and European policy strategies. States are therefore obliged not only to protect children from materials that may be detrimental to their physical, mental, or moral development, but also to promote and support the production of content that fosters children's cultural expression and creativity.

This right finds a parallel in Article 22 of the Charter of Fundamental Rights of the European Union[10], which promotes cultural diversity and equitable access to content. However, in the current digital environment, the effective realisation of such rights faces considerable structural obstacles: closed ecosystems, profit-driven engagement logics, lack of transparency in content curation, and the absence of harmonised standards for the protection of minors across platforms.

In this context, the cinematic experience in the digital age emerges as an ambivalent frontier. On the one hand, it offers extraordinary opportunities for access, creativity, and cultural agency; on the other, it risks fostering passive, homogenised, and commercially-driven forms of consumption. Consequently, public policies and regulatory frameworks - including cooperation among institutions, digital platforms,

[8] Convention on the Rights of the Child Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989 entry into force 2 September 1990, in accordance with article 49, available at https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

[9] Regarding this article, see also the following paragraph.

[10] Charter of Fundamental Rights of the European Union, Art. 22: "Cultural, religious and linguistic diversity. The Union shall respect cultural, religious and linguistic diversity".

ISSN 2281-5147

schools, and families[11] - must respond not only to the imperative of protecting minors, but more fundamentally, to the need to actively promote their cultural rights, recognising them as autonomous and competent individuals capable of participating fully in cultural life.

Against this backdrop, the present contribution aims to critically examine the evolution of children's cinematic experience in the European digital context. It seeks to interweave the international and European legal frameworks with an analysis of the strategies adopted by streaming platforms and the regulatory gaps that continue to hinder effective protection. The objective is twofold: first, to identify the structural risks that undermine children's rights in digitised audiovisual environments; and second, to propose legal and policy measures for the construction of a more inclusive, pluralistic, and child-centred cinematic ecosystem—one that meaningfully integrates protection, participation, and cultural diversity.

To set up an EU competitive and child-friendly film industry, the rights of the child shall be enhanced and promoted by institutional and private stakeholders. To this end, a preliminary step involves analysing the international frameworks established by the UN Convention on the Rights of the Child, alongside the EU Strategy on the Rights of the Child (2021)[12] and the Council of Europe Strategy for the Rights of the Child (2022–2027)[13], in order to understand how these instruments inform and guide policy development within the film industry.

It is therefore useful to first proceed with a brief analysis of the general legal framework for the protection of minors and then identify the specific relevant provisions relating to the relationship between minors and cinema.

---

[11] On the educational role of parents, see G. Di Rosa, *I termini giuridici della funzione educativa nell'attuale quadro delle relazioni tra genitori e figli*, in *Actualidad Jurídica Iberoamericana* Nº 17 bis, 2022, p. 806 ff.

[12] https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/rights-child/eu-strategy-rights-child-and-european-child-guarantee_en#documents.

[13] https://rm.coe.int/council-of-europe-strategy-for-the-rights-of-the-child-2022-2027-child/1680a5ef27.

ISSN 2281-5147

2. Legal Framework on Children's Rights and the Cinematic Experience: United Nations Convention on the Rights of the Child and European Strategies.

In outlining a framework for the protection and promotion of children's rights in the digital environment[14]-specifically in relation to contemporary cinematic experiences- it is essential to recall the legal and programmatic instruments that, over the past decades, have profoundly reshaped the concept of childhood and the role of children in society. First and foremost, the United Nations Convention on the Rights of the Child (CRC), adopted in 1989[15], marks a turning point in the legal recognition of children as full rights-holders, endowed with intrinsic dignity and capable of forming and expressing their own views[16]. Far from considering children as merely passive objects of care or tutelage, the CRC introduces a legal paradigm in which children are active protagonists of their personal and social lives. The Convention enshrines not only the right to protection but also civil, political, cultural and participatory rights. These include the right to be heard in all matters affecting the child (Article 12), freedom of expression (Article 13), freedom of thought, conscience and religion (Article 14) and freedom of association (Article 15)[17]. The recognition of the child's

[14] Cf. C. Djeffal, *Children's Rights by Design and Internet Governance: Revisiting General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*, in Laws, 11, 84, 2022, https://doi.org/10.3390/laws11060084; UNICEF, D. Özkul, S. Vosloo, B. Baghdasaryan, *Best Interests of the Child in Relation to the Digital Environment*, working paper, February 2025, https://www.unicef.org/innocenti/reports/best-interests-child-relation-digital-environment?utm_source=chatgpt.com; M. Guštin, *Challenges of Protecting Children's Rights in the Digital Environment*, in ECLIC, 2022, p. 453 ff.;

[15] Convention on the Rights of the Child Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989 entry into force 2 September 1990, in accordance with article 49, available at https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

[16] C. Djeffal, *Children's Rights by Design and Internet Governance: Revisiting General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment,* in *Laws*, 11, 84, 2022, cit., https://doi.org/10.3390/laws11060084;

[17] See CRC, Art. 12: "1. States Parties shall assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child. 2. For this purpose, the child shall in particular be provided the opportunity to be heard in any judicial and administrative proceedings affecting the child, either directly, or through a representative or an appropriate body, in a manner consistent with the procedural rules of national law"; Art. 13: "1. The child 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

ISSN 2281-5147

evolving capacities, discernment, and active role in the construction of his or her identity[18] is thus central to the Convention's architecture.

These provisions are accompanied by further rights, such as the right to life and development (Article 6), to name and identity (Article 7), to family relations (Article 8), to health (Article 24), to education (Article 28), and to participation in cultural and artistic life (Article 31)[19]. At the core of the Convention lies the principle of the best interests of the child (Article 3), which must guide all decisions concerning children, whether by public or private institutions, administrative bodies, courts, or legislative authorities[20].

---

form of art, or through any other media of the child's choice. 2. The exercise of this right may 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; or (b) For the protection of national security or of public order (ordre public), or of public health or morals"; Art. 14: "1. States Parties shall respect the right of the child to freedom of thought, conscience and religion. 2. States Parties shall respect the rights and duties of the parents and, when applicable, legal guardians, to provide direction to the child in the exercise of his or her right in a manner consistent with the evolving capacities of the child. 3. Freedom to manifest one's religion or beliefs may be subject only to such limitations as are prescribed by law and are necessary to protect public safety, order, health or morals, or the fundamental rights and freedoms of others". Art. 15: "1. States Parties recognize the rights of the child to freedom of association and to freedom of peaceful assembly. 2. No restrictions may be placed on the exercise of these rights other than those imposed in conformity with the law and which are necessary in a democratic society in the interests of national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms of others".

[18] C. Hällgren, A. Björk, *Young people's identities in digital worlds*, in *International Journal of Information and Learning Technology*, 2022; K. Hamming, *A Dangerous Inheritance: A Child's Digital Identity*, in *Seattle University Law Review*, n. 43, 2020;

[19] Regarding this article, see also the previous paragraph.

[20] United Nations Convention on the Rights of the Child, New York, November 20, 1989, Art. 3, para. 1: " In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration"; Article 24 of the Charter of Fundamental Rights of the European Union ("Charter of Nice") follows in the footsteps of Article 3, establishing that in all actions relating to children, whether taken by public authorities or private institutions, the best interests of the child must be a primary consideration. See also Australian Online Safety Amendment (Social Media Minimum Age) Bill 2024, Explanatory memorandum, p. 10: "Human rights implications 4. The Bill engages the following rights: The principle that the best interests of a child shall be a primary consideration in actions concerning children in Article 3 of the Convention on the Rights of a Child (CRC)". On the best interests of the child, see also L. Lenti, «*Best interests of the child*» *o «best interests of children*»?, in *Nuova giur. comm*., 2010, p. 157 ff.; *Idem*, *Note critiche in tema di interesse del*

ISSN 2281-5147

The film industry plays a strategic role in the realization of the right to cultural participation enshrined in Article 31 CRC[21], not only because of its impact on the collective imagination, but also because of the opportunities it offers in terms of access and active involvement of children.

Article 31 reflects the awareness that play, leisure, and cultural participation are essential components of a child's harmonious development, from cognitive, emotional, and social standpoints. Recreational, artistic, and cultural activities contribute to identity formation, emotional expression, socialisation, and non-formal learning. The second paragraph of Article 31 commits State Parties to "respect and promote the right of the child to participate fully in cultural and artistic life and to encourage the provision of appropriate and equal opportunities for cultural, artistic, recreational and leisure activity". This wording is particularly significant, as it excludes any passive approach to cultural enjoyment and instead affirms the right to active and full participation, even in the cinematic experience. Such a right must be guaranteed without discrimination of any kind and in accordance with the principle of the best interests of the child (Article 3 CRC).

---

minore, in *Riv. dir. civ.*, 2016, p. 86 ff. V. Scalisi, *Il superiore interesse del minore, ovvero il fatto come diritto*, in *Riv.dir. civ.*, 2018, n° 2, p. 405 ff.; E. Lamarque, *Prima i bambini. Il principio dei best interests of the child nella prospettiva costituzionale*, FrancoAngeli, Milan, 2016; E. Lamarque, *Pesare le parole. Il principio dei best interests of the child come principio del miglior interesse del minore*, in *Famiglia e dir.*, 2023, p. 365 ff. U.C. Basset, *The Best Interests of the Child: The New Challenges of a Vague Concept*, in M. Bianca (ed.), *The Best Interests of the Child*, 2020; With regard to the evolution of the best interests of the child, it has recently been observed that analyzing the principle in question from a more general, systematic perspective, it can be seen that the concept of 'best interests of the child' encompasses not only interests understood as legal situations of a lower rank, but also the rights of the child itself, such as freedom, health, education, and training. In fact, the best interest of the child now stands as a general clause whose content is not defined in an unambiguous and abstract way, but must be completed from time to time in its concrete meaning by the interpreter: thus L. Vizzoni, *I "minori digitali" tra doveri educativi e tutele*, cit., p. 36.

[21] CRC, Art. 31: "1. States Parties recognize the right of the child to rest and leisure, to engage in play and recreational activities appropriate to the age of the child and to participate freely in cultural life and the arts. 2. States Parties shall respect and promote the right of the child to participate fully in cultural and artistic life and shall encourage the provision of appropriate and equal opportunities for cultural, artistic, recreational and leisure activity". See S. McNeill, *Article 31 of the CRC - The Right to Play, Rest and Leisure: A Forgotten Right for Children?,* in *King's Student L. Rev.*, 10, 2, 2019; P. David, *Article 31: The right to leisure, play and culture*, Martinus Nijhoff Publishers, 2006.

ISSN 2281-5147

Cinema can be a powerful tool for promoting cultural pluralism, the representation of minorities[22] and linguistic diversity. It is therefore crucial to promote the creation and dissemination of film content for children that upholds their rights, ensures accessibility, and reflects diverse social realities. Moreover, children's active involvement in film workshops, school projects, and festivals fosters their critical thinking and film literacy, while simultaneously nurturing their creativity. Indeed, for example the EU supports such initiatives through the Creative Europe MEDIA program[23], which funds inclusive and educational projects. These activities respond to the EU's strategic objective of normalizing the participation of minors and creating a child-friendly cultural environment.

In the European context, this shift has been embraced and further developed through comprehensive policy strategies aimed at making children's rights effective in contemporary societies. Among the most significant instruments are the already mentioned Council of Europe Strategy for the Rights of the Child (2022–2027) and the European Union Strategy on the Rights of the Child (2021), both grounded in the CRC and designed to respond to the complex interplay of protection, autonomy, and participation in the lives of children and adolescents.

The Council of Europe Strategy, entitled *Children's Rights in Action: From Continuous Implementation to Joint Innovation*[24], articulates a coherent vision for the promotion and

[22] D. Popa, F. Nechita, Y. Liu, S. Wei Lee Chin, *Linking Positive Psychology and Intercultural Competence by Movies: Evidence From Brunei and Romania*, in Frontiers in Psychology, 2021, 19;12:750904, doi: 10.3389/fpsyg.2021.750904. PMID: 34737717; PMCID: PMC8562382; E. D. Romero, J. Bobkina, *Including diversity through cinema-based affective literacy practices: A case study with EFL/ESL pre-service teachers*, in *Innovation in Language Learning and Teaching*, 17(4), 2023, pp. 859–871. https://doi.org/10.1080/17501229.2023.2168007; D. Bamman, R. Samberg, R.J. So, N. Zhou, *Measuring diversity in Hollywood through the large-scale computational analysis of film*, in *Proc. Natl. Acad.* 2024, 12;121(46):e2409770121, doi: 10.1073/pnas.2409770121. Epub 2024 Nov 4. PMID: 39495931; PMCID: PMC11573682.

[23] https://culture.ec.europa.eu/creative-europe/creative-europe-media-strand; https://digital-strategy.ec.europa.eu/en/policies/creative-europe-media.

[24] On this topic, see also Council of Europe Strategy for the Rights of the Child (2022-2027). First implementation report of the Council of Europe Strategy for the Rights of the Child, January 2024, available at https://rm.coe.int/cdenf-2023-27-final-first-implementation-report-2022-2023-/1680ae0ef3?utm_source=chatgpt.com; Mid-Term Review Conference for the Strategy for the Rights of the Child (2022-2027), Conference report, https://rm.coe.int/report-mtr-en-/1680b6655a

ISSN 2281-5147

realization of children's rights across the 46 member states. It is based on six strategic priorities: freedom from violence, equal opportunities and inclusion, child-friendly justice, child participation, safe access to technology, and children's rights in crisis situations[25]. Each area is addressed through an integrated and participatory methodology, seeking to overcome fragmented interventions and foster systemic change. Notably, the Strategy was co-designed through a wide consultation process involving more than 220 children across ten countries[26], whose suggestions were included in the final text under the heading *What children suggest*[27]. This process reflects a clear epistemological and political shift: from designing policies *for* children to co-constructing policies *with* children.

The EU Strategy on the Rights of the Child[28] takes a similar holistic approach, addressing both structural challenges and emerging risks through six interconnected priority areas. Indeed, it promotes children's participation in democratic life, with a focus on the use of digital tools for expression and consultation and strengthens efforts to prevent and combat all forms of violence, including online abuse and cyberbullying. The strategy also emphasizes the importance of creating inclusive societies by addressing child poverty and discrimination, while promoting safe and inclusive digital environments. Furthermore, it aims to ensure access to child-friendly justice and to promote the protection and promotion of children's rights worldwide,

---

25 Cf. https://rm.coe.int/council-of-europe-strategy-for-the-rights-of-the-child-2022-2027-child/1680a5ef27.

26 E. Kovács-Szépvölgyi , D. A. Tóth and R. Kelemen, *From Voice to Action: Upholding Children's Right to Participation in Shaping Policies and Laws for Digital Safety and Well-Being*, in *Societies* 2025, *15*(9), p. 8; https://doi.org/10.3390/soc15090243;

27 https://rm.coe.int/council-of-europe-strategy-for-the-rights-of-the-child-2022-2027-child/1680a5ef27, pp. 6-7.

28 About this topic, cf. B. M. Sacur , E. Diogo, *The EU Strategy on the Rights of the Child and the European Child Guarantee—Evidence-Based Recommendations for Alternative Care*, in *MDPI Children,* 2021, 8, 1181. https://doi.org/10.3390/children8121181; A. Dunhill, M. Schuurman, E. P. Tormen, *The EU Strategy on the Rights of the Child: What does this mean for the EU and Germany?*, in *Eurochild*, 2021, https://eurochild.org/uploads/2021/06/Eurochilds-Article-_-The-EU-Strategy-on-the-Rights-of-the-child_15.06.pdf

ISSN 2281-5147

with a particular focus on emergency contexts[29]. The Strategy is the result of a consultation involving more than 10,000 children and youth[30] and offers a programmatic roadmap for EU institutions and Member States, even though it is not legally binding. The Commission has committed to developing monitoring and evaluation tools to assess the progress of implementation.

For what is most relevant to our purposes, even within the EU Strategy on the Rights of the Child, cultural and artistic participation is listed among the rights for the well-being and development of children, including the audiovisual sector[31]. The strategy highlights the importance of safe and inclusive digital environments, with regard to the enjoyment of audiovisual online content[32], and promotes the meaningful participation of children in decision-making processes, including in the creation of cultural content[33]. Furthermore, it aims to protect children against harmful content, aggressive advertising, or misinformation, in line with European media rules[34]. Key actions include promoting environments that encourage artistic expression, play, and creativity, particularly for children at risk of social exclusion, such as Roma children,

[29] Cf. European Union Strategy on the Rights of the Child (2021), https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/rights-child/eu-strategy-rights-child-and-european-child-guarantee_en#documents.

[30] European Union Strategy on the Rights of the Child (2021), https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/rights-child/eu-strategy-rights-child-and-european-child-guarantee_en#documents, p.3.

[31] European Union Strategy on the Rights of the Child (2021), pp. 1-2.

[32] European Union Strategy on the Rights of the Child (2021), p. 15: "Children play, create, learn, interact and express themselves in an online and connected environment, from a very young age" and p. 17.

[33] European Union Strategy on the Rights of the Child (2021), p. 4: "The EU needs to promote and improve the inclusive and systemic participation of children at the local, national and EU levels[…]" and "The Commission will […] ensure the right of the child to be heard and listened to… promote meaningful and inclusive participation of children in the policy-making process".

[34] European Union Strategy on the Rights of the Child (2021), p. 16–17, "Children's online presence increases their exposure to harmful or illegal content […] The revised Audiovisual Media Services Directive has strengthened the protection of children from harmful content and inappropriate commercial communications […] The Code of Practice on Disinformation will establish a co-regulatory regime tailored for tackling the risks linked to the spread of disinformation".

ISSN 2281-5147

migrants, or children with disabilities[35]. By recognizing children's right to culture and their active role in its production, the Strategy indirectly recognizes the role of minors in the film industry, finally calling for greater investment in equitable access to culture, including through the establishment of ad hoc bodies[36].

Despite efforts to establish a favorable regulatory framework, the effective implementation of the right to cultural participation continues to encounter significant obstacles, primarily stemming from socio-economic inequalities. Many children, in fact, lack access to cinemas, theatres, museums, or extracurricular activities due to high costs or insufficient local facilities. Territorial disparities, especially between urban centers and rural or peripheral areas, further exacerbate these inequalities.[37] Furthermore, cultural and linguistic barriers continue to affect foreign, migrant, and refugee children, while media representation of LGBTQIA+ children, children with disabilities, and those belonging to ethnic minorities remains limited[38]. The EU Strategy seeks to address these critical challenges through systemic measures, including the integration of the cultural dimension into social, educational, and health policies. It also emphasizes the active involvement of children and

[35] European Union Strategy on the Rights of the Child (2021), pp. 6 –10.

[36] Cf. European Union Strategy on the Rights of the Child (2021), p. 6: "One of its main deliverables is the Commission's proposal for Council recommendation establishing the European Child Guarantee, which complements this Strategy and calls for specific measures for children at risk of poverty or social exclusion. The proposal recommends to Member States that they guarantee access to quality key services for children in need: early childhood education and care, education (including school-based activities), healthcare, nutrition, and housing".

[37] Yuke Meng, Han Li, Menghui Yin, Shanshan Sun , *Urban-Rural Disparities in Art Education Resources in China: Mechanisms and Equity Perspectives*, in Journal of Current Social Issues Studies, Vol.1, No.1, 2024, pp, 40-50; S. Rege, *Art Education in Rural vs. Urban Settings in India: A Comparative Study and Analysis*, in IJSDR, Vol. 10 Issue 3, 2025, pp. 1-6; L.M. Crispin, M. I. Beck, *Disparities in museum attendance among youth over two decades: an empirical analysis of who attends and how often*, in Arts Education Policy Review, 2023, 126(1), pp. 25–37. https://doi.org/10.1080/10632913.2023.2187499.

[38] J. Aspler, K. D. Harding, M. A. Cascio, *Representation Matters: Race, Gender, Class, and Intersectional Representations of Autistic and Disabled Characters on Television*, in Studies in Social Justice, Volume 16, Issue 2, 2022, pp. 323-348, A. L. Snyder, J. A. Bonus, D. P. Cingel, *Representations of LGBQ+ families in young children's media, in Journal of Children and Media*, 17(1), 2023, pp. 154–160, https://doi.org/10.1080/17482798.2023.2173856;

ISSN 2281-5147

adolescents in decision-making processes that concern them, by means of dedicated consultations and participatory platforms at local, national, and European levels[39].

Both strategies underscore the indivisibility and interdependence of children's rights, reaffirming the need to strengthen both protection and autonomy in response to contemporary challenges, such as the digitalization of everyday life, the persistence of inequalities, and the fragmentation of access to cultural and communicative resources[40]. Particularly significant in this regard are the axes dedicated to digital and cultural inclusion, awareness-raising on safe and responsible technology use, and the promotion of child participation in decision-making processes[41]. These priorities are not merely instrumental: they reflect a deeper paradigm shift that calls for a rethinking of cultural policies (including those relating to the use of audiovisual content) through a child-centered lens, capable of recognizing minors not only as vulnerable subjects to be safeguarded, but as active agents in the symbolic construction of shared meaning.

The Strategies therefore emphasize that ensuring every child's effective right to culture requires a comprehensive and coordinated approach that brings together institutions, schools, cultural organizations, families, and the third sector. Such integration is essential not only to eliminate all forms of discrimination but also to value children's individual identities, enabling them to become active agents within the cultural domain, and particularly within cinema. Participation in cultural and recreational life must be recognized as a fundamental and enforceable right, rather than as a privilege. This right, enshrined in Article 31 of the UNCRC and promoted by the EU Strategy on the Rights of the Child, must be guaranteed in a universal and accessible manner and cinema, as a central component of the cultural and creative industries, holds the power to educate, inspire, and amplify children's voices. However, this potential can only be fulfilled if cinema is guided by principles of inclusion, diversity, and participatory engagement. Striving toward this objective

[39] Cf. European Union Strategy on the Rights of the Child (2021), pp. 6 –10.

[40] Cf. Council of Europe Strategy for the Rights of the Child (2022–2027) pp. 8-9, 13-15, 18-19 and European Union Strategy on the Rights of the Child (2021), pp. 2, 6-8, 15-17.

[41] Cf. Council of Europe Strategy for the Rights of the Child (2022–2027) pp. 14 -19 e European Union Strategy on the Rights of the Child (2021, pp.15-17, 8-10, 3-5.

ISSN 2281-5147

ultimately contributes to the construction of a fairer, more imaginative, and more compassionate society, one that values the perspectives of younger generations as essential catalysts for cultural renewal and transnational progress.

3. European Regulation on Audiovisual Media and Digital Platforms.

Considering the fundamental contribution that cultural participation and access to high-quality audiovisual content make to children's holistic development, it becomes necessary to examine, in particular, the regulatory framework governing the creation, distribution, and reception of media addressed to young audiences. The full realization of the rights enshrined in the United Nations Convention on the Rights of the Child (CRC) and promoted by European strategies requires, in fact, a regulatory ecosystem consistent with the principle of the best interests of the child[42]. This principle — open, relational, and inherently context-sensitive — must be filled with substantive meaning in light of the specificities of each case[43]. In the present domain, it translates into the duty to adopt measures capable of shielding children from harmful content, fostering inclusion, and ensuring safe, stimulating, and culturally enriching digital environments.

Children, as well established, occupy a condition of structural vulnerability, stemming from their status as developing subjects who are particularly receptive to external

[42] The concept of the best interests of the child is enshrined in Article 3 of the United Nations Convention on the Rights of the Child (CRC), which provides that "in all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration". On the concept of the best interests of the child, see, non-exhaustively: U.C. Basset, *The Best Interests of the Child: The New Challenges of a Vague Concept*, in M. Bianca (ed.), *The Best Interests of the Child*, 2020, p. 5; E. Lamarque, *Prima i bambini. Il principio dei best interests of the child nella prospettiva costituzionale*, FrancoAngeli, Milan, 2016; J. Zermatten, *The Best Interests of the Child Principle: Literal Analysis and Function*, *The International Journal of Children's Rights*, 18(4), 2020, pp. 483–499, https://doi.org/10.1163/157181810X537391; P. Alston, *The Best Interests Principle: Towards a Reconciliation of Culture and Human Rights*, *International Journal of Law and the Family*, 8 (1994), p. 2; C. Breen, *The Standard of the Best Interests of the Child: A Western Tradition*, *International and Comparative Law*, The Hague, 2002.

[43] L. Musselli, *La tutela dei minori tra media audiovisivi e servizi di condivisione video*, in R. Mastroianni, O. Pollicino, M. Bassini (eds.), *Il T.U. dei servizi di media audiovisivi*, Milan, 2024, p. 105; P. Stanzione, *Persone vulnerabili e strumenti di tutela*, Budapest, 11 May 2023, available at garanteprivacy.it.

ISSN 2281-5147

influences and not yet fully equipped with critical maturity[44]. There thus emerges a clear need for heightened protection, a need firmly acknowledged in both legal doctrine and positive law[45]. The question, therefore, no longer concerns the *an* of protection, but rather the *quomodo*: the concrete modalities through which such protection should materialise within the contemporary media landscape.

In recent years, as outlined above (see par. 1), a profound transformation has reshaped the audiovisual environment, altering not only its economic and technological structure but also the very paradigms of content production, distribution, and consumption. The traditional model of linear broadcasting has been progressively replaced by interactive, *on-demand*, and algorithmically personalized experiences[46], made possible by the ubiquity of connected and mobile devices. At the same time, the rise of new global operators[47] and the spread of video-sharing platforms and social media[48] have driven a shift from a centralized editorial paradigm to a highly disintermediated ecosystem[49], in which users, including minors, are no longer mere recipients but also active producers of content[50].

---

[44] See: A. Spangaro, *Minori e mass media: vecchi e nuovi strumenti di tutela*, Milano, 2011; A. Barbera, *Mezzi di comunicazione televisiva e tutela dei minori*, in *forumcostituzionale.it*; G. De Minico, *Il favor minoris: un orizzonte lontano*, in G.B. Abbamonte, E. Apa, O. Pollicino (a cura di), *La riforma del mercato audiovisivo europeo*, Torino, 2019, pp. 99 ss..

[45] For a general analysis of child well-being, see: Z. Vagheri, J. Zermatten, G. Lansdown, R. Ruggiero, (eds) Monitoring State Compliance with the UN Convention on the Rights of the Child. Children's Well-Being: Indicators and Research, vol 25. Springer, 2022.

[46] For a discussion of algorithmic governance within the on-demand economy, see C. Schubert and M.-T. Hütt, *Economy-on-Demand and the Fairness of Algorithms*, in *European Labour Law Journal*, 10(1), 2019, pp. 3–16.

[47] Such as Netflix, Amazon Prime Video, and Disney+.

[48] I.e., YouTube, TikTok, Twitch, Vimeo, Instagram.

[49] F. Graziadei, *Disintermediazione e responsabilità: dai servizi di media audiovisivi alle piattaforme digitali*, in F. Bruno, V. Lobianco, A. Perrucci, A. Preta (a cura di), *La televisione del futuro. Le prospettive del mercato televisivo nella transizione digitale*, Bologna, 2023, p. 467.

[50] V. Verdoodt, E. Lievens, A. Chatzinikolaou, *The EU Approach to Safeguard Children's Rights on Video-Sharing Platforms: Jigsaw or Maze?*, cit., pp. 151-163.

ISSN 2281-5147

This structural change has necessitated a comprehensive rethinking of media governance models. The 2018 revision of the Audiovisual Media Services Directive (AVMSD) (Directive (EU) 2018/1808, amending Directive 2010/13/EU) was born precisely out of an awareness of this transition, aiming to extend existing safeguards to the evolving digital environment[51]. The Directive thus represents the Union's primary legal framework for coordinating the provision of audiovisual media services across Member States and embodies the EU's commitment to building a modern, flexible, and technologically neutral regulatory environment capable of adapting to the evolving patterns of communication and consumption.

Its core objectives include the protection of minors, the promotion of cultural and linguistic diversity, and the enhancement of the competitiveness of the European audiovisual sector. The most significant innovation introduced by the 2018 revision lies in the expansion of the Directive's material scope, which now encompasses not only linear and *on-demand* services but also *video-sharing platforms* (VSPs). These platforms, though not exercising direct editorial responsibility over user-generated content[52], are nonetheless required to implement effective measures to protect minors from material that could impair their physical, mental, or moral development[53].

[51] Recital 1 of Directive (EU) 2018/1808 amending Directive 2010/13/EU of the European Parliament and of the Council states: "The last substantive amendment to Council Directive 89/552/EEC, subsequently codified by Directive 2010/13/EU of the European Parliament and of the Council, was made in 2007 with the adoption of Directive 2007/65/EC of the European Parliament and of the Council. Since then, the audiovisual media services market has evolved significantly and rapidly due to the ongoing convergence of television and internet services. Technical developments have allowed for new types of services and user experiences. Viewing habits, particularly those of younger generations, have changed significantly. While the main TV screen remains an important device for sharing audiovisual experiences, many viewers have moved to other, portable devices to watch audiovisual content. Traditional TV content still accounts for a major share of the average daily viewing time. However, new types of content, such as video clips or user-generated content, have gained an increasing importance and new players, including providers of video-on-demand services and video-sharing platforms, are now well-established. This convergence of media requires an updated legal framework in order to reflect developments in the market and to achieve a balance between access to online content services, consumer protection and competitiveness".

[52] See Recital 47 of Directive (EU) 2018/1808.

[53] Recital 20 of Directive (EU) 2018/1808 states: "The appropriate measures for the protection of minors applicable to television broadcasting services should also apply to on-demand audiovisual media services. That should increase the level of protection. The minimum harmonisation approach

ISSN 2281-5147

Among these measures are the prohibition of content causing serious harm — such as gratuitous violence or pornography[54] —, the implementation of age-rating and parental control systems, the adoption of filtering technologies, reporting mechanisms, and age-verification procedures.

These provisions mark a conceptual turning point: from reactive censorship to a preventive governance of risks, through a *safety-by-design* model that embeds child protection within the very architecture of digital services[55].

At the same time, the Directive promotes the dissemination of positive content. Article 13 requires on-demand service providers to ensure that at least 30% of their catalogues consist of European works and that these works are given appropriate prominence on their platforms. This measure, far from being merely quantitative, seeks to sustain the production and circulation of culturally diverse narratives, contributing to the construction of a shared and inclusive imaginary that mirrors the plurality of childhood experiences across Europe.

Additional safeguards are established in the field of audiovisual commercial communication. Article 9 prohibits advertising that exploits children's inexperience or credulity, encourages unsafe behaviour or excessive consumption, or perpetuates discriminatory representations. It also bans advertising of tobacco products and

allows Member States to develop a higher degree of protection for content which may impair the physical, mental or moral development of minors".

[54] Art. 1, point (10) of Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive), which inserts Article 6a into Directive 2010/13/EU: "Member States shall take appropriate measures to ensure that audiovisual media services provided by media service providers under their jurisdiction which may impair the physical, mental or moral development of minors are only made available in such a way as to ensure that minors will not normally hear or see them. Such measures may include selecting the time of the broadcast, age verification tools or other technical measures. They shall be proportionate to the potential harm of the programme".

[55] This shift towards a *by-design* model of protection is consistent with the broader regulatory approach adopted at the European level for digital services — an approach likewise embodied in the GDPR, the DSA and the AI Act, which will be discussed *infra*.

ISSN 2281-5147

imposes strict limitations on alcohol-related advertising directed at minors[56]. Furthermore, particular attention is devoted to the effective protection of children from exposure to audiovisual commercial communications related to gambling activities[57].

In a combined interpretation, these provisions outline a European and international regulatory framework that acknowledges the essential role of media — including cinema and digital platforms — in ensuring not only children's protection, but also their well-being and cultural participation[58]. The resulting obligations rest both upon Member States and upon audiovisual service providers, who are required to integrate child-rights considerations throughout the processes of content production, curation, and distribution.

Yet, the rapid pace of technological innovation continues to raise complex normative and operational challenges.

Persistent difficulties remain in delineating the precise boundaries between audiovisual regulation and the broader regime governing digital services, now recast by the EU Reg. 2022/2065 on Digital Services Act. The latter – as will be further explored in the following sections (see parr. 4 and 5) – appears inapplicable to on-demand platforms, while its provisions fully apply in cases where users themselves create and share content on social networks or video-sharing services. This demarcation line between regulatory regimes calls for further systematic clarification.

Moreover, significant regulatory asymmetries persist between traditional broadcasters and new digital actors, resulting in gaps in accountability. The fast-evolving nature of

[56] Art. 1, point (13) (3) of Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive)

[57] See Recitals 29 and 30 of Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive).

[58] For a comprehensive analysis, see H. Ranaivoson, S. Broughton Micova and T. Raats (eds.), *European Audiovisual Policy in Transition*, London–New York, 2023.

ISSN 2281-5147

advertising formats – from influencer marketing to personalised advertising – necessitates constant normative adaptation to prevent manipulation and exploitation of minors.

Furthermore, while the AVMSD marks a decisive step towards an integrated, multi-level framework of protection, its effective implementation ultimately depends on national transposition processes. Given the varying degrees of regulatory maturity among Member States, the risk of fragmented and inconsistent application remains substantial[59]. In this respect, the European Audiovisual Observatory plays a crucial role in monitoring regulatory developments and supporting evidence-based policymaking.

The persisting asymmetries and interpretative uncertainties call for a more cohesive and participatory governance model – one capable of translating regulatory principles into everyday practices of protection and empowerment. Ultimately, the full effectiveness of the Directive depends not merely on compliance with legal obligations, but on the ability of all stakeholders – institutional and private alike — to promote a genuinely *child-centred* model of governance. This requires the establishment of monitoring and participatory mechanisms that directly involve children themselves, aligning regulatory practice with the rights-based approach advocated by the CRC and the EU Strategy on the Rights of the Child. Only through an integrated, dynamic, and co-responsible governance framework can the audiovisual environment evolve into a truly inclusive space — one that protects, empowers, and authentically represents young audiences.

4. Risks of Addiction, Manipulation and Algorithmic Influence: Regulatory Foundations and Emerging Gaps.

If the AVMSD primarily governs the content dimension of audiovisual media, a complementary layer of protection concerns the design and architecture of the digital environments through which such content circulates. In this sphere, the focus shifts from *what* children watch to *how* they are guided, nudged, or influenced in their media consumption. The regulatory question thus moves from content regulation to the

[59] L. Musselli, *La tutela dei minori tra media audiovisivi e servizi di condivisione video,* cit., pp. 104 ss.

ISSN 2281-5147

governance of the interfaces, algorithms, and recommendation systems that mediate children's audiovisual experiences online[60].

In this sense, the cinematic and audiovisual experience of minors within the digital ecosystem extends far beyond passive content consumption. It increasingly intertwines with dynamics of interaction, personalization, and algorithmic recommendation that, if not properly regulated, may pose serious risks to the physical and psychological well-being and decisional autonomy of underage users. Social networks, in particular, expose minors to short clips, trailers, and fragments of films that may be inappropriate for their age, subtly influencing their viewing preferences and cultural consumption patterns. Among the most prominent risks are addiction to audiovisual content, exposure to manipulative design mechanisms, and the distorting influence of opaque algorithmic systems.

One of the main vectors of influence is the use of recommendation algorithms, which select and promote content based on users' browsing data and inferred preferences. For minors, such systems – when lacking transparency or ethical design principles – can generate repetitive and polarised exposure, narrowing cultural horizons and fostering compulsive viewing habits. In some cases, the recommended content may offer little educational or cultural value or even reinforce addictive behaviours such as binge-watching and engagement with viral trends[61].

Particularly concerning is the pervasive use of *dark patterns* in digital interfaces: deceptive design strategies intended to manipulate user behavior and steer individuals toward unintended or commercially advantageous choices[62]. Typical examples include

---

[60] V. Verdoodt, E. Lievens, A. Chatzinikolaou, *The EU Approach to Safeguard Children's Rights on Video-Sharing Platforms: Jigsaw or Maze?*, cit., pp. 151-163.

[61] For a perspective addressing the risks of addiction associated with personalised recommendation systems, see: K. Uludag, *Personalised Video Recommendation System and its Potential Role as a Trigger of Addiction*, in *Scientific Studios on Social and Political Psychology*, 29(2), 2023, pp. 44–46; A. Tripathi, T.S. Ashwin and R.M.R. Guddeti, *Emoware: A Context-Aware Framework for Personalized Video Recommendation Using Affective Video Sequences*, *IEEE Access*, 7, 2019; T. Kollmer, A. Eckhardt, *Dark Patterns. Conceptualization and Future Research Directions*, in *Business & Information Systems Engineering*, 65(2), 2023, pp. 201–208.

[62] M. Leiser, C. Santos, *Dark Patterns, Enforcement, and the Emerging Digital Design Acquis. Manipulation Beneath the Interface*, 2023, pp. 1–31.

ISSN 2281-5147

autoplay systems, pop-ups prompting content sharing, fake countdown timers, convoluted unsubscribe procedures, or interface layouts that obscure options for declining data processing. Such practices are especially harmful to minors who, by virtue of their age, cognitive development, and limited digital literacy,[63] are disproportionately vulnerable to manipulation and behavioral conditioning.

The autoplay function, for instance, automatically queues and launches the next video without requiring any affirmative choice. For younger audiences, whose impulse-control and time-management skills are still developing, autoplay effectively removes the moment of pause that would enable reflection, thereby facilitating prolonged and passive viewing. Similarly, infinite scroll designs—where content continuously loads as the user swipes—eliminate natural stopping cues and create a seemingly endless stream of stimuli. In addition, ambiguous consent banners or interfaces that visually highlight "accept all" options while obscuring privacy-protective choices can nudge minors toward sharing more data than they would otherwise intend. These persuasive design techniques exploit cognitive immaturity and limit the child's capacity to exercise informed and autonomous choices in the digital environment, transforming viewing into a frictionless, and often compulsive, behavioural loop.

These risks do not arise solely from the content itself but, more profoundly, from the modalities through which such content is framed, recommended, and consumed. Unless appropriately regulated, the digital environment may foster passive and conditioned behaviors that compromise children's autonomy and critical development. A child-rights-based approach therefore requires recognizing minors not merely as consumers, but as developing individuals entitled to the right to cognitive self-determination and to protection from undue manipulation[64], rights increasingly viewed as integral components of "digital human dignity".

Aware of these challenges, the European legislator has progressively developed a complex and interlocking regulatory framework designed to ensure safer, more

[63] On the need to promote digital literacy as a tool to mitigate the effects of children's vulnerability in general in the digital environment, reference may be made to: N. Patti, V. Punzo, R. Romano, *Child Vulnerabilities in the Digital Environment: Comparative Insights and Operational Guidelines*, cit., passim, and specifically pp. 45 ff.

[64] See above, par. 1.

ISSN 2281-5147

transparent, and fairer digital environments for minors. The Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter GDPR), the Regulation (EU) 2022/2065, known as the Digital Services Act (DSA), and the EU Regulation 2024/1689 on AI (Artificial Intelligence Act - AI Act) all converge in acknowledging age, cognitive development, and decision-making capacity as key dimensions of vulnerability that require special protection.

Article 22 of the GDPR[65] prohibits automated decision-making producing significant effects on individuals, while Recital 38 explicitly calls for enhanced safeguards for vulnerable data subjects, including children. Article 5(1)(b) of the AI Act prohibits the use of AI systems that exploit age-related vulnerabilities, notably those designed to distort or unduly influence the behaviour of children and adolescents.

However, the DSA[66] represents the cornerstone of the new European regulatory architecture for online platforms. Recitals 81 and 83 explicitly recognise that the design and functioning of digital services can significantly affect the physical, mental, and moral development of minors. Articles 34 and 35 impose on *Very Large Online Platforms (*VLOPs) – those reaching at least 45 million monthly active users in the EU – a duty to conduct annual assessments of the systemic risks associated with minors' use of their services[67]. Such risks include those related to excessive use, persuasive design, addictive recommendation loops, and profiling for commercial purposes. These assessments must be followed by proportionate and effective mitigation measures, which may include modifications to user interfaces, algorithmic recommendation systems, and advertising mechanisms.

[65] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679.

[66] Regulation (EU) 2022/2065 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:4625430.

[67] For a comment, see: D. Amram, Children (in the digital environment), in Elgar Encyclopaedia of Law and Data Science, G. Comandé (dir.), Elgar, 2022, pp. 64 ff.

ISSN 2281-5147

The DSA also embodies a co-regulatory logic, entrusting private platforms with proactive duties of care while preserving public oversight through transparency reporting, audits, and supervision by national Digital Services Coordinators. Article 28 further prohibits profiling for advertising purposes when it concerns minors, while Article 25 bans the deployment of *dark patterns:* manipulative design practices that undermine user autonomy and informed choice[68]. Although these prohibitions formally apply to all users, they are particularly relevant for minors, who are more susceptible to opaque interfaces and persuasive behavioural cues.

Taken as a whole, the European approach marks a paradigmatic shift: from reactive censorship to *ex ante* responsibility in the design of digital services, grounded in a *fairness-by-design* principle. Regulation thus moves upstream, embedding protection into the very architecture of online environments rather than relying solely on *ex post* content moderation.

Nevertheless, the effectiveness of this framework crucially depends on the subjective scope of application of the DSA. The obligations outlined above apply certainly to online platforms that host user-generated content and enable interaction among users. Accordingly, platforms where audiovisual material is continuously created, shared, and accessed by minors – unquestionably fall within the scope of the Regulation and are bound by its transparency, risk-assessment, and child-protection obligations.

By contrast, services representing one of the primary gateways to audiovisual content for children and adolescents, do not allow users to upload content or interact with one another. As catalogue-based content providers rather than interactive platforms, and given their growing influence in shaping children's audiovisual consumption habits, it is worth considering whether such services fall within the scope of the stricter regime established by the Digital Services Act (*see following section*) and are therefore subject to the obligations previously discussed, including, among others, systemic risk assessments and the prohibition of *dark patterns*.

[68] See also European Parliament, *Regulating Dark Patterns in the EU: Towards Digital Fairness*, *At a Glance – Digital Issues in Focus*, 2025, available at: https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/767191/EPRS_ATA(2025)767191_EN.pdf.

ISSN 2281-5147

The issue is far from marginal. The exclusion of these actors, though consistent with the letter of the Regulation, raises significant concerns in terms of regulatory equity, systemic coherence, and, above all, the effective protection of children's rights in the digital environment. The research will therefore address this question more closely, examining the implications of this asymmetry and the extent to which the current European framework can ensure consistent protection for minors across both interactive and non-interactive audiovisual environments.

5. Non-applicability of the Digital Services Act to Streaming Platforms Offering Video-on-Demand (VoD).

As mentioned above, major on-demand streaming services play a central role in shaping how children and adolescents' access, experience, and interpret audiovisual content. These platforms are widely used by younger audiences and strongly influence their cultural consumption patterns. Yet, despite their relevance in the digital ecosystem, such services fall outside the regulatory scope of Regulation (EU) 2022/2065, known as the Digital Services Act (DSA)[69].

The DSA applies to all providers of "intermediary services" offered to recipients located in the European Union, regardless of the provider's place of establishment. These intermediary services are classified into three categories: mere conduit, caching,

[69] About the Digital Services Act see, *ex multis*, S. Del Gatto, *Il Digital Services Act: un'introduzione*, in *Giornale di diritto amministrativo*, 6/2023, p. 724 ff.; A. Chander, *When the Digital Services Act Goes Global, Berkeley Technology Law Journal* 38, n. 3, 2023, p. 1067 ff.; F. Casolari, *Il Digital Services Act e la costituzionalizzazione dello spazio digitale europeo*, in *Giurisprudenza Italiana*, 2024, p. 462 ff.; C. Irti, *Piattaforme digitali, contratti e protezione dei dati personali*, in *I contratti*, 1/2024, p. 5 ff.; G. Finocchiaro, *Responsabilità delle piattaforme e tutela dei consumatori*, in *Giornale di diritto amministrativo*, 6/2024, p. 730 ff.; G. Pascuzzi, *Il diritto dell'era digitale*, Bologna, 2024, pp. 289-302; M. Husovec, *Principles of the Digital Services Act*, 2024, Oxford; F. Hofmann, B. Raue (ed. by), *Digital Services Act: Article-by-Article Commentary*, Monaco, 2024. In conjunction with the Digital Markets Act (Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828),the DSA aims to build the so-called digital single market; cf. also J. Quinn, *Regulating Big Tech: The Digital Markets Act and the Digital Services Act*, in *Dublin Law and Politics Review* 2, n. Finance Special Issue, 2021, pp. 2-4; M. L. Chiarella, *Digital Markets Act (DMA) and Digital Services Act (DSA): New Rules for the EU Digital Environment*, in *Athens Journal of Law (AJL),* 9, n. 1, 2023, p. 33 ff.

ISSN 2281-5147

and hosting[70]. A further category, "online platforms", is defined in Article 3(i) as a subset of hosting services that, in addition to storing user-generated content, also disseminate it to the public at the user's request[71].

[70] The DSA has a broad scope, covering all providers of intermediation services, including providers of "mere conduit," "caching" and "hosting" services. See DSA, Art. 4, 5. 6: Article 4, 'Mere conduit' "1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, the service provider shall not be liable for the information transmitted or accessed, on condition that the provider: (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission. 2. The acts of transmission and of provision of access referred to in paragraph 1 shall include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission. […]" Article 5, 'Caching' "1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, the service provider shall not be liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient or more secure the information's onward transmission to other recipients of the service upon their request, on condition that the provider: (a) does not modify the information; (b) complies with conditions on access to the information; (c) complies with rules regarding the updating of the information, specified in a manner widely recognized and used by industry; […]" Article 6, Hosting "1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, the service provider shall not be liable for the information stored at the request of a recipient of the service, on condition that the provider: (a) does not have actual knowledge of illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or (b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content". However, intermediaries falling within the above categories enjoy exemption from liability under certain conditions. In fact, the regulation stipulates that service providers who play a "passive" role with regard to the specific information hosted are exempt from liability for the information provided by a recipient of the service. It should also be noted that Article 8 of the DSA, concerning the absence of general monitoring obligations or active fact-finding, states that intermediary service providers shall not be subject to a general obligation to monitor the information they transmit or store, nor to actively seek facts or circumstances indicating illegal activity. On this aspect, see G. Pascuzzi, *Il diritto dell'era digitale* , Bologna, 2024, cit., pp. 295-296. However, on the exemption from liability for intermediaries acting as communication facilitators and on the concept of passivity, see also G. Sartor, *Providers Liability: From the eCommerce Directive to the future. In-Depth Analysis for the IMCO Committee*, 2017, available at https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf, pp. 24 and 26: "[…] we must abandon the view that only "passive" intermediaries should be protected, i.e., the view that intermediaries that take a "non-passive", or active role" – by indexing user-generated content, or linking advertising to it, or determining what results will be provided to user queries – should lose their protection from secondary liability. What justifies the exemption from secondary liability is not the passivity of intermediaries, but rather their function as communication enablers. This function would be incompatible with initiating the communications at issue, but may

ISSN 2281-5147

Streaming services, however, operate under a radically different model. They offer video-on-demand (VoD) services that provide professional, pre-selected audiovisual content acquired or produced in-house, made available to users via subscription. These services do not allow users to upload their own content, nor do they provide public spaces for interaction, commentary, or content sharing. In short, they do not qualify as environments for user-generated content, unlike social media platforms.

Given these characteristics, VoD platforms cannot be considered "hosting services" within the meaning of the DSA, as they do not store third-party content. Nor do they meet the definition of "online platforms" under Article 3(i), since they do not disseminate user-generated material. Similarly, they are not involved in mere conduit or caching activities, as they do not passively transmit or temporarily store user data on behalf of recipients.

As a result, streaming services offering VoD content do not qualify as hosting providers, cannot be classified as online platforms under Article 3(i) DSA and do not engage in mere conduit or caching functions.

Consequently, they are not subject to the enhanced obligations imposed on Very Large Online Platforms (VLOPs), including the duty to assess systemic risks, the prohibition on targeted advertising to minors, or the ban on manipulative interface designs (*dark patterns*)[72].

allow or even require playing an active role in creating an environment in which users' communications can be delivered and made accessible".

[71] DSA, Art 3, let. (i): "'online platform' means a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation".

[72] Cf. DSA, Art. 25.

ISSN 2281-5147

This interpretation is confirmed by the *European Audiovisual Observatory*, which notes in *Unravelling the Digital Services Act Package*[73] that the DSA and the DMA[74] apply to video-sharing platforms, but exclude video-on-demand services which are instead subject to the obligations laid down by the Audiovisual Media Services Directive (AVMSD), given their editorial responsibility, a dimension not applicable to intermediary services regulated under the DSA.

Additional clarity can be drawn from the analysis of Terms of Use of platforms[75] in which the section on "User-Generated Content" refers generally to platform's suite of services but not to the video streaming services specifically[76]. While the platform's terms acknowledge the possibility for users to share content such as text, images, audio, or video, these functionalities are not specifically enabled within the streaming environment, which remains a closed, non-interactive space. Importantly, even where user-generated content is permitted across the platform's broader services, it is subject to age restrictions and strict moderation policies aimed at preventing the dissemination of harmful or offensive material[77].

Although VoD platforms fall outside the DSA's formal scope, it would be appropriate for the principles underpinning the DSA- particularly those related to child safety[78], algorithmic transparency, and fairness-by-design - to also extend to closed ecosystems

[73] European Audiovisual Observatory, *Unravelling the Digital Services Act Package,* p. 3, available at https://rm.coe.int/iris-special-2021-01en-dsa-package/1680a43e45.

[74] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

[75] For example Disney: https://disneytermsofuse.com/app/uploads/2020/09/disney_gtou_20160331v2_Italian-TOU.pdf.

[76] See https://disneytermsofuse.com/app/uploads/2020/09/disney_gtou_20160331v2_Italian-TOU.pdf, p. 3 ff.

[77] See the following paragraphs (...) and https://disneytermsofuse.com/app/uploads/2020/09/disney_gtou_20160331v2_Italian-TOU.pdf.

[78] For an overview of references in the DSA to minors and their protection, allow us to refer you to J. Fortuna, *Minors' Digital Vulnerability in the EU and the US: A Comparison Between The Digital Services Act and The Kids Online Safety and Privacy Act*, in *Comparative Law Review*, 2025, p.115 ff. See, also, L. Vizzoni, *I "minori digitali" tra doveri educativi e tutele*, Bari, 2025, p. 78 ff.

ISSN 2281-5147

that provide access for passive and non-interactive viewing of movies and video content, given their pervasive role in shaping young people's relationship with media. Indeed, this regulatory asymmetry reveals a clear gap in the European framework for the protection of minors.

Moreover, it is worth reiterating at this point, building on the considerations set out above, that the DSA remains fully applicable in two important contexts. First, when platforms moderate user-generated content that incorporates or builds upon professionally produced cinematographic material (such as video excerpts from streaming services). Second, when minors themselves take on the role of content creators—sharing their own video content inspired by or related to cinema—on platforms. In both cases, the DSA plays a pivotal role in safeguarding young users who are no longer passive consumers, but active participants in the digital cultural sphere.

6. Child Protection in Streaming Services: A Comparative Analysis of Contractual Frameworks and Platform Architecture.

In this context, the following section turns to the contractual dimension, examining how instruments of private governance – namely, the *Terms of Service* and *User Policies* of major platforms – translate the objectives of public regulation into specific operational duties and practices. This analysis is crucial to determine whether, and to what extent, the obligations arising from the European legal framework are genuinely internalised within the self-regulatory architecture of leading streaming providers, or whether they remain merely declaratory in nature.

From this perspective, a comparative analysis of the child-protection policies adopted by the principal on-demand services becomes particularly significant[79]. The inquiry focuses on the concrete mechanisms through which these platforms implement their duty of care towards underage users-parental-control functionalities, age-based content classification systems, child-oriented interfaces, and other anticipatory design

[79] The analyzed Video-on-Demand (VoD) platforms are Disney+, Amazon Prime Video and Netflix.

ISSN 2281-5147

features that embody, to varying degrees, the principle of *responsible design* promoted by the European digital governance framework.

The contractual architecture of major Video-on-Demand (VoD) streaming platforms demonstrates a progressive, though uneven, process of internalising the child-protection principles advanced by European and international digital-governance regimes. Within their terms of use and ancillary policies, these services have gradually translated public regulatory expectations – such as the *duty of care*, *safety by design*, and *age-appropriate design* – into contractual and technical obligations that articulate both the platform's normative posture and the user's sphere of responsibility.

The examination of these clauses reveals a shared grammar of protection, grounded in the dual premise that (i) the contractual relationship is reserved for adult users who assume legal responsibility for the actions of minors accessing the service, and (ii) that such responsibility must be supported by a suite of technological instruments designed to prevent exposure to age-inappropriate or harmful content.

Across the sector, the terms of service converge in assigning contractual capacity exclusively to adults. Subscription is restricted to individuals aged eighteen or older[80], while minors may access the service only with the consent and under the supervision of a parent or legal guardian. This formulation serves as both a legal and ethical pivot: it delineates the boundaries of contractual liability while shifting the practical burden of protection from the platform to the domestic sphere. The parent becomes a co-regulator, responsible for configuring the digital environment through the tools provided. In this sense, the household is transformed into a micro-site of governance where public objectives of digital safety are reinserted into private contractual relations.

[80] See, for example, the *Prime Video Terms of Use*, which stipulate that users under the age of eighteen may access the service only with the consent and supervision of a parent or legal guardian. Although phrased in general terms, this clause explicitly reaffirms the principle of parental responsibility in the child's use of the platform (see Prime Video Help, "Using Prime Video").

Similarly, pursuant to Article 4.1 of the *Netflix Terms of Use*, subscription to the service is reserved for adult users, defined as individuals aged eighteen or older. Users below the age of majority may access the service only under the direct supervision of an adult. Although succinctly drafted, this provision unequivocally places responsibility for minors' use of the service on parents or legal guardians, thereby delineating a model of self-regulation grounded in the principle of familial oversight.

ISSN 2281-5147

To enable this shared responsibility, all major providers incorporate a multilayered system of technical safeguards that materialise the principle of *safety by design*. Among these, child-dedicated profiles—variously labelled *Kids* or *Junior*—stand out for their simplified and visually distinct interface restricted to age-appropriate content. Within these environments, advertising and purchasing functions are disabled, account-management settings are inaccessible, and search or recommendation algorithms are filtered to exclude unsuitable titles[81]. The underlying design logic is preventive rather than reactive: the protective perimeter is embedded within the interface architecture itself, thereby reducing dependence on parental intervention in each individual viewing act.

A specific weakness, however, emerges from the examination of Prime Video *Terms of Service*: content downloaded through other profiles remains accessible within *Kids* profiles, constituting a potential gap in the platform's protection framework[82].

Complementarily, all services employ age-based rating systems that regulate access to content through graduated thresholds. Although terminology and granularity differ—ranging from 0+, 6+, 9+, 12+, 14+, 16+, to 18+—the underlying rationale remains consistent: to signal degrees of maturity and sensitivity in a transparent and standardised manner[83]. These classifications are either determined internally or

[81] For instance, the *Disney+ Terms of Service* provide that:

"A Subscriber may designate one or more profiles as a Junior Mode profile, which will restrict viewing of certain Content from within that profile. An Extra Member may not set their profile to Junior Mode. […] If you permit anyone else to use, view or access the Disney+ Service and/or the Content using your Disney+ Service account (including via a profile), you acknowledge that some content offered on the Disney+ Service may not be suitable for children or for some viewers and therefore discretion is advised."

(*Disney+* website, *Help Center* — "Parental Controls", *Kids Profiles* section, *Disney+ Subscription Terms and Conditions*[valid for Italy, Greece, San Marino, and Vatican City], Art. 1.3(e) "Junior Mode profiles". Available at: https://help.disneyplus.com/it/article/disneyplus-kids-profiles).

[82] https://www.primevideo.com/help?nodeId=GD6ARQYPV5H7RYA4;

[83] For example, *Disney+* assigns each title an age-based classification determined either by the platform itself or by a relevant local regulatory authority. The classification system encompasses seven levels: content rated 0+ is suitable for all audiences; 6+ indicates that certain scenes may not be appropriate for children under six; 9+ applies to those under nine; 12+ to viewers under

ISSN 2281-5147

aligned with relevant local regulatory authorities, reflecting cultural variations while maintaining structural coherence.

Some platforms reinforce these ratings with content descriptors flagging potentially sensitive elements such as violence, fear, explicit language, sexual references, or depictions of alcohol and drug use. In several cases, the rating assigned to a single title extends to an entire series, simplifying parental control but risking over-inclusive or, conversely, insufficient categorisations. The cumulative effect of these systems is to promote informational transparency and facilitate mindful mediation by parents or caregivers[84].

---

twelve; 14+ to those under fourteen; 16+ to those under sixteen; and 18+ is reserved for adults only, as some scenes may not be suitable for viewers under eighteen.

Disney+ also publishes a content-subjectivity disclaimer, which states:

"Content tends to elicit varying reactions among different people. You may come across Content that you find offensive, indecent, explicit, or objectionable. Also, content ratings, types, genres, categories, and/or descriptions are provided as suggestions to help with navigation and for informational purposes. We do not guarantee that you will agree with them. You acknowledge these risks and your responsibility for making your own choices regarding what Content is appropriate for your family."

(*Disney*+ website — *Rating Limits*, "Content Rating" section, *Disney*+ *Subscription Terms and Conditions*, Art. 1.6(b)).By contrast, *Prime Video* also employs age-based classification criteria, with variations depending on the country of access. Amazon generally adopts the following age categories: Kids, suitable for all audiences; Older Kids, recommended for ages seven and up; Teens, for viewers aged thirteen and older; Young Adults, for viewers aged sixteen and up; and Adults, restricted to viewers aged eighteen and over (Prime Video Help Center).

Likewise, *Netflix* organises its content classifications according to audience age suitability. The "ALL" category designates content recommended for all viewers, while "7+" is suitable for children aged seven and above. The "10+"rating applies to audiences aged ten and older, and "13+" targets teenage viewers, indicating material appropriate for those aged thirteen and above. For older adolescents, the "16+" rating is used, whereas "18+" is reserved for adult audiences, signalling content suitable only for viewers aged eighteen and over (Netflix Help Center).Games available on the platform are also subject to age-based classification, which varies depending on the operating system and device in use. On Android devices, classifications follow the IARC system—ranging from 3+, 7+, 12+, 16+, to 18+. On iOS devices, the Apple App Store ratings apply, with categories of 4+, 9+, 12+, and 17+. On television and via *Netflix.com*, classifications are organised as All, 7+, 10+, 13+, 16+, and 18+ (Netflix Help Center).

[84] See: https://help.netflix.com/en/node/2064; Cf. https://help.disneyplus.com/it/article/disneyplus-content-ratings

ISSN 2281-5147

Another layer of contractual protection is provided through PIN-based access control systems, allowing account holders to set numeric locks to prevent unauthorised entry into adult profiles or alteration of parental settings[85].

Some configurations also require password authentication for the creation or deletion of profiles, thereby closing potential loopholes in account governance. Certain providers go further by introducing exit-protection mechanisms—sometimes labelled *Protected* or *Kid-Proof Exit*—requiring users to complete a simple task or re-enter credentials before leaving the children's environment[86]. This device exemplifies a tangible application of *protection by default*: it prevents minors from intentionally or accidentally exiting the protected space, embedding defensive logic directly within the user experience. Such mechanisms embody the principle of architectural prevention, transforming protection from an external instruction into an intrinsic property of the interface.

The contractual clauses accompanying these technical systems serve to reinforce their normative dimension. Typical formulations stipulate that parents remain responsible for monitoring minors' use of the service and for ensuring that profile configurations and content settings are appropriate to the child's age. These provisions underline the dual approach of the platform: combining legal disclaimers that limit liability with a structured set of design features enabling users to fulfil their duty of care. The tone is declarative yet operational: it recognises the provider's limited capacity to control individual behaviour while offering the technological means to support responsible use.

---

[85] See *Disney+* website — *How to Set a Profile PIN*, section "Setting a Profile PIN" (https://help.disneyplus.com/it/article/disneyplus-it-it-parental-controls); *Prime Video Help Center — Parental Controls* (https://www.primevideo.com/help/ref=atv_hp_nd_nav?nodeId=G26NRYUT8ATMMZRB); and *Netflix Help Center — Parental Controls on Netflix* (https://help.netflix.com/en/node/114277; https://help.netflix.com/en/node/122551).

[86] This functionality is available on *Disney+* but not on *Netflix* or *Prime Video*. See *Disney+* website — *Kid-Proof Exit*, feature description (https://help.disneyplus.com/it/article/disneyplus-it-it-kids-profiles). *Disney+* allows users to enable this feature through the mobile app or a supported web browser. To activate it, users must log in to their profile, select *Edit Profile*, toggle *Protected Exit* to "ON", and enter their password to confirm the change.

ISSN 2281-5147

Another recurrent feature of these contractual frameworks concerns general standards of user conduct, which prohibit the dissemination of defamatory, harassing, obscene, or otherwise harmful content to minors. The scope of such clauses is broad: it typically extends to user-generated content, comments, and uploads, explicitly excluding material that promotes illegal activities or depicts minors in sexualised contexts[87]. While these provisions often serve to shield providers from third-party liability, they also express an ethical orientation consistent with the European Union's broader commitment to the protection of minors in digital media.

Notwithstanding these provisions, the effectiveness of such measures remains intrinsically dependent on the informed and sustained engagement of parents and caregivers, whose role in mediating and supervising children's access to digital media remains indispensable. Some platforms complement behavioural clauses with

[87] For example, the *Terms of Use* applicable to Italy (and to most *Disney* services) set forth behavioural standards under Article 8. Specifically, users agree not to distribute any material that is: (a) defamatory, offensive, harassing, threatening, or invasive of another person's privacy; (b) fanatical, derogatory, racially offensive, or otherwise objectionable; (c) violent, vulgar, obscene, pornographic, or otherwise sexually explicit; or (d) otherwise harmful to individuals or entities.

The prohibition extends to material that is illegal or that incites or promotes illegal activities, or the discussion of illegal activities with the intent to commit them — including content that constitutes or represents an attempt to engage in child pornography, stalking, sexual assault, fraud, trafficking in obscene or stolen materials, drug trafficking and/or abuse, harassment, theft, or criminal conspiracy. Users are further prohibited from distributing material that infringes or violates third-party rights, including: (a) copyright, patent, trademark, trade secret, or other proprietary or contractual rights; (b) the right to privacy (in particular, users must not disclose personal information about others without their express consent) or publicity; or (c) confidentiality obligations.

Additionally, users may not post material relating to commercial or business matters, advertise or offer to sell products, services, or other items (whether for profit or not), or solicit others to do so (including solicitations for contributions or donations). They must not upload content containing viruses or other harmful components, or otherwise interfere with, compromise, or damage the Sites or any connected networks, nor obstruct the use or enjoyment of the Sites by others. Content that is antisocial, harmful, or disruptive — including "flaming," "spamming," "flooding," "trolling," and "griefing," as these terms are commonly used online — is likewise prohibited, as is any material that falls outside the subject matter or theme assigned to a public forum.

The *Terms of Use* further state that users acknowledge and accept the possibility of being exposed to material submitted by various sources, and that *Disney* is not responsible for the accuracy, usefulness, safety, or intellectual property rights of such content. The platform explicitly disclaims liability for user-generated submissions that may be inaccurate or offensive, while acknowledging the residual risk that users may encounter such material despite compliance mechanisms.

ISSN 2281-5147

economic safeguards, disabling purchasing functions within children's profiles or requiring PIN authentication for any transaction. Although primarily aimed at preventing unauthorised spending, these measures also reduce minors' exposure to commercial persuasion and behavioural advertising, aligning contractual design with emerging norms on child-appropriate monetisation. In some cases, advertising availability itself varies by subscription level, with children's profiles exempt from targeted ads regardless of user settings[88].

Comparative evidence further highlights variations in how these protective mechanisms are integrated and prioritised. Certain providers display a preventive and user-centred orientation, embedding child-specific design within the interface architecture and limiting users' ability to alter protective thresholds. Others adopt a more reactive and discretionary model, offering flexible settings whose effectiveness depends largely on informed parental engagement. The depth of integration thus varies: some systems incorporate multi-layer authentication (for example, requiring a password to modify age-rating thresholds), while others rely on user discipline to maintain consistent boundaries across devices.

The comparative analysis of child-protection mechanisms implemented by leading platforms reveals a generally advanced yet structurally uneven level of attention to digital safety and age-appropriate design. Providers have progressively incorporated a baseline of protective functionalities—including dedicated child profiles, age-based classification, parental control settings, access PINs, and content warnings addressing potentially harmful material such as violence, coarse language, or sexual content. This convergence around a shared set of safeguards signals a consolidated awareness of the ethical and regulatory expectation that streaming services should embed child protection not as an ancillary feature but as a structural component of their technological and contractual architecture. In this sense, the platforms analyzed collectively exemplify the gradual internalisation—albeit with differing levels of maturity—of the *safety-by-design* and *fairness-by-design* principles emerging from the European digital acquis.

[88] https://www.primevideo.com/help?nodeId=GD6ARQYPV5H7RYA4; https://www.primevideo.com/help/ref=atv_hp_nd_nav?nodeId=G5VD9FKYCXW8RDK9

ISSN 2281-5147

Yet a closer examination of their respective configurations reveals notable differences in the depth, coherence, and preventive potential of these mechanisms. At this point, it is useful to give examples of specific platforms: Disney+ stands out for the high degree of integration and usability of its parental-control architecture. It is the only provider combining a simplified, child-oriented interface with a *kid-proof exit*—a function designed to prevent both accidental and deliberate navigation outside the protected environment—thus translating the notion of *protection by default* into a tangible design element. This feature reduces reliance on parental intervention and embeds protection directly into the user experience[89]. Netflix, by contrast, adopts a more flexible but also more reactive model: while it offers a simplified interface and a PIN for profile creation—an effective barrier against circumvention—the absence of an exit-protection function leaves monitoring primarily in the hands of parents or guardians[90]. Prime Video, meanwhile, presents a different configuration: although it provides standard parental-control and filtering tools, it lacks both simplified navigation and exit locks, compensating only partially through purchase-block mechanisms oriented more toward economic control than child welfare[91].

These divergences, though technical in appearance, reveal deeper structural and cultural differences in how each platform conceives and operationalises the notion of child protection. Disney+ appears to embody a preventive and user-centred philosophy, embedding safeguards at the architectural level and aiming to shape the child's digital experience within a controlled and pedagogically sensitive environment.

From a policy and governance perspective, this heterogeneity raises complex questions of both regulatory equity and substantive protection. While a core set of safety mechanisms may now be regarded as an industry standard, the quality, coherence, and preventive orientation of these tools vary considerably, resulting in unequal conditions of digital safety and well-being for young users across platforms. This unevenness underscores the need for harmonised standards within the European audiovisual ecosystem—standards capable of ensuring that minimum functionalities

[89] See https://help.disneyplus.com/it/article/disneyplus-kids-profiles#kid-proof.

[90] https://help.netflix.com/en/node/2064.

[91] https://www.primevideo.com/help?nodeId=GD6ARQYPV5H7RYA4; https://www.primevideo.com/help/ref=atv_hp_nd_nav?nodeId=GFGQU3WYEG6FSJFJ

ISSN 2281-5147

are accompanied by mandatory usability thresholds and uniform benchmarks for accessibility, transparency, and age-appropriate design.

Ultimately, comparative evidence suggests that the transition from parental control to child-centred design remains incomplete. A truly effective framework for protecting minors in streaming environments requires not only technical safeguards but also a broader cultural shift in design philosophy—from a reactive logic of user supervision to a proactive ethic of responsibility embedded within the very architecture of digital services.

The comparative evidence also highlights differences in how these protective mechanisms are integrated and prioritised. Some providers display a preventive and user-centred orientation, embedding child-specific design features within the very structure of the interface and limiting users' ability to modify protection thresholds. Others adopt a more reactive and discretionary model, offering flexible settings whose effectiveness depends entirely on the informed engagement of parents or guardians.

7. Parental Control and the Evolving Capacities of the Child: A Rights-Based Approach.

The analysis of the policies adopted by major digital platforms reveals that parental control[92] represents, within today's media ecosystem, one of the most immediate and pervasive forms of safeguarding minors' access to digital content.[93] It constitutes the

[92] The importance of employing parental control tools in the audiovisual sector is also emphasised by the 2018 Directive, which, in Recital 20, provides that: *"The minimum harmonisation approach allows Member States to develop a higher degree of protection for content which may impair the physical, mental or moral development of minors. The most harmful content, which may impair the physical, mental or moral development of minors, but is not necessarily a criminal offence, should be subject to the strictest measures such as encryption and effective parental controls, without prejudice to the adoption of stricter measures by Member States"*. For an overview of parental control and the role of parents in protecting minors from digital vulnerability, see E. Battelli, *Minori e nuove tecnologie*, in E. Battelli (eds.), *Diritto privato delle persone minori di età. Diritti, tutele, nuove vulnerabilità*, Torino, 2021, p. 111 ff.; J. Fortuna, *Il nuovo ruolo dei genitori nella tutela della vulnerabilità digitale dei minori: spunti di comparazione giuridica tra UE, USA, Italia e Australia*, in *Rivista di Diritti Comparati*, 2025, (forthcoming), cit.

[93] Mauk, M. (2021). Think of the Parents: Parental Controls in Digital TV and Family Implications. In: Holloway, D., Willson, M., Murcia, K., Archer, C., Stocco, F. (eds) Young Children's Rights in a Digital World. Children's Well-Being: Indicators and Research, vol 23, pp. 81 – 92.

ISSN 2281-5147

first layer of protection – domestic, personalised, and relational in nature – within that multilayered framework progressively built by European and international law to safeguard children's rights in the digital environment. It is, therefore, a hybrid instrument, both technical and legal, which materialises the interaction between the family sphere and the regulatory sphere. The institution of parental control stands at the crossroads of private autonomy, parental responsibility and the child's freedom, functioning as a locus of synthesis – but also of tension – between the legal duty to protect and the right of the child to progressive self-determination[94]. Technological tools for monitoring, filtering, or restricting content do not merely express parental power but rather give concrete form to a duty of protection and care grounded in Article 18 of the United Nations Convention on the Rights of the Child (CRC)[95] and Article 24 of the Charter of Fundamental Rights of the European Union[96].

However, in both international and European law, the protection of the child increasingly follows the principle of the child's evolving capacities, developed by the UN Committee on the Rights of the Child. According to this principle, every protective measure must be proportionate to the child's maturity and discernment, ensuring that protection does not become an unjustified limitation on freedom of

[94] For a comparative analysis of the relationship between parental responsibility and the child's autonomy in the digital environment, see: S. Rigazio, *L'Empowerment del minore nella dimensione digitale*, Modena, 2024, available in open access at: https://mucchieditore.it/wp-content/uploads/Open-Access/Rigazio-Prospettive-8-DEF-OA.pdf.

[95] Article 18: "1. States Parties shall use their best efforts to ensure recognition of the principle that both parents have common responsibilities for the upbringing and development of the child. Parents or, as the case may be, legal guardians, have the primary responsibility for the upbringing and development of the child. The best interests of the child will be their basic concern. 2. For the purpose of guaranteeing and promoting the rights set forth in the present Convention, States Parties shall render appropriate assistance to parents and legal guardians in the performance of their child-rearing responsibilities and shall ensure the development of institutions, facilities and services for the care of children. 3. States Parties shall take all appropriate measures to ensure that children of working parents have the right to benefit from child-care services and facilities for which they are eligible".

[96] Charter of Fundamental Rights of the European Union, Article 24 — *The rights of the child*: "1. Children shall have the right to such protection and care as is necessary for their well-being. They may express their views freely. Such views shall be taken into consideration on matters which concern them in accordance with their age and maturity. 2. In all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration. 3. Every child shall have the right to maintain on a regular basis a personal relationship and direct contact with both his or her parents, unless that is contrary to his or her interests".

ISSN 2281-5147

expression, cultural participation, or autonomous learning[97]. In light of this principle, in our view, parental control should adopt a *default-protective* design: that is, ensuring a high level of automatic protection during the early stages of the child's digital experience, while allowing for a gradual modulation of parental intervention proportionate to the child's cognitive and experiential development. This approach, now consolidated within European law, aims to avoid paternalistic drifts and instead to foster an educational and participatory accompaniment, strengthening the digital awareness and responsibility of the growing individual.

From this perspective, parental control assumes a dual function: *preventive*, insofar as it seeks to avert exposure to harmful or inappropriate content; and *promotional*, insofar as it encourages the conscious and informed exercise of freedom of information and expression online. Its effectiveness, however, remains constrained by two structural factors: on the one hand, the opacity of design choices made by platforms — from persuasive interfaces to recommendation systems driven by predictive and profit-oriented engagement models; on the other, the informational and cognitive

[97] See Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment*, Section IV – *Evolving capacities*, paras. 19–21: "19. States parties should respect the evolving capacities of the child as an enabling principle that addresses the process of their gradual acquisition of competencies, understanding and agency. That process has particular significance in the digital environment, where children can engage more independently from supervision by parents and caregivers. The risks and opportunities associated with children's engagement in the digital environment change depending on their age and stage of development. They should be guided by those considerations whenever they are designing measures to protect children in, or facilitate their access to, that environment. The design of age-appropriate measures should be informed by the best and most up-to-date research available, from a range of disciplines. 20. States parties should take into account the changing position of children and their agency in the modern world, children's competence and understanding, which develop unevenly across areas of skill and activity, and the diverse nature of the risks involved. Those considerations must be balanced with the importance of exercising their rights in supported environments and the range of individual experiences and circumstances. States parties should ensure that digital service providers offer services that are appropriate for children's evolving capacities. 21. In accordance with States' duty to render appropriate assistance to parents and caregivers in the performance of their child-rearing responsibilities, States parties should promote awareness among parents and caregivers of the need to respect children's evolving autonomy, capacities and privacy. They should support parents and caregivers in acquiring digital literacy and awareness of the risks to children in order to help them to assist children in the realization of their rights, including to protection, in relation to the digital environment". For a comment: C. Djeffal, *Children's Rights by Design and Internet Governance: Revisiting General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*, cit., pp. 11 ff.

ISSN 2281-5147

asymmetry separating digital service providers from end-users, which often deprives parents of the tools and skills required to configure security settings properly[98].

Platforms provide age-rating filters, access PINs, viewing limits, or "junior" profiles; yet these functions are rarely activated by default and even less frequently accompanied by clear explanations of content-classification criteria or recommendation-algorithm logics. This lack of transparency significantly reduces parents' capacity to exercise effective control and, by reflection, undermines their legal ability to fulfil their protective duties. In practice, platforms delineate the normative boundaries—age restrictions, behavioural prohibitions, and user responsibilities—while users operationalise them through configuration and supervision. This hybrid architecture effectively delegates regulatory functions to end-users under the banner of informed consent and digital literacy. However, it also exposes a critical vulnerability: the level of protection ultimately depends on the parent's awareness, motivation, and technical competence. In this light, the contractual allocation of responsibility can be read as a form of responsibility transfer, whereby the provider's duty of care is discharged through disclosure rather than through substantive oversight.

It is therefore essential to support parents not only through technological tools, but also through education and awareness raising[99].

To ensure that parental controls are meaningful and child-centred, platforms should: default to protected child profiles with an opt-out rather than opt-in model; provide clear, accessible, and age-appropriate interfaces, including visual cues and plain-language prompts; publish transparent age-classification criteria and offer insights into the factors that drive personalised recommendations; enable granular filtering—age brackets, thematic categories, explicit-content flags—and allow parents to lock or disable autoplay; integrate monitoring dashboards (usage time, viewing history, flagging of sensitive content) and easy-to-use reporting tools; facilitate

[98] See parr. *above*.

[99] S. P. Hammond, G. Polizzi, C. Duddy, Y. Bennett-Grant, K. Bartholomew, *Children's, parents' and educators' understandings and experiences of digital resilience: A systematic review and meta-ethnography*, cit., pp. 3018 – 3042.

ISSN 2281-5147

co-viewing and dialogue, e.g. shared watch-lists, content summaries, and parental guidance notes that prompt discussion.

Parental controls should be seen not as a substitute for parental engagement[100], but as an enabler of it. Children benefit most when technical protections are coupled with active co-viewing, critical discussion, and clear household norms. Promoting a critical approach to digital media, from shared viewing practices to open discussions about online content, can improve children's ability to navigate the digital landscape with autonomy and awareness.

In the absence of such a multilayered intervention, the transition from parental control to child-centred design remains incomplete. Genuine compliance with the spirit of *safety-by-design* requires not merely the availability of protective options, but their default activation and consistent usability across contexts. As long as protection depends on voluntary configuration and on a variable level of digital literacy, the actual degree of safety afforded to minors will continue to fluctuate. Achieving a coherent standard of digital well-being therefore demands not only contractual harmonisation, but also the establishment of minimum effectiveness thresholds—parameters ensuring that protective tools are accessible, intuitive, and resistant to circumvention.

Ultimately, protecting children in the digital media environment requires a systemic approach that goes beyond the parental responsibility.

As previously discussed, a significant regulatory asymmetry nonetheless persists: *video-on-demand* services fall outside the DSA's stricter framework, unlike interactive platforms like the social ones. This distinction — based on the structural difference between catalogue-based and intermediary services — raises issues of regulatory equity and systemic coherence, making it desirable to extend to streaming services the same obligation to conduct periodic risk assessments regarding minors, thereby ensuring a uniform level of protection.

[100] For an in-depth discussion of the educational role of parents within contemporary parent-child relationships, see G. Di Rosa, *I termini giuridici della funzione educativa nell'attuale quadro delle relazioni tra genitori e figli*, in *Actualidad Jurídica Iberoamericana*, No. 17 bis, 2022, pp. 806 ff.

ISSN 2281-5147

In this light, the rationale of the DSA delineates a multilayered *duty of care* model, in which child protection becomes an integral part of the technical and organisational architectures of digital service providers[101]. Yet the mere availability of parental-control tools does not necessarily correspond to their actual accessibility or comprehensibility. The protection of minors cannot, therefore, rely solely on isolated family autonomy or on the exclusive responsibility of platforms: it requires an integrated form of governance capable of overcoming the dichotomy between the private and the technological spheres, while recognising the child as a rights-holder in his or her own right, with progressively evolving entitlements.

Parents must be able to exercise their educational role through tools that are clear, proportionate and adaptable; service providers must ensure transparent and non-manipulative interfaces, in compliance with Articles 25 and 28 DSA; and States must promote digital literacy and oversight mechanisms ensuring the effectiveness of protection. Minors themselves should be enabled to participate in the formulation of policies that affect them. What thus emerges is a model of shared responsibility, founded on the recognition of the child not as a passive object of protection but as an active holder of fundamental rights — including cultural participation, freedom of expression and digital self-determination. In this perspective, parental control is not a restrictive barrier but a form of guided *empowerment*: a family-based regulatory instrument that complements — rather than replaces — public and technological safeguards. Only a dynamic equilibrium, grounded in continuous dialogue among parents, minors, platforms and institutions, can translate the principle of the best interests of the child into an effective system of protection and empowerment in the digital era, where freedom and safety do not stand in opposition but converge within a unified vision of digital childhood citizenship.

A coordinated effort is needed between regulators, the media and technology industries, civil society and educational institutions to establish shared standards, promote digital-media literacy and encourage design models that respect children not

[101] See, among others, C. Nyamutata, *Childhood in the digital age: a socio-cultural and legal analysis of the UK's proposed virtual legal duty of care*, in *International Journal of Law and Information Technology*, Volume 27, Issue 4, 2019, Pages 311–338; C. Ullrich, *Standards for Duty of Care: Debating Intermediary Liability from a Sectoral Perspective*, in *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, 8(2017), pp. 111 ff.; L. Woods, W. Perrin, *Obliging Platforms to accept a duty of care*, in *Regulating Big Tech*, M. Moore and D. Tambini (eds.), pp. 93 ff.

ISSN 2281-5147

only as users, but as rights holders and participants in cultural life. Only by combining these levers can we ensure that children are respected not merely as consumers, but as rights-holders and cultural participants.

7.1. Some Comparative Insights on the Role of Parental Controls in Safeguarding Children Online: UK and Australia.

A central lesson emerging from regulatory experiences beyond Europe is that parental controls can play a valuable role in protecting children online, yet their use must be carefully balanced with children's rights and evolving capacities.

A notable example is the United Kingdom's Age-Appropriate Design Code (the *Children's Code*), issued by the Information Commissioner's Office in 2020[102]. The Code establishes a set of design standards for services "likely to be accessed by children," including apps, social networks and, importantly for the present analysis, content-streaming platforms[103]. Anchored in the principle of the child's best interests, the Code places a positive duty on service providers to give primacy to children's rights over purely commercial considerations[104].

Standard 11 specifically addresses parental controls, requiring providers not only to explain such tools in an age-appropriate manner but also to clearly notify children

[102] See: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/.

[103] For a detailed comparative discussion of the UK Age-Appropriate Design Code and its relevance as a potential regulatory benchmark beyond the British context, see S. Rigazio, *L'Empowerment del minore nella dimensione digitale*, Modena, 2024, open access: https://mucchieditore.it/wp-content/uploads/Open-Access/Rigazio-Prospettive-8-DEF-OA.pdf.

[104] See standard 1: The best interests of the child should be a primary consideration when you design and develop online services likely to be accessed by a child" (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/code-standards/.)

ISSN 2281-5147

whenever monitoring systems are active[105]. This standard reflects a broader approach emphasising that parental controls should assist – but not replace – responsible platform design and should not serve as a means to shift accountability for children's safety solely onto families[106].

As highlighted in the impact assessment on the Children's Code, expanding parental controls without adequate transparency risks undermining children's autonomy and moving platforms out of compliance. Moreover, it may place undue pressure on parents or strain parent-child relationships, while diverting attention from necessary structural safeguards within the platforms themselves. In this sense, parental controls must operate within a multilayered responsibility framework, aligning with children's developmental stage and their right to be informed and heard, rather than becoming a mechanism of disproportionate surveillance or a substitute for robust platform governance[107].

In contrast, the Australian approach has aimed to exclude minors from accessing platforms, thereby diminishing the role of parents in the educational function within the digital environment through the Online Safety Amendment (Social Media

[105] Standard 11: "If you provide parental controls, give the child age appropriate information about this. If your online service allows a parent or carer to monitor their child's online activity or track their location, provide an obvious sign to the child when they are being monitored" (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/code-standards/.).

[106] See S. Rigazio, *L'Empowerment del minore nella dimensione digitale*, cit., pp. 138 ff.. Reference may also be made to N. Patti, V. Punzo, R. Romano, *Child Vulnerabilities in the Digital Environment: Comparative Insights and Operational Guidelines*, cit., pp. 12 ff.

[107] J. Mootz, K. Blocker, et al., *UK Age-Appropriate Design Code: Impact Assessment*. Report by the Institute for Digital Media and Child Development / Children & Screens, 2024. Available at: https://www.childrenandscreens.org/wp-content/uploads/2024/03/Children-and-Screens-UK-AADC-Impact-Assessment.pdf.

ISSN 2281-5147

Minimum Age) Bill 2024[108]. In fact, Australia has approved this legislation[109], which deals with the online safety of minors, setting a minimum age for accessing social media and assigning platforms responsibility for the safety of their users[110].

In particular, Parliament approved new rules setting the age of 16 for access to social media platforms[111], imposing a series of obligations on service providers[112]. Platforms are therefore required to introduce verifiable systems and processes to ensure that people below the minimum age cannot create and/or hold a social media account[113].

---

[108] For an overview of the new Australian legislation on online safety for minors (Online Safety Amendment (Social Media Minimum Age) Bill 2024) be allowed to refer to J. Fortuna, *Il nuovo ruolo dei genitori nella tutela della vulnerabilità digitale dei minori: spunti di comparazione giuridica tra UE, USA, Italia e Australia*, in *Rivista di Diritti Comparati*, 2025, (forthcoming), cit.

[109] However, the effects of the application will be postponed by 12 months: Online Safety Amendment (Social Media Minimum Age) Bill 2024, Section 63E, Delayed effect of requirement to take reasonable steps to prevent age-restricted users having accounts (1): "Section 63D takes effect on a day specified in an instrument under subsection (2) of this section. (2) The Minister may, by notifiable instrument, specify a day for the 26 purposes of subsection (1). (3) The specified day must not be later than 12 months after the day this section commences […]".

[110] Online Safety Amendment (Social Media Minimum Age) Bill 2024, Explanatory Memorandum, p. 1. For some insights into the new Australian legislation, see T. Flew, T. Koskie, A. Stepnik, *Digital Policy as Problem Space: Policy Formation, Public Opinion, and Australia's Online Safety Amendment (Social Media Minimum Age) Act 2024*, 2025, available at *SSRN*: https://ssrn.com/abstract=5310865 or http://dx.doi.org/10.2139/ssrn.5310865.

[111] Online Safety Amendment (Social Media Minimum Age) Bill 2024, Part 1, Sec. 1 provides for the addition of the following wording to Section 4 of the Online Safety Act 2021: "There are age restrictions for certain social media platforms. A provider of such a platform must take reasonable steps to prevent children who have not reached a minimum age from having accounts". Section 2 specifies that "age-restricted user means an Australian child who has not reached 16 years".

[112] Online Safety Amendment (Social Media Minimum Age) Bill 2024, Part 4A, Social media minimum age; Division 1, Introduction; 63A Simplified outline of this Part: "Providers of certain kinds of social media platforms must take reasonable steps to prevent children who have not reached a minimum age from having accounts. This requirement takes effect on a day specified by the Minister. There are privacy protections for information collected by social media platforms for the purposes of the minimum age requirement".

[113] In addition, Section 5 of the Online Safety Amendment (Social Media Minimum Age) Bill 2024, states that: "to formulate, in writing, guidelines for the taking of reasonable steps to prevent age-restricted users having accounts with age-restricted social media platforms".

ISSN 2281-5147

Social media platforms are also required to demonstrate that they have identified appropriate and reasonable measures to prevent harm to minors, and must prove that they have introduced effective systems and processes to prevent individuals under the age of 16 from creating personal accounts, with penalties imposed in the event of any violations found[114].

What emerges from an analysis of the legislation relating to the role of parents is that Australia has decided to relieve parents of responsibility for assessing their children's online activities, while highlighting the role of platforms in protecting minors. This is based on the awareness that even for those who exercise parental responsibility, it is difficult to assess the dangers of the digital ecosystem, or in any case the consequences of any online activity by their children[115].

It is no coincidence that the Explanatory Memorandum to the Online Safety Amendment Bill 2024 states that: "Parents and carers feel unsupported to make evidence-based choices about when their children should be on social media and many are overwhelmed by pressure from their children and other families […]. Setting a minimum age removes ambiguity about when the 'right' time is for their children to engage on social media and establishes a new social norm"[116].

---

[114] Cf. https://www.agendadigitale.eu/cultura-digitale/un-futuro-senza-social-per-i-minori-laustralia-apre-la-strada-le-mosse-dellitalia/. See Online Safety Amendment (Social Media Minimum Age) Bill 2024, Division 2, Civil penalty, 63D, Civil penalty for failing to take reasonable steps to prevent age-restricted users having accounts: "A provider of an age-restricted social media platform must take reasonable steps to prevent age-restricted users having accounts with the age-restricted social media platform".

[115] On the role of private law as a fundamental ally in the educational task of parents in the digital age, see R. Senigaglia, *Il dovere di educare i figli nell'era digitale*, in *Persona e mercato*, 2021, p. 511 ff. and in part. p. 525.

[116] Online Safety Amendment (Social Media Minimum Age) Bill 2024, Explanatory Memorandum, p.2. Let us also refer to J. Fortuna, *Il nuovo ruolo dei genitori nella tutela della vulnerabilità digitale dei minori: spunti di comparazione giuridica tra UE, USA, Italia e Australia*, in *Rivista di Diritti Comparati*, 2025, (forthcoming), cit.

ISSN 2281-5147

8. Conclusive Remarks.

Building on the foregoing considerations, it emerges how digitalization has profoundly reshaped the ways in which young audiences' access, engage with, and attribute meaning to cinematic experiences. Traditional theatre-based viewing has been increasingly supplanted by domestic, individual, and mobile modes of consumption, facilitated by streaming services and by the circulation of audiovisual content across social media platforms. Within this evolving ecosystem, the cinematic experience becomes intertwined with the digital one, redefining the boundaries between artistic expression, entertainment, and algorithmically mediated consumption.

This transformation entails substantial cultural and legal ramifications. Indeed, within this framework, particular significance is attributed to Article 31 of the United Nations Convention on the Rights of the Child, which acknowledges every child's right to full participation in cultural and artistic life. A similar principle is echoed in the European Union's commitment to fostering cultural diversity and ensuring equitable access to creative content, as enshrined in Article 22 of the Charter of Fundamental Rights of the EU. Nonetheless, the dynamics of film consumption in the digital environment prompt critical reflection on the actual capacity of streaming platforms to safeguard pluralistic access and to nurture aesthetic development—particularly with regard to independent or culturally non-standardized productions.

Digital platforms structure their offerings through algorithmic recommendation systems that, while enabling personalization of the user experience, tend to prioritize mass-market content, leading to phenomena of cultural homogenization and selective visibility. In this scenario, minors risk being exposed to increasingly filtered and standardized content, with a significant impact on their cultural literacy and their ability to explore narratives outside the dominant mainstream.

Furthermore, the main streaming platforms are aware that viewing is becoming a transmedia experience, often mediated by viral dynamics and the engagement logic typical of social networks.

Historically, cinema functioned not only as an artistic medium but also as a public arena for collective dialogue and participation, where shared viewing experiences

ISSN 2281-5147

encouraged reflection, debate, and cultural consolidation. In contemporary contexts, this dialogic role has been partially transferred to social media environments, where cinematic works (or their fragmented excerpts) are discussed, reinterpreted, and amplified. On the one hand, such spaces enable broader, more cross-cutting, and participatory forms of engagement; on the other, the inherently ephemeral, fragmented, and performative character of online interactions tends to diminish the depth of critical discourse, favouring short-form content, instantaneous reactions, and engagement-oriented dynamics. This transformation is far from neutral, because it reshapes not only modes of consumption but also the very quality and depth of cultural participation.

From a regulatory perspective, this scenario calls for strengthened guarantees of safe, transparent, and culturally meaningful access to content intended for minors.

In summary, the cinematic experience in the digital era represents an ambivalent frontier: on one hand, it offers extraordinary opportunities for access, creativity, and participation; on the other, it exposes minors to potentially passive, homogenizing, and market-driven forms of viewing. In this context, public policies and regulatory models—including cooperation among institutions, platforms, and schools—must address not only the protection of young users, but also the active promotion of their right to culture, as recognized in Article 31 of the aforementioned UN Convention, in its fullest sense. Within the contemporary digital ecosystem, profiling practices and targeted advertising constitute some of the most pervasive and opaque challenges to the protection of children's rights. The systematic collection of behavioural data, the construction of psychometric profiles, and the deployment of predictive algorithms aimed at shaping consumption patterns compromise not only minors' right to privacy but also their cognitive, emotional, and ethical development.

The European regulatory framework has progressively introduced strict safeguards to address these risks. The GDPR sets clear boundaries through its prohibition on automated decision-making producing legal or similarly significant effects (Art. 22) and its call for heightened protections when processing the data of children (Recital 38).

The DSA further strengthens this framework by explicitly banning targeted advertising based on profiling when it concerns minors (Art. 28). However, this prohibition applies only to services that qualify as online platforms under the DSA.

ISSN 2281-5147

As a result, video-on-demand services, which do not host user-generated content or facilitate user interaction, are not subject to Article 28 DSA. In contrast, social platforms which allow content sharing and interaction, are fully bound by this provision.

Notwithstanding significant regulatory progress, profiling practices continue to be widespread in reality. Children are often exposed, often without realizing it, to behavioral tracking, algorithmic personalization, and data aggregation across multiple platforms, processes that remain largely opaque and difficult for younger users to understand. Such mechanisms exploit minors' developmental susceptibilities, subjecting them to commercial pressures and subtly shaping their patterns of digital behaviour.

To address these risks and ensure that children's rights are adequately protected, a combination of regulatory and design-oriented interventions is needed. First, platforms should adopt default settings that ensure a high level of privacy, ensuring that profiling and behavioral tracking are automatically disabled for underage users. Any activation of such features should require explicit and informed parental consent. Equally important is the principle of age-appropriate transparency: digital interfaces and privacy notices must be designed to reflect the cognitive development of minors. This involves the use of clear and accessible language, visual symbols, and layered explanations that make data practices understandable even to younger audiences. In addition, dark patterns, i.e., interface designs that manipulate, pressure, or deceive children into sharing personal data or accepting personalized advertising, should be explicitly prohibited under Article 25 of the Digital Services Act. Particular attention should be paid to exploitative design techniques such as autoplay features, fake countdowns, or misleading consent buttons. In addition, platforms should provide non-personalized recommendation modes, allowing minors to access and explore cultural content without being subject to behavioral profiling or commercial targeting. Finally, independent control and oversight mechanisms are essential. Public institutions and regulatory bodies must be equipped with the necessary authority and resources to assess the functioning of algorithms, identify harmful or discriminatory practices, and ensure compliance with the rules in the best interests of the child.

In the end, protecting children from profiling and targeted advertising needs a big shift from consent-based protection models to preventive ones. Children's rights

ISSN 2281-5147

should be built into the system through regulatory frameworks based on built-in fairness and privacy by default that limit data exploitation and help children develop autonomy. Moreover, advertising (particularly within hybrid entertainment contexts) ought to be governed not solely as a commercial activity but as a significant vector of influence, necessitating the adoption of clear, proportionate, and enforceable safeguards in all situations involving children.

To operationalise these findings and ensure that children's cinematic experience in the digital environment aligns with international and EU commitments, a coherent set of legal and policy measures emerges from this analysis.

First, streaming services should be required to adopt privacy- and safety-by-design models, ensuring default child-appropriate settings, clear user-interfaces, and transparent content-curation practices. Second, platform accountability must be strengthened through mandatory risk-assessments relating to minors, expanded auditing obligations, and the introduction of independent oversight mechanisms able to scrutinise algorithmic recommendation systems and advertising models. Third, a gradual alignment between the AVMSD and the DSA should be pursued, extending key duties—such as the prohibition of profiling and dark patterns for minors—to VoD streaming services, thereby remedying the current regulatory asymmetry. Complementarily, standards for child-specific interfaces and parental tools should be harmonised at EU level, including mandatory child profiles, exit-protection functions, and granular content controls that respect children's evolving capacities. Finally, policy efforts should prioritise media-literacy programmes and participatory governance structures, empowering children, parents, and educators to actively contribute to shaping safer, fairer, and more culturally diverse digital environments.

Taken together, these measures reinforce a multilayered model of protection and empowerment, where platform design, regulatory oversight, and educational initiatives work in concert to safeguard minors' rights while fostering their active participation in cultural life.

ISSN 2281-5147

ISSN 2281-5147

EU DATA PROTECTION LIABILITY: THE EXEMPTION CLAUSE EX ART. 82 GDPR UNDER THE EUROPEAN COURT OF JUSTICE INTERPRETATION AND THE LIMITS OF HARMONISATION

Andrea Blatti*

Abstract

This research examines the case-law of the Court of Justice of the European Union (CJEU) on the liability regime for unlawful data processing under the General Data Protection Regulation (GDPR). In particular, it focuses on the exemption clause provided for in art. 82(3) GDPR. Starting with judgment C-300/21, the CJEU has interpreted the terms and concepts contained in art. 82 GDPR as autonomous concepts of European Union law. This attempt at harmonisation is one of the few in the field of civil liability, which has traditionally been left to the competence of EU Member States. However, the GDPR does not provide all the elements necessary to establish the liability of data controllers. Building on this gap, this research explores the appropriate methodology to support the harmonisation process initiated by the GDPR, namely comparative law, and examines the doctrines of private law relevant to the attribution of civil liability in the realm of data protection.

Table of Contents

* PhD student in Law at Sant'Anna School of Advanced Studies, andrea.blatti@santannapisa.it.
Double blind peer reviewed contribution.

ISSN 2281-5147

Keywords

Privacy liability – 82 GDPR – Tort Harmonisation – Tort Law – CJEU GDPR

1. Reasons and objectives of the research

This research originates from the uncertainty within legal scholarship regarding the nature of the exempting proof provided for by the art. 82(3) of the General Data Protection Regulation[1] (GDPR, or Regulation), and from the intention to contribute to clarifying this issue.

In this matter, the most important recent case law of the Court of Justice of the European Union (CJEU, or the Court) has, since its first 2023 decision[2], interpreted

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[2] C-300/21, *UI* v. *Österreichische Post*, Judgment of the Court (Third Chamber) of 4 May 2023, EU:C:2023:370. Commented by F. Episcopo, *UI v. Österreichische Post – A first brick in the wall for a European interpretation of art. 82 GDPR*, in Journal of European Consumer and Market Law, 13(2)/2024; S. Li, *Compensation for non-material damage under Article 82 GDPR: a review of case C-300/21*, in Maastricht Journal of European and Comparative Law, 30(3)/2023; M.J.S. Moròn, *Reflexiones en*

ISSN 2281-5147

several crucial aspects of art. 82 GDPR. Indeed, the CJEU's case-law constitutes the primary forum in which Union law is interpreted and applied, and, in this analysis, it provides a good opportunity to discuss the main doctrinal positions related to the exempting proof in the GDPR.

As will be shown, the CJEU has sought to ensure a harmonised interpretation of those GDPR provisions that do not expressly refer to the law of the Member States.

This paper, by commenting on such case-law, aims to offer suggestions for the interpretation of the exempting proof under art. 82(3) GDPR in a way that facilitates this process of harmonisation.

In particular, this research addresses the lack of consistency and coordination across the various judgments, particularly the reasoning the Court adopted to justify the choice of a fault-based liability system.

To offer a comprehensive overview, the study will reconstruct in advance the doctrinal discussion in which the CJEU's decisions have intervened.

After that, the main elements of art. 82 GDPR will be examined through a chronological analysis of the Court's decisions, complemented, where appropriate, by the opinions of the Advocates General[3].

The paper is structured as follows: paragraph 2 describes the methodology applied to conduct the research, justifying why the comparative method could be a useful tool for harmonising liability in data protection; to this end, it will examine in more detail how the EU has approached private law harmonisation to date. Paragraph 3, on the

torno a la jurisprudencia del TJUE sobre la acción indemnizatoria del art. 82 RGPD (asuntos C-300/21; C-340/21; C-456/22; C-667/21; C-687/21; C-741/21), in Cuadernos de Derecho Transnacional, 16(2)/2024; M.C. Vergès, *El concepto autònomo de responsabilidad civil en el àmbito de la protecciòn de datos personales en la era digital: anàlisis del artìculo 82 del regolamento 2016/679*, in Revista de Derecho Comunitario Europeo, 79/2024; M. Federico, *"La tempesta perfetta": ultime dalla Corte di Lussemburgo su danno (non patrimoniale) da illecito trattamento dei dati personali e possibili risvolti in tema di tutela collettiva*, in Il foro italiano, 148(6)/2023.

[3] It must be advanced that the AG's opinions are not binding, meaning that their importance is measurable only in terms of persuasiveness; secondly, the answers provided therein are significantly limited by the referred questions. On the relationship between the opinions of the Advocate General and Court's decisions see D. Chalmers, G. Davies, G. Monti, *European Union Law*, Cambridge University Press, 2019, 162.

ISSN 2281-5147

other hand, will be divided into four smaller sections: section 3.1 describes the general context, taking into account the general doctrine of civil liability and its applications in the field of data protection; section 3.2 focuses on the breach of the GDPR, required as a necessary element for compensation; section 3.3 explores the causal link between the breach and the damage; finally, section 3.4 examines the various decisions of the CJEU on the subject. These decisions will be commented on individually using the methodology described in paragraph 2.

The final paragraph will summarise the research results, discussing both the CJEU case law and the feasibility of the proposal. The following judgments will be analysed in chronological order, in order to take into account the evolution of the Court's reasoning: C-340/21[4], C-667/21[5], C-687/21[6], C-741/21[7], joint cases C-182/22 and C-189/22[8], and C-200/23[9].

---

[4] C-340/21, *VB* v. *Natsionalna agentsia za prihodite,* Judgment of the Court (Third Chamber) of 14 December 2023, EU:C:2023:986; commented by G.M. Riccio, *Danni non patrimoniali per violazione dei dati personali: verso un'alluvione giudiziaria? (Nota a Corte giust. 14 dicembre 2023, causa C-340/21)*, in Il foro italiano, 149(2)/2024; S. Nusselder, *Security measures in the GDPR & the NAP judgement (340/21)*, in Tilburg Institute for Law, Technology, and Society (TILT), 2024; F. Castagnari, *On the responsibility of the Financial Administration as "data controller" in the event of a data breach due to a "hacker attack" by third parties: critical and systematic profiles*, in Rivista telematica di diritto tributario, 2/2024.

[5] C-667/21, *ZQ v Medizinischer Dienst der Krankenversicherung Nordrhein, Körperschaft des öffentlichen Rechts,* Judgment of the Court (Third Chamber) of 21 December 2023, EU:C:2023:1022; commented by M. Buzzoni, *One, Two, Three… Fault? CJEU Rules on Civil Liability Requirements under the GDPR*, in Conflict of laws, 2024; M. Tzanou et al., *Overview 2023: Case Law of the CJEU and the ECtHR, Country Reports and Books of the Year*, in European data protection law review, 1/2024.

[6] C-687/21, *BL v MediaMarktSaturn Hagen-Iserlohn GmbH,* Judgment of the Court (Third Chamber) of 25 January 2024, EU:C:2024:72; commented by L. Tomasso, *Chronique droit de l'internet - Protection des données personnelles, dommage moral (CJUE, 3e ch., 25 janv. 2024, aff. C-687/21 et autres)*, in La Semaine juridique. Entreprise et affaires, 2024; F. Marchadier, *Précisions sur le régime européen de responsabilité pour traitement illicite de données à caractère personnel*, in RTDCiv. Revue trimestrielle de droit civil, 2024.

[7] C-741/21, *GP v juris GmbH*, Judgment of the Court (Third Chamber) of 11 April 2024, EU:C:2024:288; commented by C. Piltz, I. Kukin, *Schadenersatz bei Verstößen gegen die DSGVO*, in Daten und Sicherheit, 9/2024; P.A. de Miguel Asensio, *Determinación de la indemnización por daños derivados de infracciones del Reglamento General de Protección de Datos*, in La Ley Uniòn Europea, 125/2024.

[8] Joint cases C-182/22 and C-189/22, *JU and SO v Scalable Capital GmbH*, Judgment of the Court (Third Chamber) of 20 June 2024, EU:C:2024:531; commented by T. Petri, *Aus der Rechtsprechung zur DSGVO in den Jahren 2023 – 2024 (Teil 2)*, in Datenschutz und Datensicherheit - DuD, 49/2025; N. Jääskinen, *Robo de datos personales registrados en una aplicación de negociación con valores*, in La Ley Unión Europea, 129/2024.

[9] C-200/23, *Agentsia po vpisvaniyata v OL*, Judgment of the Court (Third Chamber) of 4 October 2024, EU:C:2024:827; commented by D.P.P. Dias, *Aplicabilidade do direito ao apagamento face à publicidade obrigatoria ds*

ISSN 2281-5147

2. Method

This paragraph outlines the legal methodology adopted to offer suggestions for the interpretation of the exempting proof under art. 82(3) GDPR to facilitate the harmonisation process conducted by the Court. It explains why comparative law may represent an appropriate methodology and how it could contribute to this objective.

The European Legislature, through the GDPR, aimed to harmonise the data protection regulatory framework across EU Member States. Furthermore, with a single provision, namely art. 82 GDPR, it attempted to harmonise the entire liability regime for unlawful data processing. This harmonisation objective is unique for two reasons: (i) traditionally, the legal instrument used by EU institutions to harmonise civil law is the directive, as liability is generally left to the discretion of Member States[10]; (ii) the harmonisation of the liability regime is achieved through a single provision, whereas in other cases the liability framework has been defined through entire laws[11].

In addition to the fact that the European Commission has chosen to implement a regulation, which is directly binding and prevails over conflicting national rules, it should be noted that the CJEU has denied the possibility of interpreting the provisions of the GDPR on the basis of national legal traditions, as long as those rules do not explicitly refer to national legal frameworks.

Therefore, both the Regulation's instrument and the CJEU's interpretative approach led to the conclusion that the provisions of the GDPR can be interpreted solely based on the Regulation's text, to ensure harmonisation between Member States.

This harmonisation process, compared with previous civil-law harmonisation efforts, is remarkable for several reasons.

---

registos publicos das sociedades, in Revista do servico de apoio jurìdico, 1(2)/2025; A. Lecourt, *Droit du numérique vs droit des sociétés: nouvelles précisions autour des données personnelles inscrites au registre du commerce et des sociétés*, in Revue trimestrielle de droit commercial et de droit économique, 2024.

[10] For an overview of the EU directives addressing civil liability see M. Bussani, M. Infantino, *Harmonization of Tort law in Europe*, in *Encyclopedia of law and economics*, A. Marciano, G.B. Ramello (edited by), Springer, 2019, 1033-1034.

[11] See for example the new product liability directive (Directive EU 2024/2853).

ISSN 2281-5147

Firstly, according to the EU treaties, the Union institutions do not have the power to intervene in the field of civil law, which has traditionally been left to the Member States[12]. However, over time, they have acquired new powers through the adoption of directives aimed at harmonising those segments of tort law considered to cross national borders and/or affect the development of the internal market[13]. This trend began in the 1970s with the Directive on civil liability insurance[14], and continued with several attempts to harmonise private law[15]. However, these initiatives have never interfered with the general architecture of substantive tort law; instead, they have only shaped particular civil torts[16]. Even today, the harmonisation of civil law is very limited and is primarily based on national law[17].

In this regard, it has been pointed out that the instruments most frequently used by the EU institutions for harmonisation purposes are directives, which, owing to their flexibility, have allowed Member States to apply their own legal categories, thereby intensifying differences rather than promoting uniformity[18]. As regards regulations, there are only a few examples, such as EU Regulation 864/2007 on the law applicable

[12] M. Bussani, M. Infantino, *Harmonization of Tort law in Europe*, in *Encyclopedia of law and economics*, cit., 1033.

[13] M. Bussani, M. Infantino, *Harmonization of Tort law in Europe*, in *Encyclopedia of law and economics*, cit., 1033. More in general, on the expansion of EU competences, see O. Scarcello, *Fundamental Rights and the Federal Equilibrium: Comparing the Doctrines of Incorporation in the USA and the EU*, in Maastricht Journal of European and Comparative Law, 6/2023,

[14] M. Bussani, M. Infantino, *Harmonization of Tort law in Europe*, in *Encyclopedia of law and economics*, cit., 1033.

[15] U. Magnus, *Tort law in general*, in *Elgar Encyclopedia of Comparative Law*, M. Smits, et al. (edited by), Edwards Elgar, 2023, 882-883; M. Bussani, M. Infantino, *Harmonization of Tort law in Europe*, in *Encyclopedia of law and economics*, cit., 1035.

[16] M. Bussani, M. Infantino, *Harmonization of Tort law in Europe*, in *Encyclopedia of law and economics*, cit., 1034.

[17] T.K. Graziano, *Comparative tort law*, Routledge, 2018, 46.

[18] M. Bussani, M. Infantino, *Harmonization of Tort law in Europe*, in *Encyclopedia of law and economics*, cit., 1035.

ISSN 2281-5147

to non-contractual obligations[19]. Even in this case, however, deep uniformity has not been achieved due to disagreement over the meanings of important concepts[20].

The GDPR provides a clear example of these tort law harmonisation objectives[21], characterised by its unusual regulatory form and the compression of the entire liability regime into a single provision. However, in this regard, legal scholars have noted a lack of essential elements in art. 82 GDPR, which, despite the promise of complete harmonisation, could lead to only partial harmonisation[22]. Indeed, several key concepts, such as the standard of conduct, the causal link, and events beyond control (e.g., force majeure), are not defined in the Regulation but are essential to give concrete form to the liability framework.

To this end, where and how should the missing and necessary information be obtained when it is not provided by the GDPR?

This paper will address this issue relying on the legal principles shared by most civil liability systems in EU Member States. The reason for this choice lies in the fact that both the objectives of the GDPR and the CJEU are to harmonise the data protection regulatory frameworks of Member States, so the missing elements should be sought with this harmonisation objective in mind, to make it as feasible as possible. Focusing exclusively on the most widely shared principles may facilitate the interpretation of

[19] Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II), OJ L 199, 31.7.2007,

Another example is the Regulation (EC) No 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit rating agencies, OJ L 302, 17.11.2009.

[20] M. Bussani, M. Infantino, *Harmonization of Tort law in Europe*, in *Encyclopedia of law and economics*, cit., 1035.

[21] On the GDPR's purpose of civil liability harmonisation see E. Tosi, *Unlawful data processing prevention and strict liability regime under EU GDPR*, in Italian law journal, 7(2)/2021, 877; more in general, on the GDPR, see J.P. Albrecht, *How the GDPR will change the world*, in European data protection law review, 3/2016, 287.

[22] F. Episcopo, *UI v. Österreichische Post – A first brick in the wall for a European interpretation of art. 82 GDPR*, cit., 91; more in general, on the GDPR, see E. Mišćenić, A.L. Hoffman, *The role of opening clauses in harmonization of eu law: example of the EU's general data protection regulation (GDPR)*, in EU and comparative law issues and challenges series (ECLIC), 4/2020, 46.

ISSN 2281-5147

art. 82(3) of the GDPR and promote harmonisation among Member States, which are already familiar with these principles.

Conversely, grounding the interpretation in principles insufficiently shared across the Union risks producing the opposite outcome: the transplantation of legal institutions into legal systems unfamiliar with them may compel Member States to undertake significant structural adjustments[23].

Therefore, this paper will firstly outline how EU Member States traditionally addressed exemption clauses in tort law. The identification of the most shared principles will help in assessing whether the CJEU is interpreting art. 82(3) GDPR consistently with the tradition of the Member States, or, whether it is transplanting a so-called legal irritant[24], potentially compromising the effects of a uniform interpretation in all EU countries[25].

The task of identifying these principles will be pursued by referring to comparative legal doctrine, and, more specifically, to that aimed at determining the common principles of national tort law systems. In other words, the gaps in the GDPR will be filled by the legal findings obtained from research into the principles of EU tort law.

Since the 1980s, the EU institutions have initiated a (partial) process of Europeanisation of tort law, creating a new field of study characterised by the method of legal comparison, with varying nuances[26].

---

[23] M. Siems, *Comparative law*, Cambridge University Press, 2018, 239.

[24] See G. Teubner, *Legal Irritants: Good Faith in British Law or How Unifying Law Ends Up in New Divergencies*, in Modern law reviews, 61/1998; E. Örücü, *Law as transposition*, in International & comparative law quarterly, 2008.

[25] «Lack of familiarity with the new rules and their underpinning rationales, as well as the possible path dependency on deep rooted local traditions, could lead to the defeat of any harmonization project» (references omitted), M. Bussani, M. Infantino, *Harmonization of Tort law in Europe*, in *Encyclopedia of law and economics*, cit., 1033.

[26] R. Zimmermann, *Comparative law and the Europeanization of private law*, in *The Oxford handbook of comparative law*, M. Reimann, R. Zimmermann (edited by), Oxford University Press, 2020, 541.

ISSN 2281-5147

Comparative law has emerged as an indispensable method in the work of European courts, which have been shown to rely on the national law of all Member States both to interpret EU law and to apply the European Convention on Human Rights[27].

As mentioned, this paper will comment on the case-law of the Court of Justice of the European Union on the exemption clause provided for in art. 82 GDPR, using comparative studies on European tort law as a reference.

This paper suggests that the Court should fill the gaps in the GDPR by drawing on comparative tort law and the results obtained over the years only when such principles are sufficiently shared among Member States.

A reliable *tertium comparationis* is provided by the Principles of European Tort Law on Liability (PETL)[28], the result of an intense period of comparative tort law studies[29]; another is the Draft Common Frame of Reference (DCFR)[30], which, although

[27] «The aims of improving national legislation or national case law scarcely exhaust, however, the pragmatic or utilitarian applications of comparative legal reasoning. A larger pragmatic objective is the regional or international harmonization of law, of great importance today within Europe but also in the worldwide process of development of international and transnational law», H.P. Glenn, *Aims of comparative law,* in *Elgar Encyclopedia of Comparative Law,* J.M. Smits, et al. (edited by), Edwards Elgar, 2023; see also M. Martìn-Casals, *The impact of the PETL on national legislation and case law – a* survey, in Journal of European tort law, 14(1)/2023.

On the courts' use of Principles of European Contract Law (PECL), see J.M. Smits, *Convergence of private law in Europe: towards a new ius commune?*, in *Comparative law. A handbook*, E. Örücü, D. Nelken (edited by), Oxford and Portland Oregon, 2007, 232; T.K. Graziano, *Comparative tort law*, cit., 66.

[28] European Group on Tort Law, *Principles of European Tort Law* (Text and Commentary), Springer, Vienna/New York, 2005.

[29] «The first and the greatest strength of the PETL thus lies in the fact that they provide, for the first time, a *tertium comparationis* and a *reference* for future discussions and deliberations on tort law in Europe and beyond in the same way that the contract law principles do…A second strength of the PETL is the method that was used to prepare them. The PETL were developed on the basis of a broad comparative study…Today, such a broad comparative view is essential for the success of any project on common principles of European law, for the outcome of the research to be acceptable, and for support to be found throughout Europe», T.K. Graziano, *Comparative tort law*, cit., 51.

[30] C. von Bar, E. Clive, H. Schulte-Nölke (edted by), *Principles, Definitions and Model Rules of European Private Law: Draft Common Frame of Reference (DCFR)*, 2009.

ISSN 2281-5147

referring more to accountability than liability, does not differ significantly from the PETL[31].

These impressive works are of great importance for this paper: the harmonisation pursued through an EU regulation and through the decisions of the CJEU represents a top-down method of harmonisation which, despite its undisputed advantages in terms of enforcing power, risks imposing legal rules that are foreign to the legal traditions of the Member States (legal irritants), potentially compromising the effects of a uniform interpretation in all EU countries[32].

In this context, legal scholars have emphasised that top-down harmonisation should be supported by bottom-up initiatives aimed at developing a common legal culture[33]. The PETL and the DCFR, which provide an overview of the most widely shared EU

[31] «In the early 2000s the EU itself began a more comprehensive attempt at harmonization, under the rather open and vague notion of the Common Frame of Reference (CFR). In preparation for this exercise, two further academic groups - the Study Group on a European Civil Code and the so-called Acquis Group - published a Draft Common Frame of Reference (DCFR) in 2009. The tort law solutions proposed in the PETL and the DCFR are rather similar. Differences concern minor points only. Yet, at present, the EU appears to be restricting its CFR harmonization initiative to contract law, perhaps even to sales contracts and related services contracts» (references omitted), U. Magnus, *Tort law in general*, in *Elgar Encyclopedia of Comparative Law*, cit., 882-883.

[32] «Lack of familiarity with the new rules and their underpinning rationales, as well as the possible path dependency on deep rooted local traditions, could lead to the defeat of any harmonization project» (references omitted), M. Bussani, M. Infantino, *Harmonization of Tort law in Europe*, in *Encyclopedia of law and economics*, cit., 1033.

[33] «"Knowledge-building" enterprises share the common view that top-down harmonization cannot be undertaken without the collateral support of bottom-up initiatives. Therefore, the real instrument and target for those who are seeking the establishment of a truly European tort law should be the development of a common legal culture, based on as much knowledge as possible of the legal experience of each European jurisdiction. Irrespective of the uses to which knowledge may be applied, which may or may not include the pursuit of legal harmonization, knowledge building is both the starting point and the final aim of two projects whose scope is broader than the ones we just examined, insofar as their focus goes beyond tort law only. These two projects are the Ius Commune Casebooks for the Common Law of Europe and the Common Core of European Private Law», M. Bussani, M. Infantino, *Harmonization of Tort law in Europe*, in *Encyclopedia of law and economics*, cit., 1038.

ISSN 2281-5147

principles on tort law, can be considered as such, as can other studies, justifying their presence in this paper[34].

3. Infringement and liability exemption

3.1 The context

Before the Court initiated its jurisprudential process, scholars had pointed out that art. 82 GDPR highlights the shortcomings in the coordination between European and national tort law[35].

Art. 82 GDPR is generally interpreted as recognising the right of data subjects to compensation without any recourse to national law[36]. However, despite this intention, the provision was formulated ambiguously, reflecting a middle ground between partial and complete harmonisation, leaving commentators with considerable doubts[37]. This ambiguity has amplified the CJEU's role, which has been called upon to identify and specify which national rules remain permitted and which should be considered pre-empted by the GDPR[38].

[34] Despite this reliance, this research considers the issues related to the findings of comparative studies. To this connection, see U. Kischel, *Comparative law*, Oxford University Press, 2019, 88; M. Bussani, M. Infantino, *Harmonization of Tort law in Europe*, in *Encyclopedia of law and economics*, cit., 1038.

[35] J. Knetsch, *The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases*, in Journal of European Tort Law, 13(2)/2022, 153; see also F. Episcopo, *The vicissitudes of life at the coalface: remedies and procedures for enforcing union law before national courts*, in *The evolution of EU law*, P. Craig (edited by), Oxford University Press, 2017.

[36] G. Zanfir-Fortuna, *Article 82. Right to compensation and liabilty*, in C. Kuner, L.A. Bygrave, C. Docksey, L. Drechsler, *The EU General Data Protection Regulation (GDPR): A Commentary,* 2020, 1163; S. Li, *Compensation for non-material damage under Article 82 GDPR: a review of case C-300/21,* cit., 336.; J. Knetsch, *The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases*, cit., 137-138.

[37] F. Episcopo, *UI v. Österreichische Post – A first brick in the wall for a European interpretation of art. 82 GDPR*, cit., 91.

[38] P.A. de Miguel Asensio, *Determinación de la indemnización por daños derivados de infracciones del Reglamento General de Protección de Datos*, cit., 496.

ISSN 2281-5147

To this end, in interpreting art. 82 GDPR in C-300/21, the Court ruled that the «terms of a provision of EU law which makes no express reference to the law of the Member States for the purpose of determining its meaning and scope must normally be given an autonomous and uniform interpretation throughout the European Union, having regard, inter alia, to the wording of the provision concerned and to its context»[39] (para 29)[40].

This line of interpretation has been followed in subsequent decisions, implying that the entire case-law of the CJEU on art. 82 GDPR represents an attempt to harmonise the data protection liability regime across all Member States, except for the quantification of compensation, which remains within the competence of national courts[41].

In C-300/21, the Court identified the conditions necessary for civil liability in data protection: (i) processing of personal data that infringes the provisions of the GDPR; (ii) damage suffered by the data subject; (iii) a causal link between the unlawful processing and the damage (para 32, 36).

This paper aims to shed light on the exemption clause provided for in art. 82(3) GDPR, and this objective requires analysing two of the three conditions necessary for liability: the infringement and the causal link. Both elements can be discussed without a deep inquiry into the nature of the damage, which would not affect the notions of infringement and causation.

---

[39] «Un concepto propio o autónomo constituye un término común a todos los Estados miembros de la Unión Europea que se va formando a partir de las interpretaciones que realiza el Tribunal de Luxemburgo de conformidad con los Tratados a petición de los órganos jurisdiccionales nacionales», M.C. Vergès, *El concepto autònomo de responsabilidad civil en el àmbito de la protecciòn de datos personales en la era digital: anàlisis del artìculo 82 del regolamento 2016/679,* cit., 58; see also F. Gotzen, *Autonomous Concepts in the Case Law of the Court of Justice of the European Union on Copyright*, Revue Internationale du Droit d'Auteur, 262/2020; L. Mancano, *Judicial Harmonisation Through Autonomous Concepts of European Union Law. The Example of the European Arrest Warrant Framework Decision*, in European law review, 43/2018.

[40] The Court refers to judgments of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraph 81; of 10 February 2022, *ShareWood Switzerland*, C-595/20, EU:C:2022:86, paragraph 21; of 15 April 2021, *The North of England P & I Association*, C-786/19, EU:C:2021:276, paragraph 48, and of 10 June 2021, *KRONE – Verlag*, C-65/20, EU:C:2021:471, paragraph 25).

[41] C-300/21, para 59.

ISSN 2281-5147

3.2 The GDPR infringement

What constitutes a violation can be inferred from recital 146 GDPR, according to which unlawful data processing is that which violates the Regulation, its delegated and implementing acts, and the laws of Member States specifying the rules of the GDPR.

Before the CJEU's case-law on art. 82 GDPR, since the Regulation does not explicitly identify all possible unlawful processing, scholars wondered whether only some violations of the GDPR, or all of them, should be considered sufficient to establish a cause of action for compensation[42], refraining from the old issue of protected interests[43]. The view that art. 82 GDPR is a general rule of liability[44] that has gained widespread popularity and is followed by most national courts in the EU[45].

Moreover, although it was generally accepted that any obligation established by the GDPR, if breached, could give rise to a right to compensation, some authors noted that, in order to determine whether a provision had been breached, the nature of the obligation in question had to be taken into account[46].

---

[42] «However, it is not without reason that the European Parliament insisted on the general term 'infringement'. Indeed, this term can also be interpreted in a way that any kind of infringement is sufficient to give a cause of action to the claimant. If so, this would also include violations of information rights laid out in arts 12–15 GDPR», J. Knetsch, *The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases*, cit., 142.

[43] U. Magnus, *Tort law in general*, in *Elgar Encyclopedia of Comparative Law*, cit., 878-879; see also S.D. Lindenbergh, *Damages (in tort),* in *Elgar Encyclopedia of Comparative Law,* J.M. Smits, et al. (edited by), Edwards Elgar, 2023, 289; European Group on Tort Law, *Principles of European Tort Law* (Text and Commentary), cit., 24.

[44] M. Gambini, *Responsabilita e risarcimento nel trattamento dei dati personali*, in Cuffaro V., D'Orazio R., Ricciuto V. (edited by), *I dati personali nel diritto europeo*, 2019, 1033.

[45] For instance, on compensation for violation of art. 15 GDPR, see Higher Regional Court (Oberlandesgericht) of Vienna, 7 December 2020, ref 11 R 153/20f, 154/ 20b; Regional Labour Court (Landesarbeitsgericht) of Lower Saxony, 22 October 2021, ref 16 Sa 761/20; Labour Court (Arbeitsgericht) of Neumünster, 11 August 2020, ref 1 Ca 247 c/20.

[46] «To properly understand the liability exposure of controllers, it is necessary to first understand the nature of controller obligations», B. Van Alsenoy, *Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation*, in Journal of Intellectual Property, Information Technology and E-Commerce Law, 7(3)/2016, 273.

ISSN 2281-5147

Such structure reflects a distinction traditionally recognised across European private law systems, which generally distinguish between two types of obligations: obligations to use reasonable care and skill (known as *Dienstvertrag* in Germany, *obligation de moyens* in France, or *obbligazione di mezzi* in Italy)[47], linked to fault-based liability systems[48], and obligations to achieve a specific result (known as *Werkvertrag* in Germany, *obligation de résultat* in France, or *obbligazione di risultato* in Italy)[49], linked to liability systems not based on fault (hereinafter, we will refer to this approach as strict liability)[50].

Obligations of means (or conduct) are framed as commitments to perform a specific task with due care and diligence, or to exert best effort[51]. They do not guarantee a particular result[52]. In the context of professional obligations, determining whether the

[47] M. Bussani, A.J. Sebok, M. Infantino, *Common law and civil law perspectives on tort law*, Oxford University press, 2019, 56; the same applies for contractual liability, see D. Alessi, *The distinction between Obligations de Résultat and Obligations de Moyens and the Enforceability of Promises*, in European review of private law, 13(5), 2005.

[48] M. Cappeletti, *Justifying strict liability: a comparative analysis in legal reasoning*, Oxford University press, 2022, 13; M. Bussani, A.J. Sebok, M. Infantino, *Common law and civil law perspectives on tort law*, cit., 43; F. Werro, E. Buyuksagis, *The bounds between negligence and strict liability*, in *Comparative Tort Law*, M. Bussani, A.J. Sebok (edited by), Edward Elgar, 2015, 203; U. Magnus, *Tort law in general*, in *Elgar Encyclopedia of Comparative Law*, cit., 880.

[49] M. Bussani, A.J. Sebok, M. Infantino, *Common law and civil law perspectives on tort law*, cit., 56; the same applies for contractual liability, see D. Alessi, *The distinction between Obligations de Résultat and Obligations de Moyens and the Enforceability of Promises*, cit.

[50] «Under a regime of strict liability, the underlying principle is that liability ought to result from the materialization of a specific risk, which is linked either to a thing or an activity under the defendant's control, irrespective of any actual lack of care on his part. A milder form of strict liability can be found where a lack of care on the defendant's part is presumed upon the materialization of a particular hazard and occurrence of certain injuries; as noted, if such a presumption is not subject to refutation, the liability is strict i). The determining factor for imposing such liability is usually that the injuries in question tend to occur even where due care is exercised, or that they can be avoided only at excessive cost (ii)» F. Werro, E. Buyuksagis, *The bounds between negligence and strict liability*, cit., 207; M. Cappeletti, *Justifying strict liability: a comparative analysis in legal reasoning*, cit, 14.

[51] B. Winiger, E. Karner, K. Oliphant (edited by), *Digest of European tort law, Volume 3: Essential cases on misconduct*, De Gruyter, 2018, 777.

[52] B. Winiger, E. Karner, K. Oliphant (edited by), *Digest of European tort law, Volume 3: Essential cases on misconduct*, cit., 28.

ISSN 2281-5147

task has been performed with due care depends on the specific type of obligation assumed and the circumstances of the case, namely, the standard of conduct[53]. To establish liability for a breach of an obligation of means, proof of fault is required[54].

Obligations of result, on the other hand, are characterised by a commitment to achieve a specific outcome and have traditionally been linked to a strict liability regime focused on whether or not the result is achieved[55]. However, even in these cases, a strict exempting proof is admitted[56].

In conclusion, an infringement cannot be established if the data controller or data processor provides valid exonerating evidence. Accordingly, obligations of means are not considered breached if the standard of conduct is met, regardless of whether damage has occurred[57]. Similarly, obligations of result must not be deemed breached when the perpetrator of the unlawful act has demonstrated *force majeure* or exonerating conduct by the victim[58].

---

[53] European Group on Tort Law, *Principles of European Tort Law* (Text and Commentary), cit., 76; similarly, C. von Bar, E. Clive, H. Schulte-Nölke (edted by), *Principles, Definitions and Model Rules of European Private Law: Draft Common Frame of Reference (DCFR)*, cit., 3274.

[54] O. Morèteau, *Basic questions of tort law from a french perspective*, in *Basic questions of tort law from a comparative perspective*, H. Koziol (edited by), Jan Sramek Verlag, 2015, 34.

[55] «In some other legal systems, and especially in an international comparative context, the notion of force majeure is first and foremost dealt with in relation to duties to achieve a specific result», M. Schmidt-Kessel, K. Mayer, *Supervening events and force majeure*, in *Elgar Encyclopedia of Comparative Law*, M. Smits, et al. (edited by), Edwards Elgar, 2023, 840; O. Morèteau, *Basic questions of tort law from a french perspective*, cit., 34.

[56] European Group on Tort Law, *Principles of European Tort Law* (Text and Commentary), cit., 127; similarly, C. von Bar, E. Clive, H. Schulte-Nölke (edted by), *Principles, Definitions and Model Rules of European Private Law: Draft Common Frame of Reference (DCFR)*, cit., 3538.

[57] J. Gardner, *Torts and other wrongs*, Oxford university press, 2019, 216.

[58] European Group on Tort Law, *Principles of European Tort Law* (Text and Commentary), cit., 129 on *force majeure*, stating that «if a natural phenomenon causes the victim's loss which has to be considered part of the latter's sphere anyway (see Art, 3:106), to that extent liability cannot be established in the first place, so that no defence is needed on the keeper's side»; similarly, C. von Bar, E. Clive, H. Schulte-Nölke (edted by), *Principles, Definitions and Model Rules of European Private Law: Draft Common Frame of Reference (DCFR)*, cit., 3539-3540; M. Bussani, A.J. Sebok, M. Infantino, *Common law and civil law perspectives on tort law*, cit., 24-25.

ISSN 2281-5147

These distinctions are also relevant in the context of the GDPR.

In this regard, it has been emphasised that most of the obligations imposed on data controllers under the GDPR are formulated as obligations of means, for example, art. 17(2) GDPR, which requires data controllers to take 'reasonable steps' to inform other data controllers of the erasure request, was intended as such[59]. Conversely, the obligation under art. 35(1) GDPR, which requires processors to consult the supervisory authority in advance for high-risk data processing, could be classified as an obligation of result, as it leaves no room for a different outcome.

However, some obligations have hybrid characteristics. For example, the obligation to ensure processing in accordance with art. 32 GDPR has been considered both an obligation of means by some[60] and an obligation of result by others[61], with the consequence of different liability regimes.

As explained, according to the traditional relationship between the legal nature of the obligation and the relevant liability regime, when a duty is considered an obligation of means, the data controller only has to demonstrate compliance with the required standard of conduct; this means that, for example, a data breach would not be sufficient in itself to establish the inadequacy of security measures under art. 32 GDPR. Conversely, if considered as an obligation of result, the loss of data resulting

[59] B. Van Alsenoy, *Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation*, cit. 282.

[60] «Under the GDPR, damages due to a breach of the security do not always lead to private law liability. Pursuant to Article 82(1), the data subjects are only entitled to receive compensation if there is an infringement. There is no violation if the security of the personal data was breached despite the implementation of appropriate measures», P.T.J. Wolters, *The security of personal data under the GDPR: a harmonized duty or a shared responsibility?*, in International Data privacy law, 7(3)/2017, 172; B. Van Alsenoy, *Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation*, cit.; L.A. Bygrave, *Security by design: aspirations and realities in a regulatory context*, in Oslo law review, 8(3)/2021.

[61] «For example, considering the way the GDPR defines 'pseudonymisation', it implies that pseudonymisation has not only to be technically implemented in data protection systems, but also to result in organisational measures, such as management of access rights for the personnel that has access to the key of the pseudonymised data», L. Jasmontaite, et al., *Data protection by design and by default: framing guiding principles into legal obligations in the GDPR*, in Data protection by design and by default, 2/2018, 7; F. Bilotta, *La responsabilita civilenel trattamento dei dati personali*, in *Circolazione e protezione dei dati personali, tra liberta e regole del mercato*, R. Panetta (edited by), 2019.

ISSN 2281-5147

from a data breach should automatically trigger the controller's liability. In the latter case, however, the controller could still demonstrate that it is not in any way responsible for the event giving rise to the damage under art. 82(3) GDPR, for example, by demonstrating *force majeure* or significant conduct on the part of the data subject.

That said, it should be noted that, while this relationship is traditionally understood as described, some scholars have deviated from it in their interpretation of the provisions of the GDPR, for example, by associating obligations of means with strict liability[62], highlighting a lack of certainty as to how this relationship should be understood.

Although art. 82(3) GDPR certainly excludes forms of absolute liability[63], the legal nature of the data protection liability regime provided for in art. 82 GDPR was controversial even before the CJEU's case-law. Most scholars were inclined to interpret art. 82 GDPR as a strict liability regime[64]. In support of this interpretation, it was noted that this liability regime could be considered a continuation of the one provided for in art. 23 of Directive 95/46/EC[65], which was interpreted as requiring proof of an external cause or event beyond control, such as *force majeure* or error on

[62] Van Alsenoy links art. 32 GDPR, intended by him as an obligation of means, to a strict liability regime: B. Van Alsenoy, *Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation*, cit., 283.

[63] «"absolute liability" (where no or hardly any defences apply)», European Group on Tort Law, *Principles of European Tort Law* (Text and Commentary), cit., 102; M. Bussani, A.J. Sebok, M. Infantino, *Common law and civil law perspectives on tort law*, cit., 24.

[64] *Ex* multis, see R. Strugala, *Art. 82 GDPR: Strict Liability or Liability Based on Fault?*, in European Journal of Privacy Law & Technologies (EJPLT), 2020; G. Zanfir-Fortuna, *Article 82. Right to compensation and liability*, cit.; E. Tosi, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, Giuffrè, 2019; S. Li, *Compensation for non-material damage under Article 82 GDPR: a review of case C-300/21*, 336.

[65] «Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage».

ISSN 2281-5147

the part of the data subject[66]. Given their similar wording, art. 82 GDPR has been interpreted as requiring the same type of proof[67]. From this perspective, the mere absence of fault would not be sufficient to exempt from liability[68].

3.3 The causal link between infringement and damage

Moving on to the causal link, the Regulation does not even mention it. The Court of Justice of the European Union has inferred it through a literal interpretation of art. 82 GDPR, which refers to «damage caused by processing which infringes this Regulation» (paragraph 2) and to «any damage caused by processing» (paragraph 3)[69].

This is not new: even national legislatures have not explicitly addressed its definition or its actual functioning[70], given the difficulties in defining a generally applicable criterion of causation test[71].

---

[66] B. Van Alsenoy, *Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation*, cit., 283; other scholars admitted the possibility to establish a fault-based liability system based on art. 23, see T. Kosmides, *The legal nature of the controller's civil liability according to art. 23 of Directive 95/46 EC (Data Protection Directive)*, in *Honorary Volume for Evi Laskari*, M. Bottis, A. Giannakoulopoulos (edited by), texts and articles from the 5th International Conference on Information Law (ICIL), 2012.

[67] «Interestingly, the GDPR does not contain a recital similar to recital (55) of Directive 95/46, which provides two examples of how a controller might prove that it is "not responsible for the event giving rise to the damage" (i.e., force majeure or error on the part of the data subject). Nevertheless, it is reasonable to assume that the words "not responsible for the event giving rise to the damage" should still be interpreted in the same way. As a result, the escape clause of article 82(3) still refers exclusively to "events beyond control", i.e. an abnormal occurrence which cannot be averted by any reasonable measures and which does not constitute the realisation of the risk for which the person is strictly liable. If anything, the addition of the words "in any way" (in comparison to article 23 [2] of Directive 95/46), suggests a desire to tighten the scope of the escape clause even further», B. Van Alsenoy, *Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation*, cit., 283.

[68] J. Knetsch, *The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases*, cit., 142.

[69] C-300/21, para 32, 36, 37.

[70] M. Bussani, A.J. Sebok, M. Infantino, *Common law and civil law perspectives on tort law*, cit., 177-178.

[71] C. Van Dam, *European tort law*, Oxford University Press, 2013, 307.

ISSN 2281-5147

In the context of data protection, the literature is very limited. The few scholars who have addressed it have invoked general principles of causality without providing specific adaptations for data protection[72].

In analysing traditional causality theory, it should be emphasised that most EU Member States recognise the fundamental distinction between factual and legal (or policy-based) investigations of causality. However, despite this common ground, a comparison between Member States has highlighted the fragmentation of how these inquiries actually work[73]. Indeed, in some cases, national legal systems have used different tools and reasoning yet arrived at similar results; in other cases, even when the same tool or rule was invoked, it was applied with different meanings or produced different results[74]. In this regard, it has been observed that once general theories are abandoned, practical cases demonstrate that they are applied differently[75].

[72] «La relación de causalidad implica que esa infracción del Reglamento de protección de datos es la *conditio sine qua non* de la causa del perjuicio a la víctima, ya que, si no se hubiese producido la misma, no hubiera habido daños. La infracción en el ámbito de la protección de datos personales ha de estar suficientemente demostrada a nivel objetivo, pero no podemos obviar que la relación causa-efecto acostumbra a ser de carácter subjetivo. Por tanto, es preciso aportar pruebas que la apoyen basadas en los medios permitidos en derecho. En algunos casos son relaciones difíciles de demostrar o justificar, debido a la subjetividad que implican, especialmente en el ámbito de la imagen personal» (references omitted), M.C. Vergès, *El concepto autònomo de responsabilidad civil en el àmbito de la protecciòn de datos personales en la era digital: anàlisis del artìculo 82 del regolamento 2016/679*, cit., 276; see also J. Knetsch, *The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases*, cit., 145 ff.

[73] «Second, all European jurisdictions acknowledge a fundamental divide running through the causal inquiry, which can be broken down into different sub-species of investigation: one eminently factual, and the other quintessentially legal or policy-based.6 In many legal systems, the divide overlaps with that between issues of facts and issues of law, thus determining the reviewability of judgments», M. Infantino, E. Zervogianni, *Unravelling causation in European tort laws*, in Rabels zeitschrift fur auslandisches und internationals privatrecht, 83/2019, 649-650, 672.

[74] «Still, the disagreement as to the outcome does not necessarily imply a different approach to causation as such, the disagreement being attributable to reasons other than causation. This confirms Sacco's well-known finding about the possible mismatch between declamatory statements, official rules and operational results, but it also corroborates the idea that it is hard to see clear lines of convergence in European legal systems' approaches to causation» (references omitted), M. Infantino, E. Zervogianni, *Unravelling causation in European tort laws*, cit., 672.

[75] C. Van Dam, *European tort law*, cit., 308.

ISSN 2281-5147

These differences stem from the different theories applied at each stage. While factual causation is generally established on the basis of the but-for/*condicio sine qua non* test[76], the second stage of the investigation is governed by a wide range of tests rooted in different key concepts[77]. Indeed, on the one hand, the factual investigation requires little more than establishing that the damage would not have occurred in the absence of the unlawful activity; on the other hand, the more indirect and distant the link between the data processing activity and the damage, the more political reasoning is required to determine whether causality should be accepted or not[78].

As regards the factual examination, as mentioned above, the standard criterion is the but-for test, according to which, in the absence of the defendant's unlawful activity, the claimant would not have suffered such damage[79]. The assessment of legal causality is carried out through various theories[80], such as that based on the predictability of the damage caused, which makes the defendant liable only for those damages whose occurrence was foreseeable; or based on the scope of application of the violated rule, according to which compensation is granted only for damages that can be considered

[76] The PETL describe this test as «an activity or conduct…is a cause of the victim's damage if, in the absence of the activity, the damage would not have occurred», European Group on Tort Law, *Principles of European Tort Law* (Text and Commentary), cit., 43.

[77] «Third, it is often emphasized – especially in comparative tort law literature – that the space and the role reserved for causation analysis are not uniform across legal systems. On the basis of studies whose focus was largely on the triad of the "major" European jurisdictions (that is, England, France and Germany), it is often observed that jurisdictions whose main liability equation includes extensive analysis on whether the defendant breached a duty of care owed to the victim (England), or on whether the latter's injury is worthy of tort law protection (Germany), leave in principle less room for causation reasoning than jurisdictions based on a broad formula for negligence liability (France)» (references omitted), M. Infantino, E. Zervogianni, *Unravelling causation in European tort laws*, cit., 649-650; C. Van Dam, *European tort law*, cit., 310.

[78] «Among those considerations rank the foreseeability of the damage, the magnitude of the damage, the value of the violated right or interest and the protective purpose of the violated rule or duty», U. Magnus, *Tort law in general*, in *Elgar Encyclopedia of Comparative Law*, cit., 879.

[79] I. Puppe, *The concept of causation in the law,* in *Critical essays on causation and responsibility*, B. Kahmen, M. Stepanians (edited by), De Gruyter, 2013, 69; M. Infantino, *Causation theories and causation rules*, in *Comparative tort law*, M. Bussani, A.J. Sebok (edited by), Edwards Elgar, 2015, 283-284; for the problems related to the *condicio sine qua non* test see C. Van Dam, *European tort law*, cit., 311.

[80] For an overview see cit. European Group on Tort Law, *Principles of European Tort Law* (Text and Commentary), cit., 61ff.

ISSN 2281-5147

within the scope of application of the rule violated by the wrongdoer; however, legal causality can also be determined on the basis of the so-called "proximity rule", which assesses the proximity between the activity in question and the resulting damage[81].

An important difference between Member States concerns the evidence required to establish/break the causal link. In some jurisdictions, indeed, the causal link is established if ascertained with certainty (*überwiegende Wahr-scheinlichkeit* in Germany), while in others a predominant probability (*più probabile che non* in Italy, or *degré suffisant de probabilité* in France) of the purported cause is deemed sufficient[82].

The fragmentation that characterises theories of causality in the EU makes it difficult to envisage harmonising this element. Given the GDPR's silence on this matter, the CJEU would be left to interpret the causality nexus without any explanation from the GDPR on how it should work and without a generally accepted theory among Member States. The risk of harmonisation would be to impose concepts and notions that could be in sharp contrast to the traditions of some Member States.

In light of the above, it appears to be a broad consensus on the general notion of infringement. In contrast, the practical functioning of the causal link remains highly fragmented across the Member States. Taking this into account, and considering additional elements, such as the absence in the GDPR of a clearly identified liability criterion (whether fault-based or not) and of the required exonerating evidence, as well as the harmonisation purpose of both the GDPR and the case law of the CJEU, it may be suggested that the Court interprets the notion of infringement under art. 82 GDPR in light of the legal traditions of the Member States. Given the broad consensus outlined above, such an approach could facilitate the Court's objective of promoting harmonisation.

Conversely, any attempt to harmonise the operation of the causal link may result in the transposition of legal irritants into national systems, where such concepts risk

[81] M. Infantino, *Causation theories and causation rules*, cit., 283-284; C. Van Dam, *European tort law*, cit., 311.

[82] C. Van Dam, *European tort law*, cit., 324-326; M. Infantino, *Causation theories and causation rules*, cit., 295; T.K. Graziano, *Comparative tort law*, cit., 279.

ISSN 2281-5147

colliding with pre-existing doctrinal categories and procedural frameworks, thereby generating frictions rather than convergence.

However, as will be described, the CJEU did not delve into the concept of infringement, ultimately associating the criterion of fault with obligations of result (see C-741/21), thereby requiring Member States to adopt an interpretation of the law that, in most instances, runs counter to their established legal traditions.

Section 3.4 examines the trajectory of the CJEU's case law, highlighting the specific developments that led the Court to depart from the legal traditions most widely shared across the Member States, ultimately undermining the harmonisation purpose of the GDPR.

3.4 The CJEU path

The case-law of the Court of Justice of the European Union will be presented below in chronological order, including the opinions of the Advocates General where relevant to the analysis. Each decision will be accompanied by commentary and linked to others to reflect the Court's evolving interpretation.

As will be described, the Court set out its position in cases C-340/21 and C-667/21 and, albeit with nuances, adopted a fault-based liability regime, which it confirmed in subsequent decisions. In the analysis, it will be highlighted that the principles set out in cases C-340/21 and C-667/21, while appropriate with respect to obligations of conduct, do not provide a solid basis for harmonisation in relation to breaches of obligations of result, as was the case in C-741/21.

The discussion will offer a different interpretation of the GDPR liability regime, connecting it to the general doctrine of EU tort law, the GDPR's harmonisation purpose, and the specific peculiarities of the case presented to the Court.

C-340/21.

The first judgment assessing the infringement as a necessary condition to establish liability is C-340/21, whose AG's opinion is particularly relevant.

The first preliminary question asked whether art. 24 and 32 GDPR should be interpreted as that unauthorised disclosure of personal data or unauthorised access by

ISSN 2281-5147

third parties are in themselves sufficient elements to hold that the technical and organisational measures implemented by the controller were not appropriate in the meaning of art. 24 and 32 GDPR.

The Advocate General's Opinion.

The Advocate General's opinion is based on two fundamental premises: i) the technical and organisational measures required by the principle of accountability[83] should be appropriate, in the sense that they should achieve a certain level of acceptability «both in technical terms (relevance of measures) and qualitative terms (effectiveness of protection)» (para 26); ii) the GDPR would be modelled on risk prevention and the accountability of the data controller, thus adopting a purposive approach aimed at achieving the best possible result in terms of effectiveness (para 27).

In answering the first question referred, the Advocate General first focused on the literal interpretation of art. 24 and 32 of the GDPR, emphasising the discretion of the data controller in determining the most appropriate measures, in light of the specific assessment factors listed therein (paras 30, 31). In particular, the AG focused on two criteria: the state of the art and the costs of implementation.

The state-of-the-art factor was discussed in relation to the security measures prescribed by art. 32 GDPR. In the AG's opinion, this implies that appropriateness should be measured on the basis of what was technologically reasonably possible at the time of implementation (also taking into account the costs of implementation) (para 32). Such appropriateness was conceptualised as being maintained despite possible breaches, carried out using highly sophisticated tools capable of overcoming measures implemented in accordance with the state of the art (para 33).

[83] «The principle of accountability is established by Article 5(2) GDPR, affirming that 'the controller shall be responsible for, and be able to demonstrate compliance with paragraph 1 (accountability). By stating so, Article 5(2) establishes the autonomy of the principle of accountability in the data protection law eco-system, and at the same time the strict operational connection to other principles relating to the processing of personal data - such as the principle of lawfulness, of fairness and of transparency - and to the rules that substantiate these principles», G. Schneider, *Accountability*, in *Elgar encyclopedia of law and data science*, G. Comandè (edited by), Edward Elgar, 2022, 9.

ISSN 2281-5147

Turning to implementation costs, the AG claimed that a balance is required between the interests of data subjects, who generally tend towards a higher level of protection, and the economic interests of data controllers, who sometimes favour a lower level of protection (para 36).

This literal interpretation was complemented by a teleological one[84], according to which it would be illogical to impose on data controllers the obligation to prevent any personal data breach regardless of the diligence required for the preparation of security measures; moreover, the AG continued, if it is true that the GDPR establishes a framework of accountability, then data controllers should always be able to demonstrate their compliance (para 35).

This opinion, expressed on the first referred question, should be linked to that expressed on the fourth referred question, which analyses the exempting proof contained in art. 82(3) GDPR.

It was asked whether the liability exemption clause provided for in art. 82(3) GDPR should be interpreted as excusing data controllers merely because the damage resulted from an unauthorised disclosure of, or access to, personal data realised by third parties.

The Advocate General's response began by recalling the philosophy underlying the Regulation, namely the rejection of automatisms (para 59). It follows a literal interpretation of art. 82(3) GDPR and recital 146 GDPR, both of which require to be «not in any way responsible for the event giving rise to the damage». From this wording, the AG deduced that the standard of proof required is quite high (para 60) and recalled, by analogy, the case law of the CJEU, according to which exceptions to a general rule must be interpreted restrictively (footnote 21)[85].

On this basis, the AG directly addressed the question of the nature of the liability regime. It argued that a coordinated reading of art. 82 GDPR and the obligations to

[84] The Advocate does not explicitly differentiate between the different types of interpretation, however, how it will be shown, it could have been relevant.

[85] It cites the following decisions: 15 October 2020, *Association française des usagers de banques* (C-778/18, EU:C:2020:831, paragraph 53), and of 5 April 2022, *Commissioner of An Garda Síochána and Others* (C-140/20, EU:C:2022:258, paragraph 40).

ISSN 2281-5147

implement and demonstrate the appropriateness of technical and organisational measures (defined as obligations of conduct) allow for the recognition of a form of liability aggravated by the presumption of fault (para 62). The AG based its position on the fact that data controllers can provide exonerating evidence, contrary to what is permitted in strict liability regimes (para 63). Furthermore, it added that the reversal of the burden of proof reflects the need to make compensation effective, as data subjects would encounter excessive difficulties in proving the fault of data controllers. Conversely, the data controller is in the best position to prove that she is not responsible for the event that caused the damage (para 63). Based on the above regarding the nature of the data controller's liability, the AG stated that data controllers can always prove that they are in no way liable for the event that caused the damage; however, the mere fact that the event was caused by a person outside their sphere of control cannot be considered sufficient evidence to exempt them from liability (para 65). Indeed, it continued, the event that caused the damage could be precisely the inadequacy of the measures applied, resulting from the data processors' fault (para 66). If such scenarios did not fall within the scope of art. 82 GDPR, data subjects would not be entitled to compensation and the protection objective pursued under art. 1(2), recitals 10, 11 and 13 GDPR could not be achieved (para 68).

For these reasons, the Advocate General concluded that, under art. 82(3) GDPR, which exempts the controller from liability on the sole ground that a third party has infringed the Regulation, would have an effect incompatible with the protection objective pursued by the GDPR (para 69).

Comment

In highlighting the critical aspects, the fundamental principles underlying the opinion on the first referred question require some clarification. First, the Advocate General emphasised that the entire regulation is guided by risk prevention and accountability of the data controller; subsequently, however, it concluded in favour of a fault-based liability regime. In this regard, it is worth noting that risk-based regulations and fault-based liability systems are not inherently at odds. However, Member States have

ISSN 2281-5147

traditionally linked risky activities, such as data processing, to strict liability regimes to narrow the scope for exemptions[86].

Subsequently, when the AG states that the GDPR requires only the *best possible* result in terms of the effectiveness of the measures, it provides its own interpretation based on the entire regulation, rather than on specific sentences (there are no sentences in the regulation that require only the *best* effectiveness or appropriateness of the measures, as understood by the AG)[87]. In this case, the AG considered art. 24 and 32 GDPR as obligations of means, defining them as obligations of conduct, which reflect a specific diligence and require only the exercise of best efforts. In this regard, concluding in favour of a fault-based liability regime is consistent with the legal traditions of the Member States, thus making harmonisation in this area feasible.

Moving on to the criterion of implementation costs, the AG's interpretation appears particularly problematic. The AG interprets this parameter as requiring only the adoption of measures that entail reasonable costs. However, this interpretation appears in contrast to the European Data Protection Board's (EDPB) opinion on the principles of data protection by design and by default[88]. In that opinion, the EDPB stated that implementation costs should not be a reason not to implement data protection by design; indeed, the EDPB continues, the measures chosen must ensure compliance with the principles of the GDPR, regardless of the financial effort

[86] G.C. Keating, *Reasonableness and risk: right and responsibility in the law of torts*, Oxford University press, 2022, 230; the PETL distinguished between dangerous and abnormally dangerous activities, both falling under the strict liability regime, European Group on Tort Law, *Principles of European Tort Law* (Text and Commentary), cit., 101; in this regard, it was stated that the references to risks enshrined in art. 24 and 32 GDPR should not be interpreted to investigate the nature of the liability regime, see B. Van Alsenoy, *Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation*, cit., 282.

[87] Such reading is in line with the idea, generally accepted, according to which risk-management frameworks are not intended to require the removal of every possible risk. In this sense see M. Macenaite, *The "riskification" of European data protection law through a two-fold shift*, in European journal of risk regulation, 2017.

[88] EDPB, Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, version 2.0, adopted on 20 October 2020.

ISSN 2281-5147

required[89]. In this regard, it was stated that, even taking into account implementation costs, the measures taken must at least ensure the effective protection of data subjects[90]. Although not directly applicable, the EDPB's opinions are of great importance for interpreting data protection rules. Therefore, if the AG's purpose were to suggest that the CJEU overrules the EDPB's statement, further justification would have been necessary. Instead, the AG opted for a succinct interpretation of *reasonable* costs, without adequate elaboration.

The CJEU's decision

Moving on to the Court's decision on the first question referred, it concerned the autonomous and uniform interpretation of art. 24 and 32 GDPR. It is worth recalling that the Court was asked whether art. 24 and 32 GDPR could be interpreted as meaning that the unauthorised disclosure of personal data or unauthorised access by third parties is sufficient to establish that the measures taken by data controllers were not appropriate.

The Court began by pointing out that art. 24 and 32 GDPR do not expressly refer to the law of the Member States for the purposes of determining their meaning and scope, so the terms contained therein must be interpreted autonomously and uniformly throughout the European Union, taking into account the wording of the provisions, their objectives and their context (para 23).
As a preliminary point, the Court held that art. 24 GDPR imposes a general obligation to implement appropriate technical and organisational measures to ensure that data processing activities are carried out in accordance with the GDPR and to demonstrate such compliance (para 24)[91]. In this regard, the Court stated that the principle of accountability laid down in art. 5(2) GDPR finds its operational expression in art. 24 GDPR (para 48)[92].
The actual analysis began with literal and teleological interpretations of art. 32 GDPR, clarifying that it can be inferred from its wording that the Regulation establishes a

[89] EDPB, Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, version 2.0, adopted on 20 October 2020, 9, para 25.

[90] A. Selzer, *The appropriateness of technical and organisational measures under article 32 GDPR*, in European Data Protection law review, 1/2021, 123; C. Quelle, *The 'risk revolution' in EU data protection law: we can't have our cake and eat it, too*, in Tilburg Law School Legal Studies Research Paper Series, 17/2017, 20.

[91] Confirmed in C-687/21, para 36.

[92] Confirmed in C-687/21, para 43.

ISSN 2281-5147

risk-management system and that it in no way purports to eliminate all risks of personal data breaches: such risks must be managed and mitigated by appropriate measures, such as those referred to in art. 32 GDPR (para 29). In this regard, with respect to data breaches, the Court analysed the wording of art. 24 and 32 GDPR and stated that these provisions simply require data controllers (and data processors, if appointed) to take technical and organisational measures to prevent, as far as possible, data breaches (para 30)[93].

The Court therefore concluded that art. 24 and 32 GDPR cannot be interpreted as meaning that the unauthorised disclosure of personal data or unauthorised access by third parties is sufficient to establish that the measures taken by the data controllers were not appropriate (para 31, 39)[94]. If this were the case, the Court of Justice of the European Union stated, the irrefutable presumption that would result would be contrary to art. 5, 24, 32 and recital 74 GDPR, according to which controllers can demonstrate that the measures implemented are effective and comply with the Regulation (para 32, 34, 35). Furthermore, art. 82(3) GDPR also allows data controllers to demonstrate that they are in no way responsible for the event that caused the damage.

Turning to the Court's decision on the fourth question referred, it completely ignored the issue of identifying the nature of the liability system. It simply pointed out that, under art. 82 GDPR, the evidence must be strictly limited to proving that the damage is not attributable to the controllers (para 70)[95]; in the event of data breaches, data controllers must demonstrate their compliance with the obligations laid down in art. 32 GDPR (para 71), understood as proof of the absence of a causal link between the damage and their conduct, which allegedly violated the GDPR (para 72)[96].

The Court considered that this exemption from liability is consistent with the objective of the GDPR to ensure a high level of protection for data subjects, as set out in recitals 10 and 11 GDPR (para 73). In conclusion, the Court stated that even in cases where the damage results from the disclosure of data to unauthorised third parties, data controllers may be exempt from the obligation to pay compensation if they prove that they are in no way responsible for the event that gave rise to the damage in question (para 74).

Comment

[93] Confirmed with different reasoning in C-687/21, para 39.

[94] Confirmed in C-687/21, para 40.

[95] Confirmed in C-200/23, para 164 and C-741/21, para 51.

[96] Confirmed in C-200/23, para 165.

ISSN 2281-5147

In commenting on this judgment, it should first be noted that the CJEU issued its decision without addressing some of the arguments put forward by the AG[97]. Unfortunately, it is not possible to find arguments for or against many important positions taken by the AG, which would have been highly significant for a broader understanding of the issue.

Firstly, the Court interprets the meaning and scope of the provision in question as autonomous concepts to be interpreted uniformly across all Member States; to this end, it must read these provisions in light of their wording, objectives, and context. While the Advocate General is not referring to this specific method of interpretation, she reads these provisions in a similar way, providing a literal, systematic and teleological argument. For these reasons, the AG's arguments remain valid for an autonomous interpretation of the provisions in question.

The first preliminary question delves into the element of infringement, asking when art. 24 and 32 GDPR can be considered infringed; in its response, the AG clarified that these duties must be understood as obligations of means; therefore, the occurrence of damage is not sufficient to establish their infringement. The CJEU's response is largely in line with the AG's opinion; however, it omits significant details. Indeed, it did not repeat the key factors of the literal interpretation of art. 24 and 32 GDPR, namely the analysis of the state of the art and the criteria relating to implementation costs. Regarding the interpretation of implementation costs, given the concerns expressed, it is welcome that the Court of Justice of the European Union did not repeat this argument, which can therefore no longer be taken into consideration.

Regarding the state of the state-of-the-art factor, however, clarifications would have been necessary.

The AG interprets the concept of appropriateness of the measure (also) in terms of effectiveness of protection, in the sense that the measures must meet a certain level of qualitative acceptability. This level should be achieved by meeting the standard set

[97] M. Buzzoni, *One, Two, Three… Fault? CJEU Rules on Civil Liability Requirements under the GDPR*, cit., 3.

ISSN 2281-5147

by current knowledge (ie state of the art), with the consequence that only such measures could be considered as appropriate (para 26). Along the same lines, the AG stated that the objective of protection under the GDPR is to ensure the «best possible result in terms of effectiveness» (para 27). However, the AG considered that the reference to the state of the art implies that the required technological level of the measures would be limited to what is reasonably possible at the time of implementation (para 32).

These specifications were particularly relevant. Indeed, as explained above, the obligation to implement and demonstrate the appropriateness (and effectiveness within the meaning of recital 74 GDPR) of the measures has been interpreted by scholars as both an obligation of means and an obligation of result.

In this regard, if interpreted strictly, the concept of effectiveness is inextricably linked to that of result[98], with the consequence that the only appropriate measure would be one that actually prevented the breach. The only effective measure, indeed, is one that succeeded *ex post* in avoiding the damage.

However, the AG provided acceptable arguments for considering these duties as obligations of means. On the contrary, the Court did not elaborate on the criteria of state of the art and implementation costs[99]. It simply stated that, pursuant to recital 74 GDPR, data controllers are required to implement appropriate and effective measures and that such effectiveness must be demonstrated in accordance with the criteria set out in art. 24 and 32 GDPR[100]. The problem with this statement is that it is inconsistent with the other argument that the GDPR does not require the measure to be perfectly abstract, but only its concrete appropriateness to mitigate, as far as possible, the risks arising from the processing (C-340/21, para 30).

---

[98] «*Producing a result that is wanted: having an intended effect»,* "effective", in The Britannica dictionary. https://www.britannica.com/dictionary/effective <<last accessed: 22/07/2025>>; «*successful or achieving the results that you want»,* voce "effective", in Cambridge dictionary. https://dictionary.cambridge.org/dictionary/english/effective <<last accessed: 22/07/2025>>.

[99] S. Nusselder, *Security measures in the GDPR & the NAP judgement (340/21)*, cit., 5.

[100] P.G. Chiara, *The internet of things and EU law,* Springer, 2024, 170.

ISSN 2281-5147

Despite this misalignment, the Court was sufficiently clear in stating that measures could be considered appropriate even if breached, so the unjustified reference to effectiveness does not compromise the decision's meaning[101].

Furthermore, to reconcile the concept of effectiveness with this judgment and the entire Regulation, it can be understood as an attribute of the measure to be assessed *ex ante* only, when the measure is applied or updated. Judges and authorities should not assess it from an *ex post* perspective, since, if it were breached, it would be self-evident that it was not effective[102].

Moving on to the answer to the fourth referred question, the CJEU's response provides important arguments. Indeed, it clarified that the violation of the measure cannot be attributed to the data controller if the latter proves that it has fulfilled the obligations laid down in art. 32 GDPR (para 71); immediately afterwards, the Court stated that data controllers can also escape liability by demonstrating the absence[103] of a causal link between their conduct and the damage (para 72). Reading these two paragraphs together, it can be inferred that the Court essentially interpreted art. 32 GDPR as an obligation of means. The picture that emerges is as follows: art. 32 GDPR establishes obligations of means, thus requiring only the best efforts[104]. In the event of damage, the data controller may be exempt from liability by demonstrating that: i) it is in no way responsible for the event that caused the damage, by proving compliance with the standard set by art. 32 GDPR, *i.e.,* the appropriateness of the security measures in light of the criteria listed therein; ii) an external cause caused the

[101] Its importance is however not neglectable. Indeed, while recital 74 GDPR is not binding, this CJEU's decision that reads it in conjunction with articles 24 and 32 GDPR is directly enforceable within the Member States. On the effects of a CJEU preliminary ruling see C. Barnard, S. Peers (edited by), *European Union Law*, Oxford University Press, 2014, 291.

[102] Such interpretation is in line with the Italian one on dangerous activities under art. 2050 c.c., requiring to adopt all the adequate measures to prevent the damage, C.M Bianca, *La responsabilità*, Giuffrè Francis Lefebvre, 2021, 677.

[103] It was disputed whether the exempting proof shows the absence of the causal link, or, whether it breaks it. To this regard see J. Gardner, *Torts and other wrongs*, cit., 216.

[104] S. Nusselder, *Security measures in the GDPR & the NAP judgement (340/21)*, cit., 4.

ISSN 2281-5147

damage. In this way, the data controller demonstrates the absence/elision of the causal link.

This framework is reminiscent of a fault-based liability framework, in which each case is assessed individually, taking into account the criteria described in art. 32 GDPR[105].

This interpretation is entirely consistent with the principles of civil law generally accepted among EU Member States; therefore, this decision is well-suited to the harmonisation objective pursued by the European legislature through the GDPR and by the CJEU in this decision.

C-667/21

The issue of the nature of the liability regime was directly addressed in C-667/21 (fifth referred question), where it was asked whether the existence and/or proof of a fault or intent are necessary conditions to establish the data controller's liability under art. 82 GDPR.

The Advocate General's opinion

Particularly relevant to the analysis is the AG's opinion, according to which the civil liability regime established by the GDPR is not subject to the existence or proof of intent or fault, resulting in a strict liability regime. The AG put forward several arguments: one literal, another based on the preparatory work for the GDPR, one teleological, and one systematic.

Starting with the literal argument, it obviously focused on art. 82(1) GDPR, which, the AG observes, links compensation only to the damage suffered by data subjects as a result of a breach of the Regulation, regardless of other elements such as fault (para 74).

It is also noted that where the legislature wanted to require an assessment of fault, it did so readily; for example, the AG remarked that art. 83 GDPR explicitly mentions fault as an element to be assessed when estimating administrative fines (para 77). For

[105] F. Castagnari, *On the responsibility of the Financial Administration as "data controller" in the event of a data breach due to a "hacker attack" by third parties: critical and systematic profiles*, cit., 5-6.

ISSN 2281-5147

these reasons, the AG concluded that a literal interpretation tends to exclude fault from the conditions for establishing compensation under art. 82 GDPR. Despite this statement, the AG noted that the lack of consistency in the Regulation's wording renders literal interpretations less persuasive (para 78).

The AG's argument, based on the preparatory work for the GDPR, highlighted only two specific passages: first, an amendment tabled in the Parliament's Committee on Civil Liberties, Justice and Home Affairs, which sought to link liability to intent or negligence, but was not adopted (para 83). Secondly, a choice between two options, agreed by the Council, for the criterion for attributing liability in data processing activities involving several persons. The first option provided for a model similar (but certainly not equal) to the principle of liability follows fault (para 84). The second option, instead, would have imposed on art. 82 GDPR, the inevitable obligation to compensate the data subject for the full amount of the damage, in the form of absolute liability, as no exemption was provided for (para 84). The first option was followed by the Council, which used it as the basis for the compromise text presented and implemented it by making the exemption rule more stringent: «... if ... it proves that it is not *in any way* responsible ...». This wording was subsequently approved (para 85). For these reasons, the AG concluded that even from an analysis of the preparatory work for the GDPR, it cannot be inferred that the liability regime provided for in art. 82 GDPR involves the element of fault (para 86).

Turning to the teleological argument, the AG observed that, according to recital 10 GDPR, the Regulation aims to ensure a high level of protection for natural persons while removing obstacles to the flow of personal data; in this context, art. 82 GDPR primarily pursues a compensatory function (para 87). From this, the AG deduced that ensuring full and effective compensation is an objective in itself and a right of the injured data subject (para 88). The right to compensation, the Court added, is linked to the objective of strengthening citizens' trust in the digital environment, which is expressly recognised in the GDPR (recital 7). To that end, ensuring that data subjects do not have to suffer the consequences of damage resulting from the unlawful processing of their data promotes such trust: «their assets are protected and, procedurally, their claims are more straightforward» (para 89). The fact that art. 82 GDPR does not require a breach of a duty of care, is consistent with this, and,

ISSN 2281-5147

according to the AG, it is consistent with the aforementioned objective of the Regulation (para 90).

Subsequently, the AG emphasised that what really matters for the purposes of compensation is the situation of the victim: it is irrelevant to the latter whether the wrongdoer acted intentionally or in fault; as long as the victim has suffered damage causally linked to the breach of the GDPR, they are entitled to claim compensation under art. 82 GDPR (para 91, 92).

The final argument analysed the entire GDPR scheme. In this case, the AG argued that a fault-based civil liability model promotes diligence and, therefore, protection against risks, while the alternative model, which does not take into account the behaviour of the parties, would discourage them from taking action (because, in the event of damage, they would still have to compensate for it) (para 99). The AG considered this result acceptable on the basis that art. 82 GDPR is part of a complex regulatory framework comprising public and private legal instruments for the protection of personal data. Within that regulatory framework, fault and intent are relevant only for determining administrative penalties; it is not necessary to make them relevant to civil liability. Indeed, the resulting fault-based liability would not be consistent with the objectives pursued by art. 82 GDPR (para 100).

To conclude, it is significant that the AG added that the actions of the data subjects may, depending on the circumstances, break the causal link between the infringement and the damage (para 110).

The CJEU's decision

Moving on to the CJEU ruling, it started by recalling the three conditions required to establish compensation under art. 82 GDPR: infringement, causal link and damage.

It then compared the wording of the Regulation's different versions (German, French, Finnish, Spanish, Estonian, Greek, Italian, and Romanian), seeking to establish whether, under art. 82(2) GDPR, any data controller involved in processing activities should be held liable for damage caused by other participants in that processing (para 91). According to the results of this comparison, the first sentence of art. 82(2) GDPR would presuppose that the controllers have participated in the unlawful processing

ISSN 2281-5147

(para 92)[106]. This was particularly evident in the Spanish[107], Estonian[108], Greek[109], Italian[110] and Romanian[111] language versions, where the provision refers to his/her processing, rather than to a general processing activity (para 92)[112].

Based on this assumption, the CJEU stated that art. 82 GDPR provides a fault-based liability regime, which allows the possibility of always proving that the controllers are not responsible for the damage, even if they are presumed to have participated in the unlawful processing (para 93, 94).

The Court continued with a contextual reading of art. 82(3) GDPR. It combined art. 82(3) GDPR with art. 24 and 32 GDPR, as interpreted by the Court itself in C-340/21, thus simply requiring the data controller to take technical and organisational measures to prevent, as far as possible, any personal data breaches (para 96). From this interpretation, the CJEU derived that art. 82 GDPR provides for fault-based liability in which the burden of proof lies with the data controllers (para 94).

From the teleological interpretation that reads art. 82 GDPR in conjunction with recitals 4 to 8 GDPR, the Court assessed the balance between the interests of data controllers and the rights of data subjects enshrined in the Regulation (para 98) and, as the AG, considered that this compromise was established to promote the

[106] Confirmed in C-741/21, para 46.

[107] «Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente Reglamento».

[108] «Kõnealuse töötlemisega seotud vastutav töötleja vastutab kahju eest, mis on tekkinud sellise töötlemise tulemusel, millega rikutakse käesolevat määrust».

[109] « Κάθε υπεύθυνος επεξεργασίας που συμμετέχει στην επεξεργασία είναι υπεύθυνος για τη ζημία που προκάλεσε η εκ μέρους του επεξεργασία που παραβαίνει τον παρόντα κανονισμό».

[110] «Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento».

[111] «Orice operator implicat în operaţiunile de prelucrare este răspunzător pentru prejudiciul cauzat de operaţiunile sale de prelucrare care încalcă prezentul regulament».

[112] On the contrary, other versions of the GDPR, in particular the German, French and Finnish ones, are worded in a more open manner, not allowing for a proper answer to the question (para 92).

ISSN 2281-5147

development of the digital economy while ensuring the protection of the rights of data subjects. Along the same lines, it argued that a fault-based liability system, accompanied by a reversal of the burden of proof as provided for in art. 82 GDPR would be the most appropriate legal instrument to implement that balance (para 98).

The Court then recalled the AG's observation that it would not be consistent with the objective of the GDPR to ensure a high level of protection of personal data to require data subjects to prove, in addition to the breach and the damage suffered, the existence of fault on the part of the controller (para 99). Indeed, the Court emphasised that art. 82 GDPR does not provide for such a requirement, thus limiting the burden of proof on data subjects to the three necessary conditions (breach, damage and causal link).

In conclusion, the Court stated that the determination of the controller's liability is subject to the existence of fault, which is presumed to exist unless the controller proves that she is in no way responsible (para 103)[113].

Comment

In commenting on this judgment, it should be noted that, once again, the CJEU issued its decision without any reference to the AG's opinion. In this case, however, the contrasting conclusions in the opinion and the decision highlight the need for coordination between them.

Both the opinion and the judgment can be considered incomplete, and the fact that they reached different conclusions is not surprising; despite this divergence, however, they are still reconcilable.

The AG's interpretation, which considered a strict liability regime, is perfectly in line with its reasoning, which focused entirely on art. 82 GDPR; on the other hand, the CJEU interpreted art. 82 GDPR in conjunction with the provisions establishing evidentiary duties, mainly art. 24 and 32 GDPR[114], arguing for fault-based liability.

[113] Confirmed in C-687/21, para 52; joint cases C-182/22 and 189/22, para 28; C-200/23, para 154.

[114] It should be highlighted that the referred question was related only to art. 82 GDPR.

ISSN 2281-5147

Both decisions are acceptable when read individually. What is missing in this case is an assessment of the entire liability regime provided for in the Regulation.

Focusing on the CJEU's decision, it firstly declared the fault-based liability regime based on the combination of paragraphs 2 and 3 of art. 82 GDPR, resulting in a presumption of fault on the part of data controllers.

Against this latter argument, the mere possibility of proving one's non-liability does not necessarily imply fault-based liability. Indeed, in general, even strict liability regimes provide a way out, albeit more limited than that available in fault-based systems[115]. Therefore, the exemption clause provided for in art. 82(3) GDPR should only be interpreted as a reason to exclude an absolute liability regime[116].

The main problem is that the entire GDPR liability system cannot be understood on the basis of art. 82 GDPR alone, and this was the mistake made by the AG, who did not take into account the rest of the regulation.

The liability regime should derive from a combination of art. 82 GDPR, intended as the general rule of liability in the GDPR, and the specific obligation deemed to have been breached, as is the case in most European private law systems. Indeed, in the absence of a clear statement by the European legislature, the entire apparatus should be taken into consideration. In this regard, the classic distinction between obligations of means and obligations of result, along with the related liability regimes, could be very useful for identifying the specific scheme in question.

Nevertheless, the Court's ruling remains acceptable, as it adopted a fault-based liability system linking art. 82 GDPR to art. 24 and 32 GDPR, which, as discussed above, could be interpreted as obligations of means.

However, neither the AG nor the Court analysed the different consequences for liability[117]. The Court's decision interpreted art. 82 GDPR only in conjunction with those provisions that are considered to impose obligations of means, for which fault-

[115] European Group on Tort Law, *Principles of European Tort Law* (Text and Commentary), cit., 102.

[116] R. Strugala, *Art. 82 GDPR: Strict Liability or Liability Based on Fault?*, cit., 74.

[117] M.J.S. Moròn, *Reflexiones en torno a la jurisprudencia del TJUE sobre la acción indemnizatoria del art. 82 RGPD (asuntos C-300/21; C-340/21; C-456/22; C-667/21; C-687/21; C-741/21)*, cit., 1420.

ISSN 2281-5147

based liability is considered acceptable[118]. Conversely, it did not discuss whether the liability regime remains the same for obligations of result[119], such as the obligation to follow data controllers' instructions under art. 29 GDPR, or the obligation to notify the Data Protection Authority under art. 35(1) GDPR, where there is no standard of conduct to be observed.

Furthermore, causation was barely addressed, leaving it as an empty concept within the GDPR.

Due to these omissions, the Court's decision appears incomplete rather than incorrect. It should be clarified, however, that even if the Court could have completed its reasoning by referring to the obligations of result or causation, it was not asked to do so. Indeed, the Court was asked only about the role of fault, while nothing was questioned about the obligations of result or strict liability regimes. In conclusion, the Court's decision is correct but still insufficient to account for the entire liability system.

C-687/21

The decisions issued in C-340/21 and C-667/21 were confirmed in C-687/21 (third, fourth and sixth referred questions), where the Court was asked, in essence, whether art. 5, 24, 32 and 82 GDPR (read together) must be interpreted as meaning that the disclosure of a printed document containing personal data to an unauthorised third party, realised by a company (data controller) through its employees, signifies that the technical and organisational measures required by art. 24 and 32 GDPR were not 'appropriate'.

---

[118] M.C. Vergès, *El concepto autònomo de responsabilidad civil en el àmbito de la protecciòn de datos personales en la era digital: anàlisis del artìculo 82 del regolamento 2016/679*, cit., 266; M.J.S. Moròn, *Reflexiones en torno a la jurisprudencia del TJUE sobre la acción indemnizatoria del art. 82 RGPD (asuntos C-300/21; C-340/21; C-456/22; C-667/21; C-687/21; C-741/21)*, cit., 1418.

[119] J. Eckhardt, M. Hansen, *Die Datenschutzrechtliche Verkehrssicherungspflicht*, in DuD, Datenschutz und Datensicherheit, 9/2024, 563.

ISSN 2281-5147

The Court addressed this issue by explicitly confirming the fault-based liability system described in C-667/21 (para 52)[120]. The CJEU recognised that the disclosure of data may indicate that the technical and organisational measures implemented were not appropriate within the meaning of art. 24 and 32 GDPR, for example, due to fault or a shortcoming in the organisation of the data controller (para 41). It continued by remembering that data controllers are only required to prevent data breaches as far as possible (para 30) and, from a combined reading of art. 5, 24, 32 and recital 74 GDPR, it stated that data controllers can always demonstrate that personal data have been processed in a manner that ensures appropriate security within the meaning of art. 5 and 32 GDPR (para 42).

For these reasons, confirming what has already been established in previous judgments, the CJEU answered to the referred questions by establishing that, pursuant to art. 5, 24, 32, 83 and recitals 74 and 76 GDPR, the fact that the controller's employees mistakenly provided a document containing personal data to an unauthorised third party is not sufficient, in itself, to consider the technical and organisational measures implemented by the controller as non-appropriate within the meaning of art. 24 and 32 GDPR (para 39, 45).

For this paper, this decision simply confirmed previous judgments, reading art. 82 GDPR in conjunction with the provisions imposing evidentiary obligations, which the Court implicitly treated as obligations of means. Furthermore, also in this case, the causal link was only mentioned.

Overall, this decision did not develop into the issue analysed by the previous rulings, but it is nevertheless helpful in highlighting the consolidation process of the Court's case-law on this matter.

C-741/21

Moving on to C-741/21 (second preliminary question), the Court of Justice of the European Union was asked whether, in order to be exempt from liability under art. 82(3) GDPR, it is sufficient for data controllers to demonstrate that the damage was

[120] S. Nusselder, *Security measures in the GDPR & the NAP judgement (340/21)*, cit., 6.

ISSN 2281-5147

caused by someone else acting under their authority within the meaning of art. 29 GDPR.

This judgment is beneficial for the current analysis because, as will be shown, it provides an opportunity to demonstrate what exercise the court should have carried out to interpret the liability exemption clause provided for in art. 82(3) GDPR.

In support of its answer, the Court confirmed the statements made in C-667/21, namely that art. 82 GDPR provides for a fault-based liability regime, under which data controllers are presumed to have participated in the unlawful processing activity with fault, with the burden of proof resting on them (para 46).

Reading art. 29 and 32(4) GDPR together, the Court emphasised that data controllers must take specific measures to ensure that authorised persons acting under their authority access and process personal data only in accordance with their instructions (para 47 and 48). The Court concluded that it is for data controllers to ensure that their instructions are correctly followed and applied, so that they cannot simply exonerate themselves from liability by invoking the fault of someone else acting under their authority (para 49). Indeed, the Court emphasised that controllers could only be exonerated if they proved that those acting under their authority had not followed the instructions given and that they (the controllers) had fulfilled their obligations. As explained by the Court, if they violated the GDPR, in particular art. 24, 25 and 32 GDPR, causing the violation committed by those acting under their authority, they will be liable and will have to compensate for the damage (para 50). The Court reiterated that data controllers cannot escape liability merely by demonstrating that they have issued instructions to those acting under their authority, as required by art. 29 GDPR (para 51 and 52)[121]. They must, indeed, demonstrate that there is no causal link between the breach of their obligations under art. 5, 24 and 32 GDPR and the damage suffered by the data subjects (para 51).

If this were not the case, the Court noted, and controllers were exempt from liability simply by demonstrating that the damage was caused by someone else under their authority, the right to compensation would be significantly and negatively affected,

[121] Confirmed in C-200/23, para 165, 166.

ISSN 2281-5147

and would not be consistent with the objective of the Regulation to ensure a high level of protection for data subjects (para 53)[122].

In conclusion, the CJEU ruled that art. 82 GDPR must be interpreted as meaning that it is not sufficient for data controllers to demonstrate that the damage was caused by those acting under their authority within the meaning of art. 29 GDPR (para 54).

Comment

The decision confirmed that art. 82 GDPR provides for a fault-based liability regime, as stated in C-667/21, without elaborating on it; however, while in C-667/21 the Court of Justice of the European Union was specifically asked to rule only on the role of fault, in C-741/21 it had greater freedom to address the entire issue of the nature of the liability regime.

The Court adopted fault as the sole criterion for liability, linking it only to art. 82 GDPR, whereas in previous decisions, art. 82 GDPR was understood as a fault-based liability system partly because it was read in conjunction with art. 24 and 32 GDPR.

This combination of provisions is of utmost importance. Indeed, it is in these provisions (art. 24 and 32 GDPR) that a reference to the standard of conduct can be found, and not in art. 82 GDPR considered alone (as stated also in C-667/21, para 90).

The fact that in C-667/21 the Court gave priority to the element of fault is due to its combined reading of art. 82 and 32 GDPR. In C-741/21, on the other hand, art. 82 GDPR was interpreted as establishing a fault-based system in its own (in para 46, the Court considered only the combination of paragraphs 1 and 2, referring to C-667/21).

Moving on to the motivations, the Court responded to the question referred by stating that data controllers must demonstrate the absence of a causal link between the damage and the breach of art. 32 GDPR (para 51, referring to C-340/21), and that it is not sufficient to demonstrate that instructions have been given[123]. However, in this case, the obligation in question is not that provided for in article 32(1) GDPR (*i.e.* to

[122] Confirmed in C-200/23, para 175.

[123] M.C. Gamito, H.-W. Micklitz, *EU consumer law in 2023*, in Annuaire de droit de l'Union Europèenne, 2023, 13.

ISSN 2281-5147

implement appropriate security measures in light of specific criteria), but that laid down in article 32(4) GDPR, according to which controllers must take steps to ensure that any natural person acting under their authority processes data only in accordance with their instructions. The Court referred to the decision in C-340/21, omitting to mention that the latter concerned the obligation to implement appropriate measures under art. 32(1) GDPR, whereas the case in question concerns art. 32(4) GDPR. While, in C-340/21, the Court implicitly interpreted the obligation to implement appropriate security measures as an obligation of means, in C-741/21 no reference is made to the nature of the obligations under art. 32(4) GDPR.

However, the aim of identifying the correct exonerating evidence can be pursued only by determining the nature of that obligation. This interpretative effort should be conducted in accordance with the case law of the Court of Justice of the European Union, which holds that terms contained in provisions that do not refer to the law of Member States must be interpreted autonomously and uniformly, based on their wording, context, and objectives. Since art. 32 GDPR never delegates the interpretation of the concepts contained in the provision to Member States, its terms must be interpreted as autonomous concepts.

With regard to the wording, art. 32(4) GDPR requires controllers to «take steps to ensure…». This terminology resembles a strict order; in other provisions, the EU legislator has made it clear that only reasonable steps/efforts are required, for example, in art. 17(2) GDPR[124]. From this difference in wording, it could be inferred that the provision is intentionally designed to impose a strict command rather than to require best efforts. This reading tends to interpret art. 32(4) GDPR as an obligation of result, to be linked to a regime of strict liability according to the most agreed principles of tort law across the EU.

Moving to the context, it should be noted that data controllers are presumed to be responsible for unlawful processing under art. 82(2) GDPR, while data processors are only held liable in specific situations indicated in the Regulation (art. 28 GDPR). Conversely, persons acting under the authority of data controllers are not subject to a particular regime of liability under the GDPR. The fact that controllers are presumed to be liable by default, while other actors are liable only in certain situations, suggests

[124] See also art. 5(1)(d), art. 8(2) GDPR, art. 14(5)(b).

ISSN 2281-5147

that the objective of the provision is to place the burden of breaches outside these exceptional scenarios on the controller, as they are the fulcrum of liability for unlawful processing activities.

These three arguments point to a strict liability regime, as the content of the obligation appears to require a specific result. This result is also supported by the doctrine that data controllers are liable for breaches committed by their employees/auxiliaries[125].

Finally, another element supporting a strict liability regime lies in the most widely accepted interpretation of auxiliaries' liability in the private law systems of Member States[126]. This doctrine, supported by the PETL and the DCFR, understood this as a strict liability regime in both tort and contractual contexts[127].

It is worth noting that, historically, Germany has been an important exception, basing employee liability on fault[128].

Based on this interpretation of the content of art. 32(4) GDPR, and linking it to art. 82(3) GDPR, it should be concluded that exonerating evidence cannot be the absence of fault understood as the adoption of specific diligence, as implied by the CJEU decision. Rather, the exonerating evidence should be an event beyond the data

---

[125] B. Van Alsenoy, *Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation*, cit., 282; C. Millard, D. Kamarinou, *Article 29. Processing under the authority of the controller or processor*, in Kuner C., Bygrave L. A., Docksey C., Drechsler L., *The EU General Data Protection Regulation (GDPR): A Commentary,*2020, 614.

[126] P. Giliker, *Vicarious liability in tort*, Cambridge university press, 2010; more recently, P. Giliker, *Comparative law and legal culture: placing vicarious liability in comparative perspective*, in Chinese journal of comparative law, 6(2)/2018; U. Magnus, *Tort law in general*, in *Elgar Encyclopedia of Comparative Law*, cit., 881.

[127] The liability of auxiliaries in the context of contracts is relevant because of the contractual relationship between controllers, processors and authorised individuals, as prescribed by art. 28(3)(b) GDPR.

See C. von Bar, E. Clive, H. Schulte-Nölke (edted by), *Principles, Definitions and Model Rules of European Private Law: Draft Common Frame of Reference (DCFR)*, cit., 3323; European Group on Tort Law, *Principles of European Tort Law* (Text and Commentary), cit., 116.

[128] See P. Giliker, *Vicarious Liability or Liability for the Acts of Others in Tort: A Comparative Perspective*, in Journal of European tort law, 2(1)/2011.

ISSN 2281-5147

controller's control that breaks the link between the damage and the activity enacted by the auxiliaries.

Furthermore, art. 32(4) GDPR and the related art. 28(3)(b) GDPR do not describe any form of conduct to be complied with, contrary to art. 32(1) GDPR, which lists specific parameters to guide the conduct of data controllers.

For these reasons, this decision does not appear to be sound. It does not adequately explain the nature of the liability regime and, at the same time, does not investigate the alleged obligation that has been breached. In light of the above arguments, the exonerating evidence should have been only *force majeure*, the event caused by the data subject or the liability of the data processor (if appointed).

Furthermore, unfortunately, it did not delve into the investigation of causality (both factual and legal), so there would still be no indication of how to determine whether a given event could break the causal link.

To conclude, the interpretation that reads art. 82 (paragraphs 2 and 3) GDPR as presuming the fault of data controllers, without an inquiry over the nature of the duty breached, was subsequently confirmed without further developments in joined cases C-182/22 and C-189/22[129], and in C-200/23[130], highlighting the consolidation of this case-law.

4. Conclusions

This paper seeks to show that, if analysed independently, the CJEU's decisions might appear correct, whereas viewed from a broader perspective they are far from undisputable. The CJEU, however, was never asked to consider the GDPR's entire liability regime. The questions referred constrained the Court's decisions to narrow inquiries, preventing proper, complete analyses.

In the introduction to this paper, it was suggested that a useful compass for guiding the harmonisation of data protection liability, particularly concerning the liability

[129] Para 28.

[130] Para 154, 161, 162, 163.

ISSN 2281-5147

exemption clause, could be found in the principles of tort law most widely accepted among the Member States. The Court should have compared the structure of the Regulation to the traditions commonly embraced by the Member States, and, in case of compatibility between the two, it should have interpreted those GDPR provisions in light of such traditions, at least for what concerns the elements not addressed in the GDPR, such as the nature of the liability regime and the consequent exonerating evidence.

This paper argues that, in light of the harmonisation purpose of the GDPR and the CJEU, the GDPR should be interpreted as entangling two different liability regimes: a fault-based one for the obligations of means, mainly art. 24 and 32(1) GDPR, and a strict liability regime for the obligations of results, such as art. 32(4) GDPR. Concerning the respective exonerating evidence, while for the former even the respect of the standard of conduct described in the provision proves the absence of the infringement, the latter requires proving the elision of the causal link because of an event beyond control, such as *force majeure* or error on the part of the data subject. In other cases, instead, the link is missing in the first place, for instance, when the data processor's liability under art. 82(2) GDPR is triggered.

This interpretation of art. 82 GDPR is suggested because it reflects the most widely accepted tort law principles across the EU. Consequently, it can facilitate the harmonisation of the EU legal systems.

The Court, instead, proceeded differently, ignoring the legal scholarship that highlighted the importance of identifying the obligations' nature for the purpose of determining the nature of the exempting proof[131].

In C-340/21, indeed, the Court, consistent with its typically concise style of reasoning[132], did not engage in conceptual distinctions, such as that between obligations of conduct and obligations of result. However, it reasoned accordingly,

[131] B. Van Alsenoy, *Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation*, cit., 273.

[132] «A specific example where a form of 'hybridisation" that can be observed are the judgments of the Court of Justice of the EU (CJEU). Its concise style of reasoning is akin to French courts, but it also uses a common-law style of relying on precedents and, in substance, has made use of some German concepts, such as the principle of proportionality», M. Siems, *Comparative law*, cit., 287.

ISSN 2281-5147

holding that art. 24 and 32 GDPR merely require controllers to take only the measures that can, as far as possible, prevent data breaches (para. 30). Moreover, the Court clarified that compliance with the evidentiary duties enshrined in those provisions is sufficient to demonstrate the absence of liability under art. 82 GDPR (paras. 71–72). This reasoning was subsequently confirmed in later judgments, which expressly invoked the notion of fault. This framework, in which obligations describing a standard of conduct require only what is reasonably possible, in combination with a liability regime grounded in fault, reflects the traditional doctrines common to most Member States, thereby facilitating the harmonisation objective pursued by both the GDPR and the CJEU. However, although the Court reaffirmed in subsequent decisions that liability is fault-based, it did not always reiterate the reasoning advanced in C-340/21 and C-667/21.

Since the decision in C-667/21, indeed, the Court has adopted the fault criterion, also on the basis of the presumption read into art. 82(3) GDPR, according to which data controllers can always prove they are not responsible for causing the damage, even if they are presumed to have participated in the unlawful processing (para 93, 94).

As explained, this argument is questionable; indeed, the fact that from the interpretation of art. 82 GDPR data controllers can always prove to be not liable, even if they are presumed to have participated in the processing, does not mean that the Regulation provides for a liability system based on fault. The exempting clause provided for by art. 82(3) GDPR merely precludes an absolute liability system, which is insufficient to determine whether the system is based on fault[133].

This argument was applied in C-741/21 (para 46), where the Court did not consider the nature of the obligation at issue (responsibility over auxiliaries), concluding for a fault-based liability system for a duty interpreted by most of the EU Member States as imposing an obligation of result, linked to a strict liability regime[134].

[133] U. Magnus, *Tort law in general*, in *Elgar Encyclopedia of Comparative Law*, cit., 881.

[134] P. Giliker, *Vicarious liability in tort*, cit.; more recently, P. Giliker, *Comparative law and legal culture: placing vicarious liability in comparative perspective*, cit.; U. Magnus, *Tort law in general*, in *Elgar Encyclopedia of Comparative Law*, cit., 881.

ISSN 2281-5147

The analysis of C-741/21 remarked that for these kinds of obligations it would be impossible to find a standard of conduct on which to assess the presence/absence of fault, and, provided that most of EU legal systems historically linked obligations of result with strict liability rules, the decision issued in C-741/21 risks transplanting an unfamiliar rule into them.

Therefore, it is suggested that the CJEU observes and applies the most widely accepted tort law principles across the Member States, thereby evaluating the nature of the obligation at issue so as to identify the exempting proof required.

The decision in C-741/21 is in marked contrast to the intent to interpret the terms of art. 82 GDPR, and its exempting proof (derived from the combination of different provisions not referring to the law of Member States), as autonomous concepts in a uniform way across the Member States. Indeed, it moves away from the common traditions of EU tort law, which combine liability based on fault with obligations of means, and strict liability with obligations of result[135]. In conclusion, this interpretation of art. 82 GDPR could undermine the Court's harmonisation process.

The final picture outlined by the CJEU reflects a double divergence: i) between the traditional scholarship focused on the GDPR, prone to read art. 82 GDPR as imposing a strict liability regime[136], and the CJEU jurisprudence, establishing a fault-based liability system; and ii) between such case-law and the Member States' private law traditions, linking liability based on fault with obligations of means, and strict liability with obligations of result.

[135] F. Werro, E. Buyuksagis, *The bounds between negligence and strict liability*, cit., 207; M. Cappeletti, *Justifying strict liability: a comparative analysis in legal reasoning*, cit., 14; M. Bussani, A.J. Sebok, M. Infantino, *Common law and civil law perspectives on tort law*, cit., 43; U. Magnus, *Tort law in general*, in *Elgar Encyclopedia of Comparative Law*, cit., 880.

[136] *Ex* multis, see R. Strugala, *Art. 82 GDPR: Strict Liability or Liability Based on Fault?*, cit.; G. Zanfir-Fortuna, *Article 82. Right to compensation and liability*, cit.; E. Tosi, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, cit., 2019; S. Li, *Compensation for non-material damage under Article 82 GDPR: a review of case C-300/21*, cit., 336.

ISSN 2281-5147

Furthermore, the CJEU has not yet taken a position on the causal link, most likely because Member States' theories of causation still differ significantly (at least for the legal/policy inquiry)[137].

Therefore, national courts will still apply their own causation mechanisms to determine whether the proof demonstrates the absence of causation.

To conclude, in the attempt to contribute, this work suggests interpreting the missing elements of the liability exemption established by art. 82(3) GDPR through the lens of the most widely accepted tort law principles among the Member States, in particular in relation to the burden of proof. This would favour a similar interpretation of the relevant terms and concepts across the Member States. In doing so, the CJEU could enhance the level of harmonisation, given the familiarity of the Member States with these principles. Conversely, it would be difficult to imagine how Member States could approach foreign concepts, such as the fault's assessment for obligations of result.

Finally, it should be noted that, although this work has referred to common principles in the EU regarding strict and fault-based liability systems, these concepts, despite the common terminology, are indeed not always equally interpreted across the Member States[138]. For instance, the legal inquiry into fault in Germany is highly particular within the EU framework[139]; furthermore, the distinction between obligations of means and of results is more articulated in France than in other countries, such as Italy[140].

[137] M. Infantino, E. Zervogianni, *Unravelling causation in European tort laws*, cit., 649-650, 672.

[138] M. Siems, *Comparative law*, cit., 5.

[139] European Centre of Tort and Insurance Law, *Unification of Tort Law: Fault*, Kluwer Law International, The Hague, 2005, 103 ff.

[140] The French legal scholarship distinguishes between *obligations de moyens renforcées* and *obligations de résultat atténuées*, see M. Fabre-Magnan, *Droit des obligations. 1. Contract et engagement unilateral*, PUF, Thémis droit, 7° edition, 2024, 632.

ISSN 2281-5147

Therefore, this work recognises that understanding these notions will, in any case, depend in part on national factors[141]; thus, their harmonisation is only partially possible, given their inherent national dimension[142]. Nevertheless, when the CJEU rules, its judgments harmonise, and, under certain conditions (a legal tradition sufficiently shared across the Member States), comparative law can provide a reliable means of guiding this process, thereby avoiding the transplanting of legal irritants, as described in this article.

[141] M. Siems, *Comparative law*, cit., 121.

[142] H.-W. Micklitz, *The full harmonization dream*, in Journal of European consumer and market law, 4(11)/2022.

ISSN 2281-5147

"SECTION II"

SPECIAL ISSUE

Towards a multilevel and interdisciplinary assessment for a safer use of digital services and AI-based products

Edited by D. Amram, C. Novara, M. Ratti

ISSN 2281-5147

INTRODUCTION TO THE SPECIAL ISSUE ON "TOWARDS A MULTILEVEL AND INTERDISCIPLINARY ASSESSMENT FOR A SAFER USE OF DIGITAL SERVICES AND AI-BASED PRODUCTS"

Denise Amram, Cinzia Novara, Matilde Ratti

Abstract

This is a short introduction to a special issue resulting from research conducted in the last two years, dealing with the development of a multilevel assessment for digital services and AI-based products with the lenses of children's rights.

Keywords

Digital services – AI Systems – Children's Rights.

Introduction

In the last years, the EU Commission approved a series of legislative initiatives aiming to address the fundamental rights and societal values within the new mechanisms imposed by the digitalisation of services and products.

Starting from the approval of the EU Regulation n. 2016/679 on General Data Protection Regulation, pursuing to the EU Regulation n. 2022/2065 on Digital Services Act, and the EU Regulation n. 2024/1689 on AI Act, the so-called risk-based approach has become part of the current compliance procedures both for private organisation and public institutions. This encouraged an interdisciplinary dialogue aiming to translate into organisational and technical measures considering the level of protection and the nature of the activities carried out on a case-by-case basis.

ISSN 2281-5147

At the same time, users are required to develop tailored technical and soft skills to become everyday more aware and responsible consumers, or data subjects, or users of a given digital service or product.

In this complex context, we decided to investigate the urgency to take in due consideration the vulnerabilities that especially younger users may face every day, while dealing with new technologies and / or within the digital environment.

The initial legal challenge immediately required to be completed by an interdisciplinary approach, opening to the psycho-educational and relational dynamics in order to better address the stratification of possible scenarios and the corresponding implications both in terms of risks and opportunities and policy-making contribution. Users, in fact, may play a proactive role, or being just a passive character, depending on the nature of the given service or product, on the age, grade of autonomy, personal skills and competence, and also on the relational and educational frame they are living in.

Our research dealt with the analysis of the regulatory framework to be compared with practical scenarios and empirical data generated through tailored participatory activities. From the multilevel assessment, interpretative gaps and enablers allowed to draft and validate policy and recommendations for a safer use of digital services and products applied to different stakeholders - including policy-makers, professionals, economic operators, families, and the target group (*i.e.* children) - considering the ethical-legal-technical frameworks, as well as the needs emerging from the psycho-educational domain.

The first paper of this special issue illustrates and comments the developed policies and recommendations under a comparative law perspective (N. Patti, V. Punzo, R. Romano "*Child Vulnerability in the Digital Environment: Comparative Insights and Operational Guidelines*"). In addition, in order to extend the open discussion on the project outcomes, we collected a series of articles selected through a call for papers launched within the project life-cycle among the relevant scientific communities.

We selected proposals concerning possible comparative and private law perspectives addressed both to the economic stakeholders (services providers, digital platforms, AI-based systems developers and deployers), and to the target group (children) and their families, dealing with the empowerment of children's fundamental rights (S.

ISSN 2281-5147

Rigazio "*Yes, We Can.. and We Must! Changing the Narrative of Children's rights Protection in the Digital Environment through a Child-Centred Approach. The lesson From the UK Children's Code*"), looking also at the contractual dimension of private law relationships (A. Jaci "*Minors' Contractual Autonomy in the Digital Ecosystem: Legal Protection and Self-Determination in Private Law*"), and the playful one (F. Casarosa – L. Vizzoni "*Let's play together: fair rules for minor video gamers*"). Finally, the fourth paper deals with the life-cycle design of an AI-based product, providing insights from an ethical-legal and technical perspective (S. Tibidò, N. Spatari, S. Lilli, and M.V. Zucca "*A Story of and for Children: The Lifecycle Loop of Child Rights-Based AI*").

The special issue is completed with a systematic reconstruction of the challenges faced and the methodologies developed in the project, oriented to properly review the legal measures adopted at international, European, and national levels for children's protection in the digital environment, with specific regard to the use of AI (M. Ratti "*Il minore nell'era dell'intelligenza artificiale: questioni aperte sul metodo di gestione del rischio*").

We are grateful to all the contributors as they raised original analysis to propose interpretations for a safer digital environment and a more responsible use of new technologies, by encouraging actions aiming to promote and enhance children's rights.

Acknowledgements

This special issue has been developed in the context of the project titled *Children as vulnerable users of IoT and ai-based technologies: a multi-level interdisciplinary assessment* (CURA), funded by the Italian Ministry of University and Research under the PRIN 2022 programme – Next Generation EU; CUP: J53D23005540006.

ISSN 2281-5147

ISSN 2281-5147

CHILD VULNERABILITIES IN THE DIGITAL ENVIRONMENT: COMPARATIVE INSIGHTS AND OPERATIONAL GUIDELINES

Nicoletta Patti, Veronica Punzo, Roberta Romano*

Abstract

The article investigates the condition of child vulnerability in the digital environment through a legal and comparative lens, aiming to reconcile protection with the recognition of children's evolving capacities. Embracing the concept of vulnerability as a dynamic and multilayered notion, it analyses how European regulatory instruments such as the GDPR, the Digital Services Act and the Artificial Intelligence Act address children's rights within a risk-based governance framework.

The discussion is enriched by a comparative analysis of the United Kingdom and France, whose regulatory models offer advanced examples of child-centred and participatory digital regulation. Particular attention is devoted to the online search for origins by adopted minors, a paradigmatic case where digital exposure intersects with identity-related and emotional vulnerability.

Building on these insights, the paper formulates operational guidelines and policy recommendations directed at legislators, institutions, professionals, and industry actors. Ultimately, it argues that digital literacy and education constitute the cornerstone of a rights-based approach capable of transforming child vulnerability into agency and fostering a genuinely inclusive digital citizenship.

* This paper is the result of a common research and reflection of the authors. However, within the scope of research evaluations, Nicoletta Patti drafted Sections 1, 2, 3, 4; Roberta Romano drafted Sections 5, 5.1, 6 and Veronica Punzo, Sections 7, 8, 9. The conclusions were co-authored.

This contribution has been developed within the framework of the PRIN 2022 project – *Children as Vulnerable Users of IoT and AI-based Technologies: A Multi-level Interdisciplinary Assessment* – CURA, PRIN 2022–2022KAEWYF, – Next Generation EU; CUP: J53D23005540006 Double blind peer reviewed contribution.

ISSN 2281-5147

Table of Contents

Keywords

Child Vulnerabilities – Digital Environment – Education – Adoption – Comparative Law

ISSN 2281-5147

1. The Vulnerabilities of Minors in the Digital Environment

In the contemporary digital context, technological development has opened unprecedented avenues for expression, learning and participation. At the same time, however, it has intensified forms of exposure to risk, relational dependency and informational asymmetry, particularly affecting those in structurally fragile conditions. In this regard, the condition of minors is emblematic: as individuals in the process of development, they embody an ontological vulnerability that, in legal terms, translates into a complete incapacity[1]. This legal status has traditionally been associated with a protective approach, which aims to shield children from harm through the limitation of their decision-making power.

Alongside this protective perspective – which, though grounded in legitimate concerns, risks producing exclusionary effects – a complementary perspective has gained increasing prominence. This approach recognizes and values children's evolving capacities, affirming their right to active participation and progressive autonomy, especially within digital environments.

Building on this conceptual shift, two interrelated questions have persistently guided our research and defined its normative horizon: how can children's rights be not only formally acknowledged but also effectively guaranteed within digital environments? And how can the imperative of protection be reconciled with the recognition of children's evolving capacities, thus enabling meaningful forms of autonomy and agency in their online interactions?

These foundational questions compel a preliminary conceptual clarification of the notion of vulnerability. Now central to contemporary legal and political discourse, vulnerability constitutes a crucial interpretive lens through which to examine the tension between protection and autonomy that defines the digital condition of childhood and adolescence. As early as 1989, Robert Chambers noted the pervasive yet often imprecise use of the term in development studies, highlighting its conceptual elasticity[2]. Vulnerability should not be understood as a monolithic or merely descriptive category; rather, it denotes a condition of heightened exposure to harm,

[1] For a general overview, D. Amram, *Children (in the digital environment)*, in *Elgar Encyclopaedia of Law and Data Science*, G. Comandé (dir.), Elgar, 2022, pp. 155 ff.

[2] R. Chambers, *Editorial Introduction: Vulnerability, Coping and Policy*, in *IDS Bulletin*, vol. 20, 1989, pp. 1 ff.

ISSN 2281-5147

dependency, or suffering, one that can assume diverse forms and operate across multiple, intersecting dimensions.

Recent legal and ethical scholarship has underscored the need to disaggregate the concept, distinguishing between layered and overlapping vulnerabilities that produce complex scenarios requiring differentiated responses[3]. Among the most influential contributions in this regard is the framework elaborated by Florencia Luna, who introduced the concept of "layers of vulnerability" capturing vulnerability as a dynamic, stratified and context-specific phenomenon[4].

Particularly relevant is the conceptual distinction between inherent and situational vulnerability. The former is embedded in the human condition itself, encompassing universal dimensions such as corporeality, relationality and constitutive dependency. The latter, by contrast, arises from contextual factors (economic, social, cultural, technological) or from personal histories and characteristics that heighten exposure to risk. These layers often intersect, producing complex constellations of vulnerability that require equally nuanced normative and policy responses.

In the context under consideration, developmental age represents a paradigmatic form of intrinsic vulnerability. However, digital environments can amplify situational vulnerabilities linked to limited digital literacy, manipulative design architectures, exposure to inappropriate or distressing content, the absence of adequate familial or educational scaffolding and the lack of effective legal and technical safeguards. In certain cases, dispositional vulnerabilities may also come into play, stemming from personal traits or life experiences that render some children more susceptible to harm. This is particularly true for adopted minors, whose condition frequently involves

[3] W. Rogers, C. Mackenzie, S. Dodds, *Why Bioethics Needs a Concept of Vulnerability?*, in *International Journal of Feminist Approaches to Bioethics*, vol. 5, n. 2, 2012, pp. 11-38. For a conceptual application of the multidimensional (or stratified) taxonomy of vulnerability in the specific context of the interaction between minors and AI-powered toys, see: A. Pera, S. Rigazio, *Let the Children Play. Smart Toys and Child Vulnerability*, in C. Crea, A. De Franceschi (a cura di), *The New Shapes of Digital Vulnerability in European Private Law*, Elgar, 2024, pp. 413-437.

[4] Although originally developed in the context of bioethical debates, Luna's theory of layered vulnerability offers a conceptual framework that proves equally valuable when applied to the digital environment and the specific challenges it poses to children's rights and protection. F. Luna, *Elucidating the Concept of Vulnerability: Layers Not Labels,* in *International Journal of Feminist Approaches to Bioethics*, vol. 2, n. 1, 2009, pp. 121-139, http://www.jstor.org/stable/40339200.

ISSN 2281-5147

identity-related, emotional and relational fragilities that may be intensified, or instrumentalized, within digital contexts[5].

It thus becomes evident that among vulnerable individuals, some may be more vulnerable than others[6]. Recognizing the factors that shape individual fragility is essential for devising effective protective and empowering measures. The objective is not to crystallize categories, but rather to identify with precision those conditions that render an individual, particularly a child, more or less exposed to harm, in order to formulate tailored and proportionate responses. In this perspective, vulnerability should not serve as a justification for paternalistic or exclusionary interventions based solely on prohibition. Instead, it should function as an interpretive lens for building relational contexts that reinforce individual capabilities, foster autonomy and enable informed, meaningful participation.

A multidimensional understanding of vulnerability therefore calls for a departure from fragmented or siloed approaches and for the development of integrated normative frameworks that recognise children not as passive recipients of protection, but as rights-holders entitled to the effective enjoyment of interconnected rights, such as privacy, identity and participation, particularly in digital settings. From this vantage point, vulnerability does not signify incapacity; rather, it demands a collective and institutional responsibility to construct inclusive environments where protection and empowerment are not oppositional but mutually reinforcing.

This framework is firmly grounded in the Convention on the Rights of the Child[7], which inaugurated a paradigmatic shift in the legal understanding of childhood. No longer construed merely as subjects in need of protection, children are now recognised as autonomous rights-holders, endowed with intrinsic dignity and agency. Article 12 of the Convention is particularly emblematic in this regard: it enshrines the

[5] Cf. Sections 5-7 of this contribution.

[6] F. Luna, *Identifying and evaluating layers of vulnerability – a way forward*, in *Developing World Bioethics*, vol. 19, n. 2, 2019, p. 87. This conception of vulnerability as a dynamic and context-dependent condition can also be found in several policy documents issued by the European Commission in the field of consumer protection. Notably, the Commission acknowledges that "*consumer vulnerability is situational, meaning that a consumer can be vulnerable in one situation but not in others, and that some consumers may be more vulnerable than others*", European Commission, *Understanding consumer vulnerability in the EU's key markets*, Factsheet, Brussels, 2016, Available at: https://commission.europa.eu/system/files/2018-04/consumer-vulnerability-factsheet_en.pdf.

[7] Convention on the Rights of the Child, New York, 1989.

ISSN 2281-5147

right of every child capable of forming their own views to express those views freely in all matters affecting them and requires that due weight be given to such views in accordance with the child's age and maturity. This provision not only reinforces the overarching principle of the best interests of the child but also lays the foundation for their meaningful participation in social, legal and institutional decision-making processes.

The United Nations Committee on the Rights of the Child, with its General Comment No. 25 (2021)[8], has further elaborated on the application of these principles within digital environments. It calls for an approach that respects children's evolving capacities, ensures age-appropriate protective measures, promotes digital literacy among caregivers and imposes robust obligations on digital service providers to uphold high standards of transparency, privacy and safety. In doing so, the Committee emphasises that digital engagement must be guided not only by the imperative to protect, but also by the commitment to empower children as active participants in the shaping of their digital experiences.

The approach adopted in the following pages builds on this foundation. The analysis begins with a review of the EU regulatory framework and the most advanced national strategies – notably those of the United Kingdom and France – to examine how they address the vulnerabilities of minors in digital environments, highlighting critical issues, good practices and areas for improvement[9].

The overarching aim is to promote a genuinely child-centred approach, one that transcends the abstract articulation of principles and translates them into concrete, actionable and widely shared practices. This requires establishing an operational horizon grounded in effective, multi-level co-responsibility among all stakeholders – children, families, institutions, practitioners, and industry actors – called upon to

[8] General comment n. 25 (2021) on children's rights in relation to the digital environment.

[9] A series of *Blueprint Guidelines* have been developed with the contribution of the Authors within the PRIN 2022 Italian MUR Project *Children as Vulnerable Users of IoT and AI-based Technologies: A Multi-level Interdisciplinary Assessment – CURA* (hereinafter also *CURA Blueprint*), n. KAEWYF, V03. These policy proposals are the outcome of an interdisciplinary and inter-institutional consultation involving legal scholars, psychologists, and educators, with the overarching goal of integrating the protection of privacy with minors' rights to participation and their progressive development of autonomy. This paper refers to the aforementioned *Blueprint Guidelines*, which were first drafted as part of Deliverable D6, *"First Version of the Blueprint Guidelines"*, and subsequently refined through the validation process. The final version is available at: https://www.lider-lab.it/wp-content/uploads/2025/10/PRIN-CURA_Blueprint-Policies-and-Guidelines_final.pdf.

ISSN 2281-5147

cooperate within their respective roles and competences to ensure and actualize the rights of children in digital environments.

Within this setting, the article delves into the specific condition of adopted children, a context in which vulnerabilities often become more complex and layered. Indeed, this case study exemplifies how intrinsic and situational vulnerabilities can intersect and intensify, leading to heightened exposure to risk and requiring the adoption of targeted protective measures. Consequently, particular attention is devoted to the search for biological origins in the digital environment, considering both the emancipatory potential and the risks associated with such deeply personal and identity-sensitive journeys involving the sharing of data and personal information (see infra, sections 5, 5.1 and 6).

Finally, digital literacy and education are examined as strategic levers for the empowerment of minors and for raising awareness within families and society at large. These dimensions cut across all levels of intervention and are essential for equipping all stakeholders with the tools needed to navigate digital environments safely, critically and responsibly (see sections 7, 8 and 9).

2. The European Regulatory Framework

The European legal framework has progressively broadened its focus on protecting minors in the digital environment, outlining a complex, multi-layered regulatory architecture aimed at fostering safe and accessible digital spaces. The overarching goal, in line with the principles enshrined in the UN Convention on the Rights of the Child (hereinafter UNCRC), is to foster an environment in which children can actively and consciously exercise their rights, including the right to protection, participation, and harmonious development.

One of the fundamental pillars of this system is Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter GDPR)[10], which, although not specifically addressed to minors, explicitly recognises their vulnerability (Recital 38), requiring

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679.

ISSN 2281-5147

enhanced protection of their personal data. The GDPR adopts a risk-based approach aimed at assessing the impact of each element of the processing - means, purposes, nature of the data, technology and actors involved - on the individual. Central to this logic is Article 25, which enshrines the principle of data protection by design and by default, requiring data protection measures to be integrated from the outset of system design, with particular attention to the rights and freedoms of data subjects. With specific regard to children, Article 8 sets the default age of digital consent at 16, while allowing Member States to lower this threshold to 13. Italy has opted for a lower age, setting it at 14[11]. Under the GDPR, data controllers are required to make reasonable efforts to verify that consent has been validly given by the holder of parental responsibility[12]. The Regulation also imposes strict obligations concerning transparency, accessibility, and age-appropriate language (Articles 12 and 13), placing particular emphasis on the comprehensibility of the information provided and on the child's awareness of their own rights[13]. However, the framework outlined by the GDPR does not take into account the child's evolving capacity for discernment, thereby neglecting the differences among the various stages of child and adolescent development and flattening the assessment of individual maturity to the mere formal criterion of age.

While the GDPR focuses primarily on the protection of personal data, the European Union has broadened its regulatory efforts to address the systemic risks of the digital ecosystem. In 2022, it adopted Regulation (EU) 2022/2065, known as the Digital

[11] See Article 2-quinquies of the Italian Data Protection Code (Legislative Decree n. 196/2003, as amended by Legislative Decree No. 101/2018), available at: https://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg.

[12] In this vein, the European Data Protection Board (EDPB) issued Declaration 1/2025 on Age Verification, adopted on 11 February 2025. The declaration offers detailed guidance on designing age verification systems that are compliant with the GDPR. Among the recommended practices are tokenized verification through trusted third parties, age band verification mechanisms capable of tailoring protective measures to the child's developmental stage, and multifactorial models (e.g., biometric estimation combined with parental consent), which seek to balance effectiveness, accuracy, and privacy protection. The declaration thus aligns with broader child-centred European strategies, reaffirming the commitment to harmonize the protection of minors with a regulatory framework grounded in constitutional and supranational principles on fundamental rights. Available at: https://www.edpb.europa.eu/system/files/2025-04/edpb_statement_20250211ageassurance_v1-2_en.pdf.

[13] See D. Amram, *Children (in the digital environment)*, cit., pp. 64 ff.

ISSN 2281-5147

Services Act (DSA)[14], marking a crucial step towards a more accountable governance of online intermediaries. The DSA, once again, is not specifically dedicated to children, yet it acknowledges their vulnerability in multiple provisions and imposes enhanced obligations on service providers – particularly very large online platforms (VLOPs), which are frequently used by children and adolescents (such as TikTok, Instagram and Snapchat) – with regard to algorithmic transparency, fundamental rights impact assessments and the prohibition of targeted advertising to minors. As in the GDPR, the concept of risk functions as a core regulatory principle within the DSA, shaping the structure of obligations and safeguards across the text. Articles 34 and 35 require very large online platforms to conduct both *ex ante* and continuously updated risk assessments, especially regarding systemic risks to fundamental rights. Article 28 mandates the adoption of adequate and proportionate measures to safeguard minors, particularly in terms of privacy and safety, including a ban on advertising interfaces based on profiling. Articles 12 and 44 reinforce the obligation to ensure clear, accessible communication and targeted protection for children and adolescents as especially vulnerable users. Article 45 also envisages the development of a Code of Conduct. The DSA's regulatory architecture is therefore centred on safeguarding individuals as users and consumers of digital services and operates in a complementary fashion to the broader privacy protection framework established by the GDPR.[15]

The reference to minors has been further consolidated in Regulation (EU) 2024/1689 on Artificial Intelligence[16] (commonly known as the AI Act), which introduces, for the first time in a binding legal text, a systematic use of the concept of "vulnerability" (appearing 19 times, including 7 within the operative provisions)[17]. In particular,

[14] Regulation (EU) 2022/2065 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:4625430.

[15] D. Amram, *Children (in the digital environment)*, cit., pp. 64 ff.

[16] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) n.300/2008, (EU) n. 167/2013, (EU) n. 168/2013, (EU) n. 2018/858, (EU) n. 2018/1139 and (EU) n. 2019/2144 and Directives n. 2014/90/EU, (EU) n. 2016/797 and (EU) n. 2020/1828 (Artificial Intelligence Act). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689.

[17] For a detailed discussion of how the concept of vulnerability is addressed in the AI Act, see: M.L. Rebrean, G. Malgieri, *Vulnerability in the EU AI Act: building an interpretation*, in *FAccT '25: Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency*, November 28, 2024, pp. 1985-1997, available at

ISSN 2281-5147

among others, recital 28 acknowledges children as vulnerable subjects deserving enhanced protection, while Article 5(1)(b) explicitly prohibits the use of AI systems designed to exploit their cognitive vulnerabilities, such as manipulative interactive toys or persuasive interfaces. AI systems used in educational settings are classified as high-risk and are therefore subject to stringent governance and oversight requirements (Annex III, Article 6). Additional key provisions (Articles 7(h), 27, 29(2), and 60(4)(g)) address safeguards in regulatory sandboxes and establish specific guarantees where AI systems may affect vulnerable individuals, including minors, thus reinforcing the internal coherence of the regulatory framework with the risk-based approach. In this sense, the principle of risk management, already central to both the GDPR and the DSA, thus resurfaces prominently in the AI Act, evidencing the transversal consistency of European digital regulatory strategies.

It should be noted, however, that although the AI Act marks a significant step forward by introducing the notion of vulnerability into binding legislation and including children within certain key provisions (e.g., Article 5(1)(b)), the overall protection of minors remains fragmented: direct references to children's rights are largely confined to the recitals and the normative provisions do not consistently reflect a child-centred approach, leaving their effective protection uncertain and reliant on broad interpretations[18].

This uneven recognition of children's needs within the AI Act must be situated within a broader normative and policy trajectory. In particular, the regulatory framework draws upon the strategic vision already articulated in the European Commission's Communication of 11 May 2022, *"A Digital Decade for Children and Youth: the new European strategy for a Better Internet for Kids (BIK+)"*[19], which provides a more holistic

SSRN: https://ssrn.com/abstract=5058591; F. Galli, C. Novelli, *The Many Meanings of Vulnerability in the AI Act and the One Missing*, in *BioLaw,* vol. 1, 2024, pp.. 53 – 72, available at https://doi.org/10.15168/2284-4503-3302; G. Malgieri, *Human vulnerability in the EU Artificial Intelligence Act*, in Oxford University Press blog.

[18] For a comment see: S. Lindroos-Hovinheimo, *Children and the Artificial Intelligence Act: Is the EU Legislator Doing Enough?,* in *European Law Blog*, 2024. See also: 5rightsfoundation, EU adopts AI Act with potential to be transformational for children's online experience.

[19] Available at: https://digital-strategy.ec.europa.eu/it/policies/strategy-better-internet-kids#:~:text=La%20nuova%20strategia%20per%20un,di%20bambino%20della%20strategia%20BIK%2B. It should be noted that as early as 2012 the European Commission launched the first *Better Internet for Kids (BIK)* strategy, structured around four main pillars: the promotion of high-quality online content for children, the empowerment and awareness-raising of minors, the creation of a safer digital environment, and the fight against online child sexual abuse and the dissemination of child sexual abuse material (available at: https://eur-

ISSN 2281-5147

and programmatic foundation for child protection in digital environments. The strategy – structured around three core pillars: a safe digital environment, digital empowerment and active participation - calls on platforms to adopt accessible and transparent design practices, conduct systemic risk assessments and implement safeguards against content potentially harmful to the mental, physical, or moral well-being of minors. A key initiative under the BIK+ strategy is the forthcoming EU Code of Conduct on Age-Appropriate Design (the 'BIK+ Code'), which seeks to operationalise art. 45 of the DSA. The Code will also be aligned with the broader EU legal framework and will aim to strengthen industry's responsibility in safeguarding children's privacy, safety and well-being online.

The drafting process has been entrusted to a special ad hoc group composed of representatives from industry, academia and civil society[20]. In line with the participatory aims of the BIK+ strategy, children and young people are also expected to be involved in the working group, ensuring that their perspectives contribute to shaping a regulatory instrument genuinely responsive to their needs and rights[21].

Overall, the European framework demonstrates an increasing awareness of the condition of minors in the digital environment. However, a degree of fragmentation persists among binding legal instruments (such as the GDPR, the DSA and the AI Act), soft law tools and sectoral strategies. While the explicit recognition of children's vulnerability is undoubtedly significant, it risks remaining confined to a precautionary logic unless accompanied by genuine normative integration and coherent, inclusive and enabling political action.

In this perspective, a qualitative leap appears essential – towards a model of shared responsibility involving public institutions, private actors and civil society – to foster a digital environment that truly respects the rights of the child.

---

lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012DC0196). The 2022 version, *BIK+*, represents a comprehensive update of that strategy, in line with the evolving challenges of the digital environment and the goals of the European Digital Strategy and the EU Strategy on the Rights of the Child.

[20] The list of members is publicly accessible on the European Commission's website: https://digital-strategy.ec.europa.eu/en/news/members-special-group-eu-code-conduct-age-appropriate-design. The first meeting of the dedicated expert group for the development of the EU Code of Conduct on age-appropriate design took place on 13 July 2023. See: https://digital-strategy.ec.europa.eu/en/library/meetings-special-group-eu-code-conduct-age-appropriate-design.

[21] See: https://digital-strategy.ec.europa.eu/en/policies/group-age-appropriate-design.

ISSN 2281-5147

Against this backdrop, engaging with the regulatory experiences of other European countries, particularly the United Kingdom and France, offers valuable insights into innovative solutions and complementary approaches that may enrich the ongoing debate on the future of child protection in the digital age.

3. Comparative Insights from the United Kingdom and France

Among the countries that have most decisively embraced a child-centred and design-based approach to digital regulation, the United Kingdom stands out as a pioneering example. The adoption of the Age-Appropriate Design Code[22] (commonly known as the Children's Code), which came into force in 2020, marked a paradigmatic shift in embedding children's rights within the design of digital services[23]. Issued by the Information Commissioner's Office (ICO) [24], the Code sets out 15 design standards addressed to providers of online services "likely to be accessed by children" (consider, for instance, video games, social networks...). The Code aspires to embed safeguards that protect children within the digital environment, rather than seeking to restrict or prevent their access to it.[25]

The Code explicitly incorporates the principle of the best interests of the child (Standard 1), mandating that organisations prioritise children's rights over commercial considerations. It also gives concrete effect to the principle of evolving capacities (Standard 3), requiring service design to be tailored to different age groups and functionalities that support children's understanding and progressive self-determination. Among the most significant standards are the requirement to keep

[22] See: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/.

[23] The Code has been developed pursuant to Section 123 of the Data Protection Act 2018, which mandates the Information Commissioner to issue a code of practice providing guidance on the standards of age-appropriate design for information society services that are likely to be accessed by children. The provision entrusts the Commissioner with defining the criteria deemed most suitable to ensure that digital services align with the specific needs and vulnerabilities of underage users.

[24] The ICO is the UK's independent authority responsible for data protection. See: https://ico.org.uk.

[25] For an in-depth and comparative analysis of the UK Age-Appropriate Design Code and its potential as a regulatory model beyond the British context, see: S. Rigazio, L'*Empowerment del minore nella dimensione digitale*, Modena, 2024, available in open access at: https://mucchieditore.it/wp-content/uploads/Open-Access/Rigazio-Prospettive-8-DEF-OA.pdf.

ISSN 2281-5147

geolocation services turned off by default (Standard 10), the automatic activation of the highest privacy settings for child users (Standard 7) and the prohibition of manipulative or persuasive techniques, such as dark patterns, that encourage excessive data sharing (Standard 12). Other key principles include transparency (Standard 4), data minimisation (Standard 8), limits on profiling (Standard 11) and the provision of simple and effective tools for children to exercise their digital rights (Standard 15). The Code also mandates the conduct of a data protection impact assessment (Standard 2) and expressly prohibits any data processing likely to harm the physical, mental, or emotional well-being of the child (Standard 5).

As has been noted, "all the standards are characterised by a dual dimension: they are structured according to a by-design approach and are grounded in the principles underpinning the UNCRC"[26].

Consistent with the overarching European regulatory philosophy, this Code may serve as a paradigmatic reference for the design and implementation of the forthcoming BIK+ Code, which is currently in the drafting phase[27].

This regulatory landscape is complemented by the more recent *Online Safety Act*, which entered into force in 2023[28]. The Act imposes risk assessment and mitigation duties on digital intermediaries, with a specific focus on content accessibility for children. It designates Ofcom[29] as the regulatory authority, granting it broad oversight and enforcement powers and establishes stringent obligations for digital platforms concerning the prevention, identification and mitigation of online risks to child safety.

Among the Act's most salient provisions is the mandatory preparation of Children's Risk Assessments (Section 11), requiring providers to evaluate the risks associated

[26] S. Rigazio, *L'Empowerment del minore nella dimensione digitale*, *cit.*, p. 21; translation by the author. For an in-depth analysis of the by-design approach adopted by the Code and its alignment with the principles of the UN Convention on the Rights of the Child see *Id.*, pp. 21–34.

[27] Notably, the Code has already inspired processes of legal circulation and imitation, as demonstrated by the adoption of the California Age-Appropriate Design Code. For a comparative analysis, see: M. Comite, *Prevent Phishy Business: Comparing California's and the United Kingdom's Age-Appropriate Design Code to Protect Youth from Cybersecurity Threats*, in *University of Miami International & Comparative Law Review*, vol. 31, 2023, pp. 175–200; E. Lampmann-Shaver, *Privacy's Next Act*, in *Washington Journal of Law,* in *Technology & Arts*, vol. 19, n. 1, 2024, pp. 97–129.

[28] Uk Parliament, *Online Safety Act*, 2023. https://www.legislation.gov.uk/ukpga/2023/50.

[29] See Ofcom's role under the *Online Safety Act*: https://www.ofcom.org.uk/online-safety.

ISSN 2281-5147

with content, functionalities and digital interactions likely to affect minors. These assessments must be accompanied by proportionate safety measures (Section 12), including the design of algorithms and user interfaces aimed at minimising potential harm. Furthermore, the legislation requires the implementation of reliable age verification or estimation systems (Sections 12.4–6), designed to prevent children from accessing harmful content.

In this regard, the Act offers a precise definition of "primary priority content" (e.g. material promoting self-harm or suicide) and introduces strict requirements relating to transparency (Section 22) and platform accountability. The regulatory framework as a whole seeks to strike a careful balance between child protection, freedom of expression and the right to privacy, while consistently grounding the imposed measures in the principles of proportionality and necessity.

The UK model stands out as one of the most comprehensive and coherent approaches at the European level, successfully combining *by design* principles, data protection and content regulation within a distinctly child-centred perspective. It is further distinguished by the cultural ambition underpinning it. Through the work of the ICO and other institutional actors, the United Kingdom has promoted a transversal strategy of digital literacy aimed not only at children but, crucially, also at adults: parents, educators, social workers, volunteers, local administrators and public officials. In this way, the protection of minors in the digital environment is framed as a collective responsibility, grounded in the cultivation of a widespread, informed and child-respectful digital culture.

Equally significant is the commitment to directly involve children in decision-making processes. Their views are gathered through public consultations and advisory groups, meaningfully contributing to policy design and platform development. This represents a fundamental shift from a paternalistic regulatory logic to a genuinely participatory perspective, rooted in co-creation *with* children rather than mere protection *for* children[30].

Within this framework, the British model offers an advanced example of child-centred regulation, one that integrates legal safeguards, digital empowerment and

[30] ICO, Guidelines on Data Sharing, in https://ico.org.uk/for-organisations/uk-gdpr- guidance-and-resources/data-sharing/a-10-step-guide-to-sharing-information-to- safeguard-children/.

ISSN 2281-5147

social inclusion, thereby providing a valuable benchmark for comparative legal and policy analysis.

In recent years, France has also intensified its institutional and regulatory focus on the condition of minors in the digital environment, with particular attention to the issue of early and prolonged exposure to screens. In January 2024, a national commission was established with the mandate to analyse the impact of digital technologies on the physical and mental health of children, assess the effectiveness of existing measures and formulate concrete policy proposals. The findings of this work were consolidated in the report *Enfants et Écrans – À la Recherche du Temps Perdu*[31], published in April 2024, which currently stands as the most comprehensive document produced in France on this topic.

The report offers a clear-sighted and nuanced analysis of the ambivalence inherent in minors' digital experiences. On the one hand, it acknowledges the educational and participatory potential of technology; on the other, it highlights the increasingly well-documented risks to physical health (including sleep disorders, obesity and visual impairment), mental well-being (such as anxiety, depression and social withdrawal), and identity formation within highly stereotyped and commercialized environments. In response, the report proposes a comprehensive strategy structured around six key areas of intervention: (1) combating manipulative design practices; (2) ensuring protection rather than mere control of minors; (3) enabling gradual and age-appropriate access to digital tools and platforms; (4) fostering digital autonomy through targeted education; (5) equipping responsible adults with adequate training; and (6) establishing a robust public governance framework.

Building on these six pillars, the Commission outlines twenty-nine operational proposals that collectively define a broad-spectrum public policy agenda. Particularly innovative are the measures aimed at regulating platform design. Among these, the Commission recommends shifting the burden of proof onto digital service providers regarding the impact of their algorithms, prohibiting harmful design practices, and codifying a new "right to configuration," which would grant users, especially minors, the ability to consciously modify default settings that affect them. The report also calls

[31] Commission nationale sur l'exposition des enfants aux écrans, *Enfants et Écrans – À la Recherche du Temps Perdu*, April 2024, available at: https://www.elysee.fr/admin/upload/default/0001/16/fbec6abe9d9cc1bff3043d87b9f7951e62779b09.pdf.

ISSN 2281-5147

for the introduction of effective age verification mechanisms and increased investment in educational content.

Of significant note is the proposal to prohibit screen exposure for children under the age of six within educational settings, to delay access to social media until the age of fifteen, and to adopt a phased approach to the introduction of mobile phones and personal digital devices. This graduated policy suggests: no phones before age 11; basic phones without internet connectivity from age 11; internet-enabled phones from age 13, but with restrictions on social media and illegal content; and from age 15, expanded access to vetted social media platforms. These measures are accompanied by structural interventions within the school environment, aimed at equipping students, educators and families with the critical and pedagogical tools necessary for informed digital citizenship. Digital education is conceived as a cross-cutting dimension to be integrated into pedagogical competencies, mental health curricula, interpersonal relations, emotional regulation and digital risk awareness.

The French legislator had already intervened through a series of fragmented measures. As early as 2010, the legislation on online gambling established a prohibition on access for minors[32]. However, a more substantial regulatory consolidation has been observed since 2022. The so-called *Loi Studer* (2022)[33] introduced a requirement for digital device manufacturers to pre-install free parental control tools. The 2023 law on influencers regulated advertising practices targeting minors, introducing specific

[32] Law n. 476/2018, 12 May 2010, relating to the opening up to competition and the regulation of the online gambling and games of chance sector (Loi n. 2010-476 du 12 mai 2010 *relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne*), available at : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000022204510.

[33] Law n. 330/2022, 2 March 2022, aimed at strengthening parental control over means of accessing the Internet (Loi n. 2022-300 du 2 mars 2022 *visant à renforcer le contrôle parental sur les moyens d'accès à internet*), https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045287677. For a critical reflection on the challenges faced by parents in managing children's digital exposure, see M. Haza-Pery, T. Rohmer, *Enfants connectés, parents déboussolés*, Brussels, 2023.

ISSN 2281-5147

safeguards for children engaged in "baby influencer" activities[34]. The *Loi Marcangeli*[35] on online hate speech established a so-called "digital age of majority" at fifteen years for access to social media platforms - though this provision has raised concerns regarding its compatibility with European Union law. In 2024, a dedicated law on privacy and image rights of minors was enacted[36], imposing on parents a legal duty to respect their children's privacy and establishing judicial mechanisms aimed at safeguarding the child's digital identity.

The *Enfants et Écrans* report thus positions itself within an already existing normative framework yet seeks to enhance its systemic coherence by offering an integrated, child-centred vision. At the heart of the report lies the active involvement of children and adolescents: 150 minors were consulted during the Commission's work, and their perspectives were explicitly incorporated into the formulation of the final recommendations[37]. Youth participation, combined with a strong reliance on scientific evidence and the precautionary principle, underpins a model of governance that aims to move beyond emergency-driven responses in favour of a long-term regulatory architecture. In this regard, the report calls for the establishment of a new national governance structure for digital literacy, to be financed through the

[34] Law n. 451/2023, 9 June 2023, aimed at regulating commercial influence and combating the excesses of influencers on social networks (Loi n. 2023-451 du 9 juin 2023, *visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux*), https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047663185. For a comparative analysis with the UK legal framework, particularly on influencers, labour law and social protection, see C. Marzo, *Influencers, Labour Law and Social Protection: A Comparative Analysis between France and the United Kingdom*, in *The Hashtag Hustle*, Taylor Annabell, Christian Fieseler, Catalina Goanta, and Isabelle Wildhaber (eds.), Edward Elgar, 2025, pp. 130–148.

[35] Law n. 566/2023, 7 July 2023, aimed at establishing a digital majority and combating online hate (Loi n. 2023-566 du 7 juillet 2023 *visant à instaurer une majorité numérique et à lutter contre la haine en ligne*), https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047799533. M. Saulier, *Loi no 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne*, in *Actualité juridique Famille*, vol. 9, 2023, pp. 420 ff. ⟨halshs-04206468⟩.

[36] Law n. 120/2024, 19 February 2024, aimed at ensuring respect for children's image rights (Loi n. 2024-120 du février 2024 *visant à garantir le respect du droit à l'image des enfants*), https://www.legifrance.gouv.fr/loda/id/JORFTEXT000049163317/2025-04-16/#:~:text=LOI%20n°%202024%2D120,des%20enfants%20(1)%20%2D%20Légifrance. For a comment on the effectiveness of France's new rules on children's image rights, see M. Saulier, *Garantir le respect du droit à l'image des enfants: un objectif ambitieux, une efficacité douteuse?,* in *Actualité juridique Famille*, n. 3, 2024, pp. 116 ff. ⟨halshs-04500845⟩.

[37] Commission nationale sur l'exposition des enfants aux écrans, *Enfants et Écrans – À la Recherche du Temps Perdu*, April 2024, p. 14.

ISSN 2281-5147

application of the "polluter pays" principle and sustained support for responsible actors, research institutions and widespread educational campaigns.

The French response thus stands out for the breadth and depth of its vision, marked by a strong emphasis on ethical design, child agency and the educational role of civil society. It constitutes an ambitious model that opens up promising avenues for digital child protection across Europe, although its effective implementation and stable coordination with European Union law remain, at least for now, partially pending.

The comparative analysis of legal and regulatory frameworks in the United Kingdom and France has proved especially valuable in identifying alternative or complementary models for safeguarding children in the digital environment. While grounded in distinct legal and institutional traditions, the solutions adopted in these jurisdictions offer meaningful contributions in terms of regulatory strategies, operational mechanisms and the role of independent oversight bodies. Building on these reflections, a set of blueprint policies has been developed, drawing on EU-level principles and integrating national best practices, with the aim of formulating concrete recommendations to enhance the protection of children's rights in today's digital landscape.

4. Principles in Action: Building a Digital Environment *for* and *with* Children

Adopting a child-centred perspective and drawing on an intrinsic and situational understanding of vulnerability means translating theoretical principles concerning children's rights, previously analysed, into concrete operational actions capable of guiding educational practices, regulatory frameworks and digital design[38]. Anchoring themselves in the principle of the best interests of the child (Article 3 UNCRC) and in key EU instruments such as the GDPR, the DSA and the AI Act, this framework aims to reconcile privacy protection with the promotion of participation and evolving capacities.

The theoretical architecture underpinning concrete actions is grounded in a non-reductionist conception of vulnerability, understood not as a permanent or

[38] The reference is to the *CURA Blueprint Guidelines*, cited in note 9, to which the reader is referred for further details.

ISSN 2281-5147

pathological condition, but rather as a dynamic, context-dependent expression of the interaction between individual and environment, shaped by personal, social and technological factors. Accordingly, responses to vulnerability cannot be confined to paternalistic or purely protective logics; instead, they must pursue a calibrated balance between safeguarding, progressive responsibility and the enhancement of evolving capacities. A dynamic understanding of children's evolving capacities calls for privacy-by-design measures tailored to developmental stages and for the active involvement of minors in shaping their digital environments. In this perspective, protection and empowerment are not opposing aims, but complementary dimensions of the same child-centred framework.

Although this perspective may initially appear more sociological based than legal, regulatory frameworks such as than the UK *Age-Appropriate Design Code* and the French clearly demonstrate that multi-stakeholder cooperation is not merely desirable, but legally indispensable. The UK experience is emblematic: the sanctioning powers vested in the ICO have already produced tangible effects, with substantial fines imposed on major digital platforms, as in the case of TikTok, thereby confirming the normative robustness and the effective enforceability of this model[39].

The suggested guidelines' evolutionary and plurilateral approach is fully consistent with the legal framework established by the UNCRC, which places the principle of evolving capacities at its core, and with recent case law that increasingly recognises the child's progressive autonomy in exercising rights and in shaping the scope of protective obligations[40].

Finally, to reinforce the legitimacy of a participatory and multi-level methodology in public policy-making, reference should be made to the recent Colorado AI Act White Paper (2024). Drafted precisely in this spirit, and due to enter into force in 2026, it represents a paradigmatic precedent in comparative law. The document explicitly frames governance not as a mere bureaucratic constraint but as a mechanism of *responsible value creation*, calling for cooperation among developers, deployers and

[39] In April 2023, for example, the ICO fined TikTok £12.7 million for misusing children's data, including failing to restrict underage users and processing personal data without parental consent. This is an enforcement decision that concretely underscores the legal force behind the regulatory principles. See *ICO fines TikTok £12.7 million for misusing children's data***:** https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/04/ico-fines-tiktok-127-million-for-misusing-children-s-data/.

[40] For an in-depth analysis, see S. Rigazio, *L'Empowerment del minore nella dimensione digitale*, *cit.* pp. 124 ff.

ISSN 2281-5147

regulators. In line with this logic, the Act imposes binding obligations on both developers and deployers of high-risk AI systems, requiring transparency, risk assessment, documentation and continuous monitoring, while encouraging compliance to be shaped as a form of "co-governance" rather than unilateral control. This confirms that participatory governance is no longer a merely theoretical aspiration but has now become a consolidated regulatory technique of growing comparative significance[41].

Based on these premises, the proposed actions are structured along three key dimensions - technological, ethical-legal and educational-psychological - and are addressed to four main stakeholder groups: families, professionals, public and private organisations, and minors themselves. Their design is inspired also by the advanced regulatory experiences previously discussed, such as the UK's Age-Appropriate Design Code and recent French strategies, which promote a multi-level approach based on protection by design, shared responsibility and participatory co-creation.

Families are identified as pivotal actors in creating safe and enabling digital environments. Strengthening parents' digital literacy and awareness of emerging risks is therefore essential and can be supported through accessible training programmes, tailored informational resources and opportunities for dialogue with experts. Parental responsibility should not be understood as a set of prescriptive tasks, but as a practice of empathic mediation, where relational care becomes a prerequisite for building a home environment in which children can gradually exercise their right to exploration and experimentation. Parents are thus encouraged to play an active role not only in protecting their children but also in promoting autonomy and critical thinking. Recommended operational measures include: the development of accessible digital platforms supporting authoritative parenting practices, with modules on emotional intelligence, effective digital communication with adolescents and constructive intra-family dialogue; the provision of simple, user-friendly tools to activate parental controls at the time of purchase or registration (e.g. mandatory tutorials, intuitive interfaces, quick-start guides); the integration of proactive and easily usable functionalities (control panels, risk alerts, interactive tutorials, automated flagging

[41] See S. Leunig, E. Feldman, E. Schwartz, N. Dammaschk, S. Brown, C. Miller, P. Sullivan, A. Mittal, *The Colorado AI Act: A Compliance Handshake Between Developers and Deployers*, 2025, available at: https://mcusercontent.com/4edfeaae1cfabad5c2f808237/files/9b99f02c-5a6a-771a-fadd-32907366d547/Colorado_AI_Act_white_paper.pdf.

ISSN 2281-5147

systems); the development of technologies that promote family digital safety, such as content filtering and monitoring applications, while also preserving children's evolving autonomy and privacy, in accordance with the child's age and maturity; and access to psychological support and counselling services for parents and children, coordinated with educational and healthcare services[42].

Professionals working with children[43], such as teachers, educators, psychologists, healthcare providers and social workers, occupy a key position in the construction of digital environments that are not only safe, but also developmentally appropriate and inclusive. In this capacity, they are called upon to act as reflective intermediaries between minors, families and technological systems. It is essential to integrate into continuous professional training topics such as digital citizenship, emotional intelligence, risk prevention and critical digital engagement, in order to promote a shared culture of digital well-being.

Beyond individual training, it is important also to promote the adoption of accessible and context-sensitive tools that enable professionals to guide children in navigating the digital world. These include intuitive control systems and didactic resources co-designed with children themselves, as well as digital platforms offering contextual guidance on emerging technologies. Specific features, such as "Educator controls" modelled on parental settings, can empower professionals to supervise educational platforms in ways that respect children's autonomy while ensuring appropriate safeguards.

Crucially, professionals are encouraged to facilitate open conversations with children about their online experiences, helping to bridge the divide between digital and offline life[44] and enabling the recognition of signs of emotional discomfort or distress. These practices are reinforced through collaborative initiatives involving families and social services, supported by practical tools such as short videos, intergenerational workshops and materials for use in school or home-based consultations. This approach finds solid grounding in the child's right to be heard, enshrined in Article

[42] *CURA Blueprint Guidelines*, *cit.*, pp. 5-8.

[43] *Ibidem*.

[44] On the topic, and with reference to the neologism "onlife" – describing the constant interpenetration of physical and digital realities – see L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017.

ISSN 2281-5147

12 of the UNCRC and widely affirmed in both European and Italian jurisprudence, which underscore the centrality of listening to the child as a prerequisite for meaningful protection and participation[45].

Particular attention should be paid to the development of diagnostic and preventive tools capable of identifying adolescents who may be especially vulnerable to the emotional effects of AI-driven interactions. These tools, ideally designed in co-participation with children, should enable early and tailored interventions in cases of distress. Specialised training modules and certification programmes are also recommended, with a strong emphasis on emotional intelligence as a central component of digital safety. In line with this, the proposed approach underscores the need for professionals to be equipped to handle identity-sensitive issues, especially in the context of adoption, by supporting families in fostering emotionally aware and ethically grounded digital practices.

This multidimensional approach, combining technical, educational and emotional competences, resonates with the public strategies implemented in the UK and France, where the promotion of children's participation and the cultivation of digital resilience are recognised as essential pillars of digital governance.

Public and private organisations, particularly digital platforms and service providers are called upon to uphold principles of proactive responsibility and enhanced protection. Specific recommendations include: designing age-appropriate interfaces differentiated by age groups, using comprehensible language and layered functionalities; adopting transparent, updateable and interoperable systems for age verification and parental control; implementing accessible and responsive reporting mechanisms for minors and their caregivers, with immediate feedback and differentiated pathways based on age and exposure to risk; developing adaptive

[45] In the domestic legal framework, this orientation finds confirmation in the so-called *Cartabia Reform* (Legislative Decree n. 149 of 10 October 2022), implementing Delegated Law n. 206/2021. The reform introduced a far-reaching overhaul of civil procedure and of alternative dispute resolution mechanisms, with significant repercussions on proceedings concerning persons and family matters. Within this context, a more structured and detailed regulation of the child hearing procedure was established, designed to enhance not only the child's natural capacities and inclinations, but also his or her expectations and developmental aspirations. This approach emerges with particular clarity from the Explanatory Report to the decree, which expressly underscores the child's right to self-determination as an individual asset to be recognised and protected. See S. Rigazio, *L'Empowerment del minore nella dimensione digitale, cit.*, pp. 130 ff.

ISSN 2281-5147

recommendation systems that avoid polarisation and stereotyping, tailoring content suggestions to children's cognitive and emotional development; and publicly disclosing the indicators used in risk assessment systems, as part of accessible transparency and monitoring reports. Active involvement of minors in service design, through co-creation processes, is strongly encouraged. These recommendations draw directly on the UK's Age-Appropriate Design Code, which introduced the first legally binding requirements for information society services targeting children, and which remains a key comparative reference for integrated online child protection[46].

The active involvement of minors in shaping the strategies that affect their digital lives should be recognised as a central element of any child-centred regulatory framework. Emphasis should be placed on their participatory role and on the importance of developing tools that are genuinely responsive to their evolving needs. In this regard, particular value lies in the creation of child-friendly digital instruments[47], designed according to usability and accessibility principles appropriate to different age groups and aimed at fostering emotional awareness, privacy protection and responsible online behaviour (such as educational avatars, gamified learning paths, narrative interfaces and alert notifications that encourage dialogue with trusted adults).

Children's participation is further supported through co-design workshops, focus groups and iterative feedback mechanisms[48]. In line with the BIK+ Strategy and best practices developed in France and the UK, this participatory approach is recognised as an effective form of empowerment. Crucially, however, it does not represent a sociological novelty but rather the continuation of a legal and regulatory trajectory already consolidated elsewhere. On the one hand, it follows the path traced by case law and international instruments, which have progressively emphasised the child's right to be heard and to be actively involved in decisions affecting them. On the other hand, it reflects broader regulatory trends in the digital economy, where experimentation and collaborative governance have increasingly been embraced as guiding principles. The analogy with the "regulatory sandbox" model is instructive: initially developed in the financial sector as a controlled environment in which

[46] *CURA Blueprint Guidelines*, *cit.*, pp. 3 – 4 – 7 - 8.

[47] Notably, even the Convention on the Rights of the Child itself has been made available in a child-friendly version, underscoring that accessibility and participation are not matters of sociology alone, but are firmly rooted in legal practice and principles.

[48] *CURA Blueprint Guidelines*, *cit.*, pp. 6 and 9.

ISSN 2281-5147

innovative tools could be tested under light-touch supervision, this methodology has progressively spread to other domains of digital and AI governance[49]. In this perspective, children's involvement in shaping digital environments can be seen as part of the same experimental logic, a regulatory laboratory where rights, technologies and responsibilities are co-constructed through inclusive processes.

Listening to children and adolescents, valuing their digital expertise and recognising their concerns, means acknowledging them as active co-constructors of the digital world. In this sense, protection cannot be meaningfully separated from participation: one cannot truly protect those who are not included in the decisions that affect them.

Taken as a whole, the proposed framework reflects an integrated and multi-layered vision of child protection in digital environments, one that views vulnerability not as a fixed attribute, but as a dynamic and situated condition to be addressed through the careful balancing of safeguarding and the progressive development of autonomy. In this perspective, building truly child-friendly digital ecosystems requires moving beyond paternalistic approaches and embracing collective responsibility across all stakeholders.

Yet, the good practices outlined above are put to the test when vulnerabilities become more complex and interwoven, as in the case of adopted minors seeking information about their biological origins online. In such situations, standard protective frameworks may prove insufficient, calling instead for context-sensitive responses that combine legal safeguards with ethical guidance and emotional support. These more specific challenges are addressed in the following sections (5, 5.1 and 6), which focus on how vulnerability multiplies in adoption-related contexts and explore the corresponding need for targeted and ethically grounded policy interventions.

Then, a constant emphasis is placed on digital literacy and education as foundational dimensions, not only for fostering awareness and resilience, but also for enabling children's meaningful and informed participation in the digital sphere. While the present and following sections have primarily focused on the legal and technical pillars of intervention, Sections 7 and 8 provide a more in-depth discussion of educational practices from a comparative perspective. Section 9, in turn, offers concrete policy

[49] S. Rigazio, '*New techs, new threats': sfide e opportunità della rivoluzione blockchain*, in *La cittadinanza europea Online*, 2021, pp. 61 ff.

ISSN 2281-5147

recommendations relating to the educational pillar, understood as a key instrument for addressing and reconnecting the various layers of vulnerability through the large-scale promotion of digital awareness.

5. The complex balance between privacy preserving and search for origins

As mentioned in the previous paragraphs, although childhood and adolescence are inherently associated with vulnerability, certain circumstances heighten this condition and call for targeted protective measures. The sensitivity of certain contexts is today further amplified by the potentialities of the digital environment, which can significantly impact already fragile family scenarios. Adoption represents one such context: the emotional and legal complexities surrounding identity and belonging render children particularly exposed, while digital technologies intensify this vulnerability by opening new, often risky, avenues for exploring their past and connections.

The case of adopted minors, specifically within the Italian legal framework, is particularly relevant for examining the balance between two different fundamental rights: on the one hand, the individual's right, including that of the minor, to know their origins, as an essential element in the construction of personal identity; on the other hand, the right to privacy during a safe navigation, which imposes limits on the access to, collection and dissemination of sensitive personal data, particularly in digital contexts. This requires a legal approach capable of reconciling self-determination with protection.
This analysis highlights the challenges in formulating legal solutions that can simultaneously safeguard the minor's need for truth and their exposure to digital risks, calling for an approach that is sensitive to context, age, and the vulnerability of the individual concerned.

The Italian legal framework on the search for origins is especially significant, as it reveals inconsistencies between the letter of the law, which grants only adult adoptees the right to undertake such a search, and actual practice, where even very young adoptees increasingly engage in this process, often leveraging digital technologies in a smart and intensive manner.

ISSN 2281-5147

Following an overview of the legal framework governing origin tracing in Italy, the analysis will focus on the peculiarities of such a search when carried out online by a minor. Finally, the article will offer a comparative perspective, exploring how the search for origins is regulated in French and English legal systems, taking into account recent debates and the role played by new technologies in such jurisdictions.

Adopted minors are particularly vulnerable individuals, even when compared to their peers. They are often faced with the challenge of coming to terms with a difficult and obscure past, which compels them to question their biological origins and seek to discover the identity of their birth parents and relatives[50]. This process inevitably involves a highly emotional component, marking the search with unique features[51].

Such considerations have led several countries to institutionalize this process by establishing dedicated mechanisms aimed at assisting adoptees in tracing their origins, while also safeguarding the privacy and rights of other individuals potentially involved. This is the case of Italy, which in its legislation on both domestic and international adoption, has included a specific provision addressing the situation of an adoptee who wishes to discover their origins, particularly the identity of the birth mother[52]. Specifically, the adoption law provides that adoptees over the age of twenty-five may submit a petition to the Juvenile Court of their place of residence in order to access information concerning their origins and the identity of their biological parents[53].

A notable peculiarity of the procedure lies in the age requirement set by the legislature: the threshold of 25 years substantially exceeds the legal age of majority in Italy, set at

[50] M. D. Schechter, D. Bertocci, *The meaning of the search. The psychology of adoption*, New York, NY, US: Oxford University Press, 1990; W. Tieman, J. van der Ende, F. C. Verhulst, *Young adult international adoptees' search for birth parents*, in *Journal of Family Psychology*, 2008.

[51] R. Rosnati, R. Iafrate, *Psicologia dell'adozione e dell'affido familiare*, Vita e Pensiero, Milano, 2023, pp. 206 ff.; D.M. Brodzinsky, M.D., Schechter, R. Marantz Henig, *Being adopted. The lifelong search for self anchor,* New York: Books Ed., 1993.

[52] L. n. 184/1983, the Italian adoption law, entitled "*Diritto del minore a una famiglia (Child's right to a family)*".

[53] Article 28, par. 5 and 6. The same article provides for exceptions regarding the age threshold where particular conditions exist: 18 years if there are serious and proven reasons relating to the psycho-physical health of the adopted child while, in the case of serious and proven reasons, such a request can be made directly by the adoptive parents of the minor. This is, in any case, a delicate procedure, involving hearings of individuals deemed necessary by the Court, and, more importantly, a psychosocial assessment of the applicant. The aim is to prevent such disclosure from excessively disturbing the applicant's psychological well-being.

ISSN 2281-5147

18, when an individual is already legally entitled to make independent decisions and manage their own interests[54].

Nonetheless, the most distinctive aspect of the Italian legal framework is found in another provision: the so-called "anonymous birth" (*parto anonimo*), which establishes that access to the requested information is not permitted if the birth mother, at the time of delivery, declared her wish not to be identified[55]. According to the letter of the law, such a declaration entails an absolute and irreversible prohibition for the adoptee to initiate any procedure to discover the birth mother's identity[56].

Within the European context, Italy stands as a significant exception. In addition to Italy, only France and Luxembourg provide for anonymous birth, granting pregnant women the option to remain unidentified[57]. In contrast, most of the EU Member States do not recognise this possibility, giving priority to the principle of automatic maternal recognition. In these jurisdictions, anonymous birth is prohibited to ensure that the child's right to know their origins is always preserved[58].

---

[54] Upon reaching adulthood, individuals are generally granted access to most private and public rights, including employment and voting. For an overview of the legal capacity of minors within the Italian legal system: F.D. Busnelli, *Capacità ed incapacità di agire del minore,* in *Diritto di famiglia e delle persone*, Milano, 1982, pp. 54 ff.; F. Giardina, *La condizione giuridica del minore*, Napoli, 1984.

[55] This is possible pursuant to Article 30, paragraph 1, of Presidential Decree n. 396 of 3 November 2000, which states: "*The birth declaration is made by one of the parents, by a special proxy, or by the doctor or midwife or other person who attended the birth, respecting the mother's wishes not to be named*".

[56] The rationale behind this provision is rooted in the legislature's intent to prevent abortion and infanticide by allowing for safe deliveries and avoiding dangerous abandonment. At its core lies the protection of the right to life of both the mother and the newborn. However, the law also aims to safeguard additional rights, including health, privacy, personal autonomy, and the right to be forgotten: E. De Belvis, *Il diritto dell'adottato di conoscere le proprie origini biologiche*, in *Fam. Dir.*, n. 10, 2017, pp. 396 ff.; G. Casaburi, *Il parto anonimo dalla ruota degli esposti al diritto alla conoscenza delle origini*, in *Foro it.*, n. 1, 2014, pp. 8 ff.; V. Marcenò, *Quando da un dispositivo d'incostituzionalità possono derivare incertezze*, in *Nuov. Giur. civ. comm.*, n. 4, 2014, pp. 279 ff.

[57] For an overview in legal European field: L. Balestra, E. Bolondi, *La filiazione nel contesto europeo*, in *Fam. Dir.*, n. 3, 2008, pp. 310 ff.; B. Knoll, *Il diritto al parto in anonimato*, in *Milan Law Review*, v. 3, n. 1, 2022, pp. 100 ff.; E. Andreola, *Fratelli biologici di madre anonima e riservatezza dei dati genetici*, in *Fam. Dir.*, n. 3, 2020, pp. 281 ff.; Outside the strictly EU area, Russia and Slovakia, in accordance with Italian, Luxembourg, and French law, provide for anonymous birth. For a comparison with English and French law, see the next section.

[58] Specifically, Spain initially allowed anonymous births, which was declared unconstitutional in 1999 by the Supreme Court: B. Grazzini, *Diritto alla conoscenza delle proprie origini e riservatezza nei rapporti di filiazione*, Aracne, Roma, 2018, pp. 47 ff. Other countries that prioritize maternity certification include England, the Netherlands, Portugal, Belgium and Denmark.

ISSN 2281-5147

Between these two regulatory models lies a third: the Germanic legal systems. Germany and Switzerland, long-time advocates of the right to origin disclosure, have recently introduced the institution of "confidential birth" (*vertrauliche Geburt*), which constitutes a moderated approach to the previously absolute nature of the right to biological identity[59].

Until the last decade, the Italian framework was extremely rigid, admitting no exceptions or derogations and establishing the mother's anonymity as an unchallengeable principle. It took judicial intervention - both domestic and supranational - to soften the rigidity of the institution[60].

Over time, awareness has grown regarding the importance for adoptees of knowing their origins as part of the process of constructing their individual and psychological identity[61]. This aligns with the principle of the best interest of the child, which encompasses the right of the grown child to understand their own past[62]. This has led to the introduction of the so-called *interpello* procedure, a legal mechanism that partially recognises the right of the adoptee to know their origins.

The *interpello* allows the Court to contact the birth mother and give her the opportunity - if she so wishes - to revoke the anonymity declared at the time of birth. If the mother consents, the adoptee gains access to her identifying information. If not, her identity remains protected.

---

[59] On the German legal system: C. Rusconi, *La legge tedesca sulla vertrauliche Geburt. Al crocevia tra accertamento della maternità, parto anonimo e adozione*, in *Eur. Dir. priv.*, n. 4, 2018, pp. 1347 ff. Regarding the Swiss legal system, however, please consult the Rapporto del Consiglio federale in adempimento del postulato Maury Pasquier 13.4189 "Migliorare il sostegno alle madri in difficoltà e alle famiglie vulnerabili", 12 December 2013, 12 October 2016, available on www.admin.ch.

[60] M.N. Bugetti, *Parto anonimo: la secretazione dell'identità della madre si protrae anche dopo la sua morte*, in *Fam. Dir.*, n. 12, 2020, pp. 1140 ff. and, the same author, *Il diritto all'anonimato della madre incapace prevale sul diritto del figlio a conoscere le proprie origini*, in *Fam. Dir.*, n. 7, 2021, pp. 748 ff.

[61] G.M. Wrobel, H.D. Grotevant, *Minding the (information) gap: what do emerging adult adoptees want to know about their birth parents?*, in Adoption Quarterly, 22(1), 2019, pp. 29 ff.; A.Y. Kim, O.M. Kim, A.W. Hu, J.S. Oh, R.M. Lee, *Conceptualization and measurement of birth family thoughts for adolescents and adults adopted transnationally*, in *Journal of Family Psychology*, 34(5), 2020, pp. 555 ff.; F. Vadilonga, *Curare l'adozione*, Milano, Raffaello Cortina, 2010.

[62] United Nations Committee on the Rights of the Child (2013). General comment n. 14 (2013) on the Right of the Child to Have His or Her Best Interests Taken as a primary consideration, CRC/C/GC/14. https://www.refworld.org/docid/51a84b5e4.html; Z. Vaghri, R. Ruggiero, G. Lansdown, *Children's Rights-Based Indicators. Strengthening States' Accountability to Children*, Springer, 2025.

ISSN 2281-5147

The introduction of this institution was made possible by the intervention of the Italian Constitutional Court, which declared unconstitutional the provision of the Adoption Law insofar as it did not allow the biological mother to revoke her anonymity, and urged the legislator to enact legislation on the matter[63].

Despite the Constitutional Court's explicit call, no implementing legislation has been enacted since 2013. In the absence of statutory regulation, the Juvenile Courts have been *de facto* entrusted with managing this delicate issue. As a result, diverse and often inconsistent judicial practices have emerged, which the Court of Cassation has occasionally attempted to standardise[64].

Furthermore, the courts are now faced also with increasingly complex and unforeseen scenarios. These have led to the development of additional judicial interpretations, including: the right to know the identity of a deceased mother; the inadmissibility of the *interpello* in cases where the birth mother is still alive but legally incapacitated; and the possibility of identifying biological siblings[65].

Therefore, the legal possibility of giving birth anonymously and of searching for one's origins is currently governed by a limited number of legislative provisions and a few, but fundamental, rulings from the highest Italian courts.

Despite the active role played by the Constitutional and Supreme Courts, the *interpello* procedure still suffers from a significant legislative gap[66]. This lack of legislation

---

[63] Godelli v. Italy, HUDOC, 25 September 2012, appeal n. 33783/09. V. Carbone, *Corte Edu: conflitto tra diritto della madre all'anonimato e diritto del figlio a conoscere le proprie origini*, in *Corr. giur.*, n. 7, 2013, pp. 960 ff.; G. Currò, *Diritto della madre all'anonimato e diritto del figlio alla conoscenza delle proprie origini. Verso nuove forme di contemperamento,* in *Fam. Dir.*, n. 6, 2013, pp. 537 ff.; A. Margaria, *Parto anonimo e accesso alle origini: la Corte europea dei diritti dell'uomo condanna la legge italiana*, in *Min. Giust.*, n. 2, 2013, pp. 340 ff.; D. Butturini, *La pretesa a conoscere le proprie origini come espressione del diritto al rispetto della vita privata*, in *Forum di quaderni costituzionali*, 24 October 2012, pp. 1 ff.

[64] The Supreme Court of Cassation provided an overview of the practices adopted by various Italian Juvenile Courts, accounting for the differences and commonalities that characterize the *Interpello* procedure, in its Joint Sections ruling n. 1946 of January 25, 2017.

[65] These rulings were reached in Supreme Court rulings n. 15024 of July 21, 2016, n. 7093 of March 3, 2022, and n. 6963 of March 20, 2018.

[66] Over the years, several legislative proposals have been advanced, yet none has been enacted into law. The last two, dating back to the previous legislature, are: S. n. 1039, Provisions regarding social welfare services, anonymous births, and access to information on the origins of a child not recognized at birth, initiated by the Hon. Giuseppe Luigi Salvatore Cucca (Pd) and others, 31 January 2019, last discussed on 6 July 2022; S. n. 922, Provisions regarding the right to know one's biological origins, initiated by the Hon. Simone Pillon and F. Urraro (L.-Sp.-Psd'Az.) 7 November 2018, also last discussed on 6 July 2022.

ISSN 2281-5147

undoubtedly jeopardises the right of adoptees to investigate their roots, a right that remains dependent solely on judicial interpretation. Furthermore, new challenges are emerging in the field of adoption, closely linked to the issues of origin tracing and the *interpello* procedure.

First, it is increasingly likely that in the near future, adoptees will seek to identify not only their birth mothers and siblings but also other biological relatives, such as fathers, grandparents, and uncles or aunts.

Second, it is likely that one of the most pressing issues on the horizon is the right of children born through heterologous assisted reproduction or international surrogacy to discover their origins[67].

Finally, there is the issue that concerns all adopted individuals: the possibility of tracing their origins via the internet, bypassing institutional channels and in the absence of a clear regulatory framework defining its limits, methods, and ethical implications. This exposes them, as minors, to a range of risks and opportunities that are inherent to online navigation and deserve careful examination[68]. For this reason, it is essential that children and adolescents are adequately equipped to understand and recognise the dynamics of the digital environment, enabling them to navigate it with greater awareness and autonomy, particularly given its significance in the construction of personal identity. Such preparation necessarily involves a process of digital literacy aimed at developing critical skills and discernment, thereby promoting safe and informed use of online tools.

To this end, it is useful to examine how the issue of origin tracing has been addressed in other legal systems. A comparative analysis of normative frameworks, judicial approaches, and administrative practices may offer valuable insights and reflections for the development of more balanced and child-friendly models of intervention, capable of integrating the right to know one's origins with the need for protection, privacy, and appropriate support throughout the digital search process.

---

[67] V. De Santis, *Diritto a conoscere le proprie origini come aspetto della relazione materna. adozione, pma eterologa e cognome materno*, in *Nomos. Le attualità di diritto - Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale*, 2018, pp. 1 ff.

[68] See paragraph 6.

ISSN 2281-5147

5.1 Towards a responsible approach: lessons learnt from the French and UK systems

Continuing from the previous paragraphs, a comparative analysis was carried out on the issue of origin tracing in the legal systems of France and UK. This choice is motivated by several factors.

As far as the French legal system is concerned, various elements must be considered. Firstly, French law shares with Italian law the same historical roots of the adoption institution, both being grounded in the Roman law tradition[69]. Furthermore, with specific regard to the right to origins, France has played a pioneering role in influencing the Italian legal debate[70]. Finally, in terms of the solutions adopted, the French legal framework has opted for a model that significantly diverges from the Italian one.

As for the UK legal system, the comparative interest stems from different considerations, primarily related to the fact that the two countries exhibit profoundly different legal and cultural traditions in the field of adoption. This divergence is reflected in the legal practices and regulations governing access to personal and biological origin information for adopted children, laying the foundation for different approaches to autonomous searches via the internet. These differences mirror distinct conceptions of the right to identity and the protection of the individuals involved.

All these aspects may provide valuable insights for the Italian legal system, which appears to be "caught" in an unresolved situation requiring prompt and well-structured solutions. The first steps in this direction must necessarily include a long-overdue process of digital literacy, which should engage all segments of society, albeit to varying degrees, with the aim of genuinely implementing the principle of the best interest of the child, including within the digital environment.

---

[69] J. Long, *Uno sguardo altrove: l'adozione dei minorenni in Francia, Inghilterra e Spagna,* in *Min. Giust.*, n. 4, 2017, pp. 132 ff.

[70] A. Renda, *La sentenza Odièvre c. Francia della Corte Europea dei diritti dell'uomo: un passo indietro rispetto all'interesse a conoscere le proprie origini biologiche*, in *Familia*, n. 6, 2004, pp. 1109 ff.; A. O. Cozzi, *La Corte costituzionale e il diritto di conoscere le proprie origini in caso di parto anonimo: un bilanciamento diverso da quello della Corte europea dei diritti dell'uomo?*, in *Giur. Cost.*, n. 6, 2005, pp. 4609 ff.; D. Paris, *Parto anonimo e bilanciamento degli interessi nella giurisprudenza della Corte costituzionale, del Conseil constitutionnel e della Corte europea dei diritti dell'uomo*, in *Forum di Quaderni costituzionali*, n. 10, 2012, pp. 447 ff.

ISSN 2281-5147

The French legal system shares with the Italian one the historical and legal foundations that led to the current institution of adoption, governed by Articles 343 ff. of the *Code Civil*. Notably, France is one of the few European countries to allow anonymous childbirth (*accouchement sous X*), introduced to safeguard the life and health of both mother and child[71].Moreover, France has historically served - and continues to serve, as a model for the Italian legal system with regard to the *interpello* procedure (i.e. the process of contacting the birth mother to seek her consent to disclose her identity), which was directly inspired by the French experience[72].

Since 2002, French law has allowed that, notwithstanding the mother's right to give birth anonymously, the child may later request access to information about their origins, subject to the biological mother's consent to waive anonymity[73].

Specifically, this process is facilitated by a dedicated body, the *Conseil National pour l'Accès aux Origines Personnelles* (CNAOP), established within the Ministry of Social Affairs. This body acts as an intermediary: it receives requests from adoptees and attempts to contact the birth mother; if consent is granted, it enables contact between the two parties[74].

This legal mechanism attracted scholarly attention in 2003 when it was brought before the European Court of Human Rights in the landmark case *Odièvre v. France*[75]. In that decision, the Court upheld the compatibility of the French system with Article 8 of

[71] A woman's right to give birth anonymously is provided for both in the *Code de l'action sociale et des familles* (Articles L.222-6 and L.224-5, as amended by Law n.. 2002-93 of 22.1.2002) and in the *Code civil* (Articles 341 and 341-1, as amended by Law 93-22 of 8.1.1993).

[72] N. Falbo, *Il diritto alle origini fra ordinamenti nazionali e giurisprudenza europea. Spunti per una comparazione*, in *Dirittifondamentali.it*, n. 2, 2020, pp. 1060 ff.

[73] L. 2002-92 del 22.1.2002. F. Bellivier, *Accès aux origines. Loi No .2002-92 du 22 janvier 2002 relative à l'accès aux origines des personnes adoptées et pupille de l'Etat*; B. Mallet-Bricout, *Réforme de l'accouchement sous X: quel équilibre entre les droits de l'enfant et le droit de la mère biologique?*, in *JCP*, 2002, pp. 119 ff.

[74] J. Long, *La corte europea dei diritti dell'uomo, il parto anonimo e l'accesso alle informazioni sulle proprie origini: il caso Odièvre c. Francia*, in *Nuov. Giur. Civ. Comm.*, n. 2, 2004, pp. 295 ff.

[75] This is the ruling issued on 13 February 2003, appeal n. 42336/1998. F. Rivero Hernández, *De nuevo sobre el derecho a conocer el propio origen. El asunto Odièvre (sentencia del Tribunal Europeo de Derechos Humanos de 13 de febrero de 2003)*, in *Actualidad Civil*, 2003, pp. 593 ff.; L. Rodríguez Vega, *Los límites del derecho a conocer la propia identidad. Comentario a la sentencia del tribunal europeo de derechos humanos de 13-2-2003, caso Odièvre contra Francia (TEDH 2003, 8)*, in *Repertorio Aranzadi del Tribunal Constitucional*, 2003, n. 4, Parte Estudio.

ISSN 2281-5147

the European Convention on Human Rights, laying the groundwork for subsequent Italian jurisprudential developments.

Although the Italian *interpello* procedure is explicitly inspired by the French model, significant and evident differences remain. First, the French approach is codified in statutory law, whereas Italy still lacks specific legislative intervention, despite long-standing academic and institutional calls for reform. Second, the Italian procedure is entirely judicial in nature, while the French CNAOP operates as an administrative (non-judicial) body. This latter structure is arguably more suitable to perform the mediating role assigned to it by law.

In the context of origin tracing conducted online, the structure of the CNAOP lends itself more readily to integration with the measures outlined in the next paragraph. Its centralised, institutional design is well-suited to balance the right to know one's origins with the privacy rights of those involved. The integration of secure digital tools, identity verification procedures, and protected communication platforms could further enhance its effectiveness, ensuring personalised support, respect for fundamental rights, and greater protection against the risks of indiscriminate use of online platforms.

Digital literacy initiatives could also acquire a more systemic scope if coordinated by a dedicated body capable of addressing the needs of all actors involved: minors, adoptive families, social workers, and institutions. A coordinated, multidisciplinary effort by a specialised unit could develop shared guidelines, provide differentiated and up-to-date training programmes, and design educational tools tailored to different age groups and vulnerabilities. This would strengthen minors' ability to navigate the digital environment in a conscious and safe manner.

With regard to the UK legal system, it is based on entirely different premises[76]. Unlike France and Italy, UK belongs to the group of jurisdictions that automatically recognise parental relationships at birth and do not provide for anonymous childbirth. Under this legal framework, adopted individuals who reach the age of majority may request access to the information contained in their personal file from the competent

[76] The legal framework is broadly similar regarding the legislation in the UK, Wales, Scotland, and Northern Ireland. Specifically, adoption is governed in England and Wales by the Adoption and Children Act 2002; in Scotland by the Adoption and Children (Scotland) Act 2007; and in Northern Ireland by the Adoption (Northern Ireland) Order 1987.

ISSN 2281-5147

court and the adoption agency.
If such information is subject to confidentiality restrictions, the agency has a margin of discretion and must weigh the adopted person's interest against other competing rights and circumstances of the individual case.

To facilitate this, the *Adoption Contact Register* was established[77], allowing adult adoptees, their siblings, and other members of their birth families to express their interest in re-establishing contact with relatives from whom they have been separated. Access to information is granted only where there is a match between registered requests, based on a logic of reciprocity and voluntary contact[78].

As in the French experience, and unlike the Italian model, the English system for accessing origins is structured and governed by legislative provisions, rather than left to judicial interpretation and case law. However, unlike France, UK has opted for a system based on registries and databases, rather than a centralised administrative authority.

Following this approach, the UK has also begun to reflect on origin tracing in the context of medically assisted reproduction (MAR[79]). In this area, the *Donor Conceived Register* and the *Donor Sibling Link* have been established to facilitate, within legal limits, access to information about donors and potential genetic siblings. These tools extend the principle of transparency to non-adoptive but medically assisted forms of parentage[80].

In both legal contexts, however, the issue arises previously discussed of minors seeking information about their genetic past through digital tools and online platforms.

---

[77] Available at https://www.gov.uk/adoption-records. In Scotland, the relevant bodies are National Records of Scotland (https://www.nrscotland.gov.uk/) and Birthlinks (https://birthlink.org.uk/); Northern Ireland has its own Adoption Contact Register (https://www.nidirect.gov.uk/articles/tracing-and-contacting-birth-relatives-and-adopted-adults#toc-4).

[78] O. Faranda, *Il mantenimento della memoria dei bambini adottati nell'esperienza anglosassone*, in *Min. Giust.*, n. 1, 2017, pp 116 ff.

[79] Known also as assisted reproductive technology (ART).

[80] R. Hertz, *The Importance of Donor Siblings to Teens and Young Adults: Who Are We to One Another?*, in F. Kelly, Dempsey D, Byrt A, (eds). *Donor-Linked Families in the Digital Age: Relatedness and Regulation*, *Cambridge University Press*; 2023.

ISSN 2281-5147

England has undoubtedly adopted a more structured approach to ensuring the safety of minors online, but it is not exempt from the safeguards and recommendations outlined above. Despite its institutionalised and regulatory framework for digital safety, the UK system still requires complementary educational measures, support mechanisms, and operational practices to guide minors in a safe, informed, and rights-respecting journey of origin tracing.

Across all three legal contexts examined, there is a clear need to complement the normative frameworks, albeit differing in structure and foundation, with measures that ensure a safe and informed support system for the search for origins conducted through digital means. Within this framework, the promotion of digital literacy plays a central role: adequate digital education is essential to enable minors to navigate the online environment, understand the implications of their choices, recognize potential risks, and protect themselves as well as other parties involved. Secure digital environments and tailored educational pathways should be integrated within a coordinated and multidisciplinary institutional approach. Such a systemic intervention can effectively balance the right to identity and knowledge of one's origins with the safety and protection of all individuals concerned.

6. Search for origin on digital environment: take away recommendations

The Italian legal system, as has been noted, establishes a judicial procedure enabling adopted individuals to initiate research into their origins only once they reach the age of twenty-five. In practice, however, a different reality emerges: many adopted minors pursue information about their biological families through the internet well before reaching that age.

This discrepancy is unsurprising: on one hand, there is the statutory age threshold required by law; on the other, the now-established practice of promptly informing the child of their adoptive status[81]. With such awareness, a desire to explore one's past may arise early on. The internet is the most immediate, convenient, and cost-free medium to commence such an inquiry.

[81] Furthermore, Article 28, paragraph 1 of Law 184/1983 provides that "*the adopted minor is informed of his or her condition and the adoptive parents shall provide for this in the ways and within the terms they deem most appropriate*".

ISSN 2281-5147

Certainly, the wealth of online information, the ease of device usage, and the speed of browsing encourage children and adolescents to pursue their origins domestically. The variety of devices, smartphones, tablets, personal computers, further facilitates autonomous research by young users[82].

Moreover, widespread use of social media provides unprecedented opportunities for connection, expanding how one may come into contact with biological relatives. Although young people often display apparent proficiency in digital environments, they frequently navigate the web unaware of inherent risks and the behavioural dynamics of social platforms. The term "digital natives" may be misleading: being immersed in digital media does not automatically equip minors with appropriate technological competence, especially when their adoptive status might compromise the cautiousness normally expected in online activity[83].

As explored above, the digital environment presents numerous opportunities and risks for minors. In the case of adopted minors, the impact is more significant, particularly absent adequate digital literacy. Nonetheless, multiple and varied benefits should not be overlooked or dismissed.

First and foremost is access to knowledge of one's cultural and geographical roots, whether in international adoptions (outside Italy) or domestic ones (adoption across regions within Italy), which supports the development of personal identity. Likewise, connecting with peers facing similar experiences can be beneficial: healthy peer interaction and shared experiences may reduce the isolation and distress often felt by adopted individuals.

In general, origin-related research can serve as an educational opportunity, stimulating interests in history, geography, or the language of the country of origin, and fostering

[82] G. Mascheroni, A. Cuman, *Net Children Go Mobile: Final Report*, Educatt, Milano, 2014; G. Mascheroni, K. Ólafsson, *Net Children Go Mobile: risks and opportunities. Second edition*, Milano: Educatt, 2014; C. Garitaonandia; I. Karrera, N. Larrañaga, *Media convergence, risk and harm to children online*, in *Doxa Comunicación*, n. 28, 2019, pp. 179 ff.

[83] M. Prenksy, *Listen to the Natives*, in *Educational Leadership*, v. 63, n. 4, 2005, pp. 8 ff.; A. Guarini, *S.M.E.N., Internet e social: i ragazzi raccontano le possibilità e i rischi della rete*, in *I Quaderni dell'Ufficio Scolastico Regionale per l'Emilia Romagna,* 2018, pp. 61 ff.; M. Martoni, *Datificazione dei nativi digitali. Una prima ricognizione e alcune brevi note sull'educazione alla cittadinanza digitale*, in *Federalismi.it*, 8 January 2020.

ISSN 2281-5147

digital, cultural, and relational competencies, thus empowering the individual[84]. Additionally, autonomous research allows the minor to choose the pace and mode of inquiry, aligning with their emotional rhythm and cultivating self-awareness of needs, desires, and curiosity.

Another positive dimension of such online research is access to legal resources: the minor can gain information about their rights as an adopted individual, the protections available, and the instruments designed specifically with origin-search procedures in mind[85].

These advantages are counterbalanced by a similarly extensive array of risks to which adopted minors, experienced web users, children or adolescents, are exposed when conducting origin research via digital devices.

Impulsivity, a characteristic common in youth, coupled with the powerful desire to reconstruct one's personal history, renders adopted minors particularly vulnerable to digital risks, amplifying their consequences. Typical online hazards, such as privacy breaches, exposure of personal or non-personal data, grooming, emotional manipulation, fraud, identity theft, and scams, take on heightened significance.

Specifically, the emotional intensity of origin searches may lead the minor to initiate and sustain contact with strangers whom they might otherwise distrust, contravening basic safety guidelines. Even prudent behaviour during the inquiry cannot eliminate significant risks: children and adolescents may still encounter misinformation or harmful content that can profoundly affect identity formation.

Furthermore, even when research yields tangible results, minors may not be psychologically prepared to process those outcomes, which could provoke emotionally destabilizing or even traumatic effects, especially absent adequate psychological support. When such research is conducted autonomously or clandestinely, without adult awareness or guidance, it becomes difficult to manage potentially life-altering revelations.

[84] G. Martínez, M. Garmendia, C. Garitaonandia, *La infancia y la adolescencia ante las Tecnologías de la Información y la Comunicación (TIC): oportunidades, riesgos y daño*, in *Zer*, 25(48), 2020, pp. 349 ff.
[85] M. Casonato, *Adolescenti "in rete": navigare alla ricerca delle proprie origini*, in *Min. Giust.*, n. 4, 2015.

ISSN 2281-5147

The modalities of origin research online vary. Some minors may post announcements on dedicated websites, though many of these platforms are unsuitable for minors, containing advertisements, donation requests, or product sales[86]. Certain sites offer DNA testing kits for purchase, often promising access to census records, passenger lists, or birth registries in exchange for payment[87].

Social media usage is the most common method for locating biological relatives: through dedicated Facebook groups, specialized hashtags, or personal reels recounting one's story, sharing photos or documents, and appealing to the internet community. Such practices sacrifice basic safety measures: they frequently compromise privacy and encourage sharing information with anyone who expresses interest.

Similarly, there are online services offering accompaniment for origin searches in the adoptee's country of origin. Many of these services lack official certification or guarantees of professionalism, transparency, and reliability[88]. Often, they advertise the possibility of direct contact between the adoptee and a found relative without psychological or legal mediation. This exposes minors to significant emotional, safety, and rights-related risks, particularly when the desire to reconnect intersects with fragile expectations and deep emotional needs.

Moreover, beyond scenarios where the adoptee initiates research, it is increasingly common for biological relatives to search for and contact the minor via digital means. In the social media era and with widespread sharing of personal information, unexpected contact can lead to complex and potentially invasive dynamics. It is therefore essential to prepare adopted minors to handle unsolicited contact, including from biological family, through digital literacy and protection of their private sphere, to safeguard their psychological well-being and security.

---

[86] B. Bertetti, *Adottivi italiani alla ricerca delle origini: voci dal web*, in *Min. Giust.*, 2013, n. 2, pp. 203 ff.

[87] Suffice it to say that the website Ancestry.it promises to reconstruct your family tree for 199 euros a year, offering "*access to over 20 billion historical documents from Italy and around the world*".

[88] There are certainly valid services: Ser.I.O. is an Italian service that provides comprehensive assistance in the search for origins but scrupulously adheres to the age limits required by law. The results can be consulted at M. Parente, L. Ricciardi, *Centro Regionale di documentazione e ricerca per l'infanzia e l'adolescenza, La ricerca delle informazioni sulle origini. Riflessioni sulla complessità dei processi e proposte per un percorso condiviso*, 2022, Istituto degli Innocenti, Firenze; The same can be said for Radici Russe, based in France, whose activity is visible on https://russianroots.org/en/achievements/.

ISSN 2281-5147

Considering these dynamics, integrating robust digital literacy initiatives into adoption support pathways is essential.

Equipping minors with tools to navigate the digital environment consciously involves not only imparting technical skills but primarily educating them to recognise risks, protect their online identity, and critically assess information and contacts, including those originating from their familial background. Digital literacy functions here as a cornerstone of self-determination, security, and emotional safeguarding within an increasingly complex and permeable online ecosystem. Furthermore, against this background, it serves as a practical tool for achieving the child's best interests, as required by national and international regulations.

Based on these considerations, practical recommendations grounded in a children's rights-based approach may be directed to multiple stakeholders: legislators; social services; businesses; professionals (educators, psychologists); minors; and parents[89].

The first set of recommendations concerns the legislator, who bears the urgent and inescapable responsibility of developing a modern, child-centered legislative framework, capable of responding to the pressing contemporary relevance of the issue.

First and foremost, it is necessary to follow up on Constitutional Court judgment by introducing the formal request mechanism (so-called *interpello*), which has already been validated through the consolidated practice of Italian courts. However, such legislative action should not merely comply with the Court's recommendations but should instead take into account - and adapt to - the realities of the digital environment, while at the same time ensuring the full spectrum of safeguards that children currently require, including the protection of privacy, identity, and the right to be heard.

On one hand, it would be appropriate to reconsider the minimum age requirement for access to the origin-search procedure currently established by Italian law. On the other hand, it is essential to address the growing phenomenon of online origin searches, by acknowledging the associated risks and the potential impact on minors involved. This includes a thorough evaluation of the implications of digital

[89] For the specific set of policy recommendations targeting young adoptees, see *CURA Blueprint Guidelines*, *cit.*, pp. 14-8.

ISSN 2281-5147

technologies and artificial intelligence algorithms, particularly regarding their role in facilitating unauthorized or unexpected contacts between adopted minors and their biological relatives.

Therefore, the law itself should also reinforce the capacity of social services to implement psychological support programs for those minors who express the need to inquire into their biological origins.

Moreover, it would be desirable to establish a clear procedure for conducting origin searches even in cases of international adoption, taking full advantage of the unprecedented opportunities offered by the web[90]. In addition, another area where legislative intervention would be appropriate concerns the establishment of an institutional, public, free-of-charge, and specialized service to mediate origin searches, available to individuals who wish to make use of such support[91].

More broadly, there is a compelling need to promote policies that require digital platforms to adopt specific measures aimed at recognizing and mitigating the potential emotional harm caused by the repeated and automated exposure to adoption-related content and narratives.

Given the importance that social services play in the field of pre- and post-adoption, being called to accompany the family unit that has embarked on the path of adoption so that the best interest of the child is guaranteed, some recommendations must also be made with respect to them.

These are measures designed with the objective of creating a specialized sector within the public service, focused on the needs of adopted minors, equipped to manage origin searches, including those conducted online, and active throughout the national territory.

Certainly, it is of primary importance to rethink university education in Social Work, strengthening academic programs in order to better prepare future professionals for

[90] Currently, the origins search is only available for national adoptions, not international ones. Despite this, the number of applications from international adoptees is increasing: R. Romano, *Parto anonimo e interpello: considerazioni alla luce di uno studio sulle prassi in uso presso il Tribunale per i Minorenni di Trento,* in Fam. Dir., n. 7, 2024, pp. 709 ff.

[91] Similar to the French CNAOP: see previous section.

ISSN 2281-5147

the complexities of contemporary social challenges[92]. Still on the academic level, it is fundamentally important to invest in research on the well-being of minors, allocating resources to studies that guide evidence-based practices and policy development in the sector[93].

Similarly, coordination among territorial social services is desirable, establishing collaboration mechanisms to harmonize practices and share best approaches. This would facilitate the implementation of uniform procedures at the national level, as well as the standardization of processes among regions, to ensure fair provision of services and protect the rights of minors throughout the country.

The guarantee of consistency and quality in social services should also be ensured through the publication of guidelines and the dissemination of standardized protocols[94].

With regard to the focus on the online search for origins, the development of specialized training programs and guidelines for social workers is necessary, focusing on digital literacy, emotional intelligence, and understanding of the risks related to algorithms.

This with the aim of preparing them to effectively support adopted minors and families in managing emotional distress and unexpected online encounters with biological relatives.

Finally, the drafting of psychological support protocols specifically addressing digital vulnerabilities and emotional triggers specific to adopted minors conducting online searches on their biological origins would also constitute a valuable operational tool.

---

[92] Indeed, it's the Social Work's code of ethics itself that establishes in the preamble that "*Social workers are required to systematically improve their knowledge and skills through processes of constant debate, training, and self-reflection, to ensure the proper practice of the profession*" (on chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cnoas.org/wp-content/uploads/2020/03/Il-nuovo-codice-deontologico-dellassistente-sociale.pdf).

[93] As suggested by A. Bartolomei, E. Tognaccini, *Il diritto del minore agli interventi necessari: affidamento solidaristico e/o al servizio sociale (d.l. n. 149 art. 5-bis)*, in Min. Giust., n. 2, 2022, pp. 34 ff.

[94] A. Bartolomei, E. Tognaccini, *cit.*

ISSN 2281-5147

Regarding the category of economic operators, the aim is to establish a series of safety measures to make platforms safer for adopted minors engaged in the search for their origins.

First and foremost, the mandatory integration of privacy by design and by default, as required under Article 25 GDPR, should be ensured in the design of digital products and services, adapted to the possible vulnerabilities of users.

Also the regular conduction of audits and vulnerability assessments, on the one hand, and the drafting of reporting and response protocols for security incidents, on the other, would be part of a strategy aimed at making the activities of economic operators more child-friendly, in line with the obligations set out in the DSA (Art. 34 ff.) concerning systemic risk assessment and mitigation.

Among the other measures that could be adopted are greater attention to content moderation, the promotion and adoption of specific codes of conduct, pursuant to Article 95 of the recent AI Act, and the inclusion of specific warnings for sensitive topics (e.g.: bulletins similar to TV news, mandatory warnings similar to cookie notifications).

Moreover, such economic operators should promote and support investment in the research and development of ethically oriented digital technologies and artificial intelligence systems, structurally involving experts in child development and applied ethics. This interdisciplinary collaboration is essential to ensure that the design of digital products takes into account the developmental, cognitive, and emotional needs of minors, particularly in highly sensitive contexts such as origin searches by adopted individuals.

In parallel, it is essential to implement digital safety measures specifically calibrated to the characteristics of different digital platforms, such as social media and search engines. These measures should be able to proactively prevent the activation of undesired algorithmic connections, which could expose the minor to unsolicited contact with biological family members or to potentially destabilizing content. Such an approach aims not only to protect privacy and safety but also to safeguard the emotional and psychological well-being of adopted minors during delicate journeys of online identity reconstruction.

ISSN 2281-5147

It is recommended to provide targeted educational materials and guidelines that specifically address the digital risks to which adopted minors may be exposed, such as unexpected online contact with biological relatives or the emotional impact resulting from content recommended by AI-based systems.
It is also appropriate to provide professionals with practical tools and adequate training to support adoptive families in understanding and managing the emotional and identity implications connected to the search for origins online. his approach is consistent with the principle of the best interests of the child enshrined in Article 3 UNCRC.

Lastly, it is essential to promote the development of guidelines aimed at supporting adopted minors in developing emotional resilience and building conscious and responsible digital practices.

As far as the category of professionals is concerned, including educators and psychologists, the goal is to provide tools that prevent the scenario in which the minor autonomously initiates an origin search on the web, in the absence of appropriate accompaniment.

Also in this case, it is useful to act already from the stage of professional training, introducing awareness programs on the issue of origin search addressed to adoptive families (both to parents and minors). This helps to increase awareness of the online risks, in line with the preventive and educational function assigned to parental and professional figures under Articles 5 and 18 UNCRC, as well as with the duty of parental responsibility recognised under Articles 2 and 30 of the Italian Constitution. These programs should provide explicit examples of concrete scenarios of exploitation of user vulnerabilities, also based on age and individual needs., echoing the requirements of age-appropriate design and protection of minors' data under Recital 38 and Article 8 GDPR, as well as the Age-Appropriate Design Code which, although originating from the UK, has been influential at the European level.

Certainly, this digital literacy activity requires active listening from parents, so that they learn to interpret their parental duties – such as education, care, protection - in a "digital perspective": thus, allowing for the introduction of possible alerts as preset functions on devices available to minors, in order to monitor search and access to specific social networks/groups related to the domestic search for origins through parental control tools.

ISSN 2281-5147

Last only in expository order, but central in relevance, is the category of minors, subjects around whom the entire discipline of adoption revolves and who, in recent times, have attracted the attention of the legislator as particularly active users of the digital environment.

As seen, the increasing use of digital tools has deeply transformed the delicate theme of origin search, which has taken on new forms and characteristics, requiring appropriate tools for accompaniment and protection.

In this context, it is fundamental to provide minors with clear, legally grounded and psychologically respectful guidance, so that the search for origins takes place in a safe and conscious way.
First of all, it is appropriate to encourage the minor not to undertake this journey alone, but to talk to a trusted adult figure, such as a parent, guardian or teacher, who can offer listening, guidance and support.
Secondly, it is essential to promote awareness regarding personal information shared online. Data such as adoptive status, date or place of birth, if publicly disclosed, can make the minor traceable in unexpected and potentially dangerous ways. Therefore, the publication of generic messages (e.g. "*I am looking for my biological family*") on open forums or publicly accessible social platforms should be discouraged. Alternatively, safer digital environments can be considered, such as closed and moderated groups, which offer greater guarantees of confidentiality and protection.
It should also be emphasized that caution is needed towards those who might make contact online claiming a family bond. In such situations, it is advisable to take time, avoid immediately providing sensitive information (such as phone numbers, addresses or other personal data), and maintain a vigilant attitude.

Another relevant aspect concerns emotion management. The journey of origin search can indeed stir up complex and conflicting feelings that need to be acknowledged and, where possible, accompanied by competent figures. In this sense, the involvement of a professional may prove particularly useful. It is also fundamental to promote respect for one's own personal story and that of others. Every adopted person has the right to decide whether and how to share their own story, just as biological relatives retain a right to privacy.

Finally, minors should be made aware of their rights regarding access to information about their origins. As seen above, in Italy the legal system recognizes to adopted

ISSN 2281-5147

persons, once certain requirements are met, the possibility to undertake an official path of reconstructing their family history. Before turning to informal tools such as the internet, it is therefore important to check the existence of appropriate legal channels, being able to count on the support of specialized operators, such as social workers, authorized bodies, or lawyers expert in family law.

If these recommendations were actually followed by all the subjects involved in this delicate scenario, the digital search for origins would be more oriented towards ensuring the delicate balance between identity protection, digital safety, and the right to knowledge, protecting all the figures involved in the field.

Overall, the good practices and recommendations examined and proposed thus far may contribute to making the search for origins not only more structured, but also less exposed to risks concerning the safety of minors. The adoption of an integrated, multi-level, and comparative approach makes it possible to lay the foundation for a complex yet essential intervention: the promotion of digital literacy. This effort goes beyond merely fostering greater awareness among the parties involved. It also aims to achieve genuine empowerment of minors by strengthening their ability to navigate the digital environment in an informed and autonomous manner.

7. Digital Education as a Response to (not only digital) Vulnerability: educational practices and regulatory frameworks

As emphasized in the previous sections[95], digital literacy represents a cornerstone of minor-centered strategies aimed at transforming vulnerability into agency within digital ecosystems. Moving beyond purely legal and technical interventions, the educational dimension emerges as a key lever for promoting resilience, critical awareness, and informed participation. In the era of pervasive digitalization, digital literacy, defined as the ability to access, understand, evaluate, and create content through technology, is crucial for citizen education and full citizenship, especially among minors[96]. Children and adolescents grow up in a context where the distinction

[95] Relevant to this point, see paragraphs 4 and 7above.

[96] See G. Spadafora, *Processi didattici per una nuova scuola democratica* (vol. 1), Anicia, 2018.

ISSN 2281-5147

between online and offline is increasingly blurred, with profound effects on social interaction, learning, identity construction, and the exercise of rights.

The following sections expand on this viewpoint by going into greater detail about the theoretical underpinnings and civic significance of digital literacy, particularly in light of the larger framework of democratic citizenship and global social inclusion. The discussion that follows in the next paragraphs places digital and media education at the nexus of civic engagement, ethical responsibility, and human rights, emphasising its crucial role in educating the next generation to navigate, influence, and engage in the digital society.

Digital literacy is the new citizenship[97], as it allows individuals to participate consciously and critically in public life, countering phenomena such as misinformation, hate speech, and digital exclusion. Digital education is therefore no longer simply a technical matter, but a profoundly civic and social process[98].

Digital skills are not exclusively technical but include critical, ethical, and relational dimensions that enable citizens - including minors - to actively participate in democratic life, exercise their rights, and recognize their duties, even in the digital space[99]. For this reason, digital literacy is an essential component of global citizenship, inextricably linked to the ability to participate consciously, critically, and responsibly in democratic life. It represents an essential tool for building more inclusive, peaceful, and sustainable societies, as also recognized by the United Nations 2030 Agenda[100].

The analytical approach adopted in the following sections is grounded in the conviction that digital citizenship education plays a pivotal role in ensuring the meaningful participation and protection of minors within digital environments. Building on the foundations established by the EU regulatory framework, the next section conducts a comparative examination of three countries that have integrated digital civic education into their educational curricula: Italy, the United Kingdom, and

---

[97] See P. Mihailidis, *Civic media literacies: Re-imagining engagement for civic intentionality*, in *Learning, Media and Technology*, 43(2), 2018, pp. 142-164.

[98] See D. Buckingham, *Media education goes digital: an introduction,* in *Learning, Media and technology*, 32(2), 111-119, 2007, pp. 111-119.

[99] See UNESCO, *Digital literacy in education. Policy brief,* 2011. Retrieved from: https://iite.unesco.org/publications/3214688/

[100] See United Nations, *Transforming our world: The 2030 Agenda for Sustainable Development*. United Nations General Assembly, 2015. Available at https://sdgs.un.org/2030agenda.

ISSN 2281-5147

France. The goal is not only to evaluate the normative and pedagogical strategies used, but also to determine how these educational systems respond concretely to children's evolving vulnerabilities in increasingly digitalised societies in order to promote a comprehensive, cross-sectoral framework of digital citizenship education that actively involves professionals across education, social services, health, justice, and the digital sector, as well as families and communities, recognising their central role in upholding and advancing children's rights in digital environments[101].

From this perspective, the OECD highlights that the development of advanced digital skills is essential for training active citizens, capable of navigating the complexity of the 21st century and contributing to the ethical, cultural, and social evolution of the communities in which they live[102].

This close connection between digital literacy and civic citizenship means that digital education also includes education about legality, democratic participation, civil coexistence, and respect for fundamental rights, including those related to privacy, freedom of expression, and the protection of personal data.

In the context of contemporary digital society, it is essential that digital citizenship promotes an ethic of responsibility, legality, and active participation in an interconnected society. As a result, digital literacy entails teaching people critical thinking skills, online legality, respect for others, and an understanding of their digital rights and responsibilities.

In this perspective, the values and responsibilities associated with digital citizenship must be understood within the broader context of a hybrid reality, where the boundaries between online and offline life are increasingly blurred. This shift calls for a more integrated approach to digital education—one that acknowledges the "onlife"[103] dimension of contemporary experience and its impact on identity, relationships, and the exercise of rights[104].

---

[101] *CURA Blueprint Guidelines*, *cit.*

[102] See OECD, *21st-Century Readers: Developing Literacy Skills in a Digital World*, PISA, OECD Publishing, Paris, 2021. Available at https://doi.org/10.1787/a83d84cb-en.

[103] L. Floridi, *The onlife manifesto: Being human in a hyperconnected era, cit.*

[104] S. Livingstone, E. Helsper, G*radations in digital inclusion: Children, young people and the digital divide,* in *New media & society*, 9(4), 2007, pp. 671-696.

ISSN 2281-5147

The analysis presented in the preceding sections highlights the complex and multifaceted risks that threaten personal freedoms, particularly those of minors, if robust safeguards for digital integrity and rights are not fully implemented. In today's interconnected world, the actions of children and adolescents in both physical and digital spaces leave behind data traces that, once aggregated and analysed, generate a level of informational power far exceeding that of the original inputs. This raises serious concerns about profiling, surveillance, and the erosion of privacy.

Minors are especially vulnerable to a wide spectrum of online risks, including cyberbullying, grooming, the non-consensual sharing of images, and exposure to disinformation[105]. At the same time, they are increasingly affected by issues such as digital dependency, social comparison pressure, and premature contact with harmful content. Addressing these challenges requires more than just protective measures; it calls for an educational approach that fosters both safety and the gradual development of digital autonomy.

Digital and citizenship competences are two of the eight key competencies promoted by the Council of European Union[106] from a lifelong learning perspective, from early childhood to adulthood, through formal, non-formal, and informal learning in all contexts, including family, school, workplace, neighbourhood, and other communities.

According to the definitions in the Council of European Union Recommendation of May 22, 2018, digital competence focusses on the technical and cognitive skills required to use digital tools effectively: it entails knowing how to find, evaluate, and communicate information online, as well as how to use various platforms and manage digital risks[107]. Citizenship competence is defined as the ability to act responsibly and actively participate in civic and social life while understanding social, economic, legal,

[105] D. Smahel, H. Machackova, G. Mascheroni, L. Dedkova, E. Staksrud, K. Ólafsson, U. Hasebrink, *EU Kids Online 2020: Survey results from 19 countries*, 2020.

[106] Council of the European Union. (2018). Council Recommendation of 22 May 2018 on key competences for lifelong learning (2018/C 189/01). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018H0604(01).

[107] Council of the European Union (2018/C 189/01), *cit.* See in Annex, point 4: "*Digital competence involves the confident, critical and responsible use of, and engagement with, digital technologies for learning, at work, and for participation in society. It includes information and data literacy, communication and collaboration, media literacy, digital content creation (including programming), safety (including digital well-being and competences related to cybersecurity), intellectual property related questions, problem solving and critical thinking*".

ISSN 2281-5147

and political structures and concepts, as well as their global evolution and sustainability principles[108].

The concept of digital literacy has gradually expanded to include an educational component, resulting in the concept of digital citizenship education. This shift reflects the need to promote structured learning that develops broader and deeper skills, rather than simply mastering the technical aspects of digital tools.

The digital citizenship education paradigm is systematically adopted in the Digital Citizenship Education Handbook[109] and serves as a key European reference for the definition, promotion, and implementation of digital citizenship education. The text provides a clear and comprehensive conceptual framework for linking responsible use of digital technologies to democratic principles, human rights, and the rule of law. The handbook, organised around ten competency domains, offers practical and pedagogical tools for teachers, educators, and education policymakers with the goal of developing active, informed, and inclusive digital citizens. Its function is both normative and transformative: it promotes civic education that is current with the challenges of the digital world, focussing on participation, ethics, and social cohesion.

In line with this vision, the European Commission further clarifies the idea of digital literacy and its close connection to citizenship competence.

With the Digital Competence Framework for Citizens (DigComp), European Commission defines digital citizenship as the set of skills needed to use digital technologies safely, ethically, and participatively in education, work, information, and civic engagement[110].

---

[108] Council of the European Union (2018/C 189/01), *cit.* See in Annex, point 6: "*Citizenship competence is the ability to act as responsible citizens and to fully participate in civic and social life, based on understanding of social, economic, legal and political concepts and structures, as well as global developments and sustainability*".

[109] J. Richardson, E. Milovidov, *Digital citizenship education handbook: Being online, well-being online, and rights online*, Council of Europe, 2019.

[110] R. Vuorikari, S. Kluzer, Y. Punie, *DigComp 2.2: The Digital Competence Framework for Citizens-With new examples of knowledge, skills and attitudes,* 2022. DigComp's framework, developed as a scientific project by the Joint Research Centre (JRC) with significant input from various stakeholders, was published in 2013 and has since become an essential reference point for the formulation and implementation of digital skills strategies at both the European and Member State levels. The first edition, titled DigComp: A Framework for Developing and Understanding Digital Competence in Europe, describes digital competence by starting with the needs that every citizen of the information and communication society has. The DigComp model is based on these needs, which include being informed, interacting, expressing oneself, protecting oneself, and dealing with

ISSN 2281-5147

Although the younger generations are considered digital natives[111], it is important to remember that digital technology is not always designed to meet these new demands. As we have seen in previous sections, minors are more vulnerable to the dangers of the internet. As a result, adult figures, particularly teachers, must be aware of the influence they can have on children's development and their relationship with information and communication technology. Educators must therefore develop effective digital skills.

In 2017, the European Commission developed a framework for teachers and educators' digital skills. The "European Framework for the Digital Competence of Educators: DigCompEdu"[112] is divided into six competency areas: professional engagement; digital resources; teaching and learning; assessment; empowering learners; facilitating learners' digital competence.

DigCompEdu is a model that allows for the description of digital pedagogical competence, the level of mastery, and self-assessment[113].

The European Commission has consistently underscored the strategic importance of digital competence as a key enabler of economic growth, innovation, and social cohesion. In addition to the DigComp framework, several major policy initiatives reflect this commitment - most notably the Digital Education Action Plan 2021 -

technological and digital environment problems. The DigComp model matrix consists of five dimensions. Dimension 1 contains the title of the competence area. Dimension 2 indicates the competence's title and description. Dimension three is dedicated to mastery levels. Dimension 4 provides examples of knowledge, skills, and attitudes that are not differentiated into mastery levels. Dimension 5 demonstrates the competence's applicability in employment and learning scenarios. A three-phase update procedure was started, utilising the DigComp first edition matrix. The first update was R. Vuorikari, Y. Punie, S. C. Gomez, G. Van Den Brande, *DigComp 2.0: The digital competence framework for citizens*, 2016. The second update was G. S. Carretero, R. Vuorikari, Y. Punie, *DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use*, 2017. Finally, *DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills, and attitudes*, *cit.*

[111] M. Prensky, *H. sapiens digital: From digital immigrants and digital natives to digital wisdom*, in *Innovate: journal of online education*, 5(3), 2009.

[112] C. Redecker, *European Framework for the Digital Competence of Educators: DigCompEdu*, Y. Punie, (ed)., EUR 28775 EN. Publications Office of the European Union, Luxembourg, 2017.

[113] "*Selfie for teachers*" is a tool based on DigCompEdu managed by the European Commission that allows teachers to evaluate their digital competence. It is one of the initiatives of the action plan or the commission for digital education. Available in https://education.ec.europa.eu/selfie-for-teachers.

ISSN 2281-5147

2027[114], which outlines a vision for high-quality, inclusive, and accessible digital education across the EU, and the Digital Decade Policy Programme 2030[115], which sets concrete targets for digital skills, infrastructure, and public services within the broader context of Europe's digital sovereignty and resilience.

Through these initiatives, the European Union is actively fostering the development of both basic digital literacy, essential for everyday life and civic participation, and advanced digital skills, such as data literacy, coding, and artificial intelligence, which are increasingly crucial for employability and competitiveness. This dual focus aims not only to support the digital transformation of education and the labour market, but also to promote digital inclusion, ensuring that all citizens, regardless of age, background, or socioeconomic status, can engage meaningfully and safely in the digital society. Particular attention is given to children and adolescents, who are among the most vulnerable users of digital technologies and therefore require targeted educational support and protection to develop the critical, ethical, and technical skills needed to navigate digital environments responsibly.

As digital technologies evolve rapidly, the concept of digital competence must also expand to address the emerging challenges posed by artificial intelligent (AI) systems. Beyond ensuring broad access and inclusion, especially for vulnerable groups such as minors, it is increasingly necessary to equip all citizens with the ability to critically engage with the technologies shaping their environment. In this broader educational vision, digital literacy becomes the stepping stone toward more advanced and nuanced forms of competence, most notably, AI literacy, which demands not only technical understanding but also ethical sensitivity, critical thinking, and social responsibility in the face of algorithmic decision-making and data-driven processes.

In this context, the European Union has launched initiatives to enhance awareness of AI and data in education, starting with the Ethical Guidelines for Educators on Using

[114] European Commission: Directorate-General for Education, Youth, Sport and Culture, *Digital education action plan 2021-2027 – Improving the provision of digital skills in education and training*, Publications Office of the European Union, 2023, https://data.europa.eu/doi/10.2766/149764.

[115] https://digital-strategy.ec.europa.eu/en/library/digital-decade-policy-programme-2030.

ISSN 2281-5147

AI and Data in Teaching and Learning[116], aiming to increase awareness of AI and data in education.

8. The role of educational institutions and educational alliances: a comparison between Italy, United Kingdom, and France

Educational institutions play an important role in promoting digital citizenship. They are expected to educate not only on the use of technology, but also on its critical, informed, and responsible application. In this context, establishing educational alliances between schools, families, and communities becomes critical.

From this perspective, educational policies serve as a starting point for providing schools with the tools and vision required to address the challenges of digital transformation, all while strengthening the educational relationship as the foundation of learning.

Regulatory strategies governing digital literacy and citizenship education vary across European contexts, reflecting distinct cultural visions and educational priorities.

In Italy, the National Digital School Plan[117] (hereinafter PNSD) identify innovation strategies for Italian schools in the digital age, with a focus on the epistemological and cultural dimensions of the educational relationship[118].

[116] See European Commission: Directorate-General for Education, Youth, Sport and Culture, Ethical guidelines on the use of artificial intelligence (AI) and data in teaching and learning for educators, Publications Office of the European Union, 2022, https://op.europa.eu/en/publication-detail/-/publication/d81a0d54-5348-11ed-92ed-01aa75ed71a1/language-en.

[117] Piano Nazionale Scuola Digitale, DM 851 del 27 ottobre 2015, https://www.istruzione.it/scuola_digitale/index.shtml.

[118] In light of the profound digital transformation that is affecting the Italian school system, the PNSD emphasises the importance of consciously and responsibly integrating technology into educational processes. Despite the emphasis on innovation, the Plan emphasises the importance of keeping the relationship between teacher and student at the heart of the educational process, recognising that human interaction is still an irreplaceable component even in the age of digital education (Since "technology cannot elude this fundamental human relationship and no educational step can be separated from an intensive teacher-student interaction" (PNSD, 2015, p. 7).

ISSN 2281-5147

As part of this plan, specific figures such as digital animators[119] and innovation teams were introduced to foster informed use of digital technologies in educational settings.

Following that, the Italian Minister of Education approved issued Decree No. 161 on June 14, 2022, approving the School Plan 4.0[120], which was funded by the Italian Recovery and Resilience Plan. This builds on the experience of the previous PNSD, which aimed to transform country's classrooms into ecosystems for integrated digital teaching in which analogue and digital, physical and digital, school and local communities converged to form an innovative and well-organised project. Although these efforts mark a structural shift, explicitly aligned with European frameworks such as DigComp 2.2[121] and DigCompEdu[122], the current approach remains predominantly focused on infrastructure and the general enhancement of basic digital skills. It lacks, however, sufficient regulatory and organizational measures to ensure the systematic protection of minors in digital environments, as well as meaningful progress in digital literacy.

The Italian Law No. 92 of August 20, 2019[123], which introduced civic education into the national school curriculum, represents a shift towards a more forward-looking and systemic vision, as does the growing recognition of the importance of prioritising digital and AI education to equip future generations with the skills required in a rapidly evolving digital society.

---

[119] The PNSD's Action #28 section provides a comprehensive and official description of the Digital Animator profile, outlining their responsibilities, areas of intervention, and strategic significance in the process of digitally transforming Italian schools. The Digital Animator must create projects in three crucial areas in order to fulfil Action #28: - internal school training, which is accomplished by planning and directing training sessions and events that involve the school community; - participation of the school community, promoting students', families', and local stakeholders' involvement in order to establish a common digital culture; - the development of novel, sustainable, and technologically and methodologically sound solutions that meet the needs of the school. This position is not just a technical support role; it is a systemic role. It receives training through specialised programmes that support educational innovation and digitisation, in line with the initiatives delineated in the Three-Year Educational Offer Plan (PTOF).

[120] Decree of the Italian Minister of Education, 14 June 2022, n. 161, which adopts "*Piano scuola 4.0*", provided for by *Piano nazionale di ripresa e resilienza*, https://www.mim.gov.it/-/decreto-ministeriale-n-161-del-14-giugno-2022.

[121] *DigComp 2.2: The Digital Competence Framework for Citizens-With new examples of knowledge, skills and attitudes, cit.*

[122] *European Framework for the Digital Competence of Educators: DigCompEdu, cit.*

[123] Law 20 August 2019, n. 92 "*Introduzione dell'insegnamento scolastico dell'educazione civica (Introduction of civic education teaching in schools)*", https://www.gazzettaufficiale.it/eli/id/2019/08/21/19G00105/sg.

ISSN 2281-5147

The law promotes the development of responsible and active citizenship by encouraging full and informed participation in civic, cultural, and social life, in accordance with the principles of rights, duties, and rule of law and duties.

In particular, Law 92/2019 establishes "digital citizenship" as one of the three pillars on which to build the 33 transversal hours of the new teaching, along with the "constitution" and "sustainable development"[124]. From this perspective, the emphasis is not on technological literacy, but on a more proactive approach centred on the five areas that comprise it: the Internet and ongoing change, media education, information education, quantification and computation: data and artificial intelligence, digital culture and creativity[125].

Law 92/2019, which established civic education as a transversal subject, identifies in Article 3 a set of skills and learning objectives related to three major thematic areas: the "constitution" (in the broad sense, national and international law, legality, and solidarity); "sustainable Development" (and environmental education, as well as knowledge and protection of heritage and territory); and "digital citizenship"[126]. This emphasises the significance of digital citizenship education as a central theme with broad educational goals. These objectives address both cognitive and non-cognitive skills, including the digital dimension, and use their transversality to make meaningful connections between learning areas.

---

[124] Decree of the Italian Minister of Education, n. 183, 7 September 2024, "*Adozione delle Linee Guida per l'insegnamento dell'educazione civica*", Gazzetta Ufficiale della Repubblica Italiana, 2024, https://www.istruzione.it/educazione_civica/norme.html.

[125] S. Past, a P.C. Rivoltella, *Crescere onlife. L'Educazione civica digitale progettata da 74 insegnanti-autori*. Morcelliana Scholé, 2022.

[126] Article 5 of Law n. 92/2019, which details the essential digital skills and knowledge to be developed in relation to the core theme of digital citizenship, identifies seven areas of interest that are directly linked to the areas of the European Framework of DigComp 2.2.

1. Analyse, compare, and critically assess the credibility and dependability of sources.
2. Interact with various digital technologies and determine the best method of communication for a given situation.
3. Obtain information and participate in public debate using public and private digital services.
4. Understand the rules of conduct when using technology.
5. Create and manage a digital identity, protect one's reputation, and manage and secure data.
6. Learn about digital services' privacy policies.
7. Be able to identify and avoid health risks and threats to one's physical and psychological well-being, as well as understand how technologies affect them.

ISSN 2281-5147

In 2023, the United Kingdom passed the *Online Safety Act*[127], one of Europe's most advanced pieces of legislation for protecting minors online, imposing a duty of care on platforms.

Section 166 of the *Online Safety Act* adds a new section 11A to the Communications Act, requiring the Office of Communications (Ofcom)[128] to develop and publish a media literacy strategy within one year of the *Online Safety Act*'s passage.

Ofcom's mandate includes the development of a media literacy programme called "Making Sense of Media"[129] (hereinafter MSOM). The MSOM focusses on two key dimensions: people and online platforms. The documented work focusses on platform interventions to promote media literacy, analysing how regulated services address this issue directly "on-platform" and developing a set of best practice principles for social media, search engines, video sharing, and gaming services.

MSOM's goal is to identify what works and what doesn't work online in order to help users improve their media skills.

Ofcom has developed 14 principles for "good media literacy by design" as part of the MSOM programme, specifically for social media, search, video sharing, and gaming services. Adopting these principles would allow platforms to foster safer and more rewarding use of their services, resulting in a positive, sustainable, and beneficial experience for both users and online service providers.

Keeping Children Safe in Education[130] (hereinafter KCSIE), a mandatory regulatory guide for all schools and colleges in England published by the Department for Education, is particularly noteworthy. It establishes the legal obligations that schools must meet to protect and promote the well-being and safety of minors under the age of 18 in their facilities.

The document outlines how school staff and leaders should identify and manage the risks of abuse, neglect, bullying, exploitation, and other forms of harm. Furthermore, in the "Online Safety" section (paragraphs 135 and 136), the guide emphasises the

[127] Uk Parliament, *Online Safety Act*, 2023, *cit.*

[128] Ofcom's role under *Online Safety Act*, https://www.legislation.gov.uk/ukpga/2023/50, *cit.*

[129] Available at https://www.ofcom.org.uk/media-use-and-attitudes/media-literacy/making-sense-of-media.

[130] UK Department for Education, *Keeping children safe in education: Statutory guidance for schools and colleges,* 2024, https://www.gov.uk/government/publications/keeping-children-safe-in-education--2.

ISSN 2281-5147

critical importance of an effective and integrated institutional approach to protect, educate, and intervene in the event of risks associated with the use of technology by pupils, students, and school personnel.

After identifying four major areas of online risk[131], the guide states that school governance bodies must integrate online safety as a cross-cutting theme into safeguarding policies and curriculum, including teacher training, parent involvement, and a clear definition of child protection coordination roles[132].

School governance bodies are in charge of incorporating online safety as a cross-cutting theme into safeguarding policies and curricula, which includes teacher training, parent involvement, and clearly defined child protection coordinator roles[133].

---

[131] According to paragraph 135 of the KCSIE: "*The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk: content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories. contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes. conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams*".

[132] The KCSIE's paragraph 140 states that it is the duty of schools to guarantee suitable filtering and monitoring systems, modifying them in accordance with particular risks and the influence on the curriculum.

[133] In this context, according to KCSIE paragraphs 102 and 103, the Designated Safeguarding Lead (hereinafter DSL) is an important component of school governance for child protection. This position, mandated by current safeguarding legislation, is assigned to a member of the senior leadership team and carries significant strategic and operational responsibilities. The DSL is responsible for ensuring that the institution responds to risks or vulnerabilities involving students in a timely, appropriate, and regulatory-compliant manner.

The KCSIE's Annex C describes the broad areas of responsibility and activities associated with the role DSL. Organisationally, he has the authority and resources to manage protection processes on his own, including coordinating reports and referring them to appropriate authorities. From this standpoint, the DSL serves as a point of reference for multi-agency collaboration, such as interprofessional strategies and interdisciplinary prevention and intervention conversations. In terms of education and training, the DSL is responsible for keeping school staff up to date on child protection issues, including digital environment risks, and incorporating this information into curricular and professional development plans. He is also responsible for keeping child protection files secure, confidential, and traceable, as well as ensuring proper transmission during school transitions. A key aspect of the role is to foster a protective school culture by disseminating and implementing safeguarding and child protection policies. The DSL also plays a preventative and inclusive role, helping to identify vulnerable students' educational and psychosocial needs early on, promoting their well-being, and promoting educational equity.

ISSN 2281-5147

In early 2023, the French Ministry of National Education published the document *Numérique pour l'éducation 20232027: la vision stratégique d'une politique publique partagée*[134] which defined a national strategy for digital education for the five-year period 2023-2027.

The document aims to create a shared ecosystem that supports all levels of education, based on four strategic axes.

In terms of educational governance, the document describes a series of actions aimed at improving educational cooperation in digital technology at the national and local levels, including the development of tools for monitoring progress (shared dashboard, indicators). The strategy also calls for investments in *Territoires numériques éducatifs*, with projects such as providing individual devices to college and high school students beginning in 2024. This aims to narrow the digital divide between regions and provide equal opportunities for digital learning.

The document describes the development of a digital skills and citizenship curriculum throughout the school year to develop digital skills (critical thinking, coding, and AI literacy), with the goals of professional and social growth, as well as systematic awareness-raising about responsible social media use and cyberbullying prevention.

The third strategic axis emphasises the importance of fostering an educational community of shared and accessible tools, known as *communs numériques* and *compte ressources*, to facilitate access to educational resources and the development of an inclusive and sustainable digital offering for all school communities.

Finally, the document outlines the plan to renew the ministerial information system based on the principles of efficiency, interoperability, user experience, and environmental sustainability (eco-responsibility), with the goal of simplifying services for staff and families.

The document is important at the institutional level because it outlines a shared public policy aimed at a broad range of stakeholders (states, regions, institutions, EdTech, and associations) and lays the groundwork for participatory governance of digital

[134] Ministère de l'Éducation nationale, *Numérique pour l'éducation 2023-2027 : La vision stratégique d'une politique publique partagée, 2023,* https://www.education.gouv.fr/feuilles-de-route-450426#:~:text=La%20strat%C3%A9gie%20num%C3%A9rique%20pour%20l,transformation%20du%20syst%C3%A8me%20d'information.

ISSN 2281-5147

education in schools. It is also accompanied by *feuille de route*; thematic roadmaps such as one for data and algorithms in 2024-2027, which supplement the strategic vision with specific operational measures.

Beyond the institutional context, France promotes digital and AI literacy through various policy initiatives that are part of a comprehensive national strategy. The *Éducation au numérique* programme[135], promoted by the *Commission Nationale de l'Informatique et des Libertés National* (hereinafter CNIL). This comprehensive set of educational resources is designed for teachers, students, and families, with the goal of raising awareness among young people about the responsible use of personal data and promoting knowledge of digital rights in accordance with the GDPR. The proposed activities, which include thematic worksheets, workshops, educational games, and training modules, are in line with the competencies established by the *Cadre de Référence des Compétences Numériques*[136] and are fully compatible with the teaching of EMI. The CNIL's initiative contributes to the development of critical and responsible digital citizenship, focussing on the concepts of online reputation, privacy, digital identity, and security. This multidimensional approach is an integrated model of digital civic education that strengthens the link between technological literacy and legal and ethical awareness in French schools.

A comparison of the United Kingdom and France reveals significant similarities, particularly an integrated approach to digital literacy that combines awareness of digital rights, personal data protection, and a comprehensive view of citizenship. This approach, which is firmly rooted in European legislation and the major digital competence frameworks, acknowledges schools as critical players in the formation of informed and responsible digital citizens.

---

[135] Available at https://www.cnil.fr/fr/mots-cles/education-numerique.

[136] Décret n. 2019-919 du 30 août 2019 relatif au développement des compétences numériques dans l'enseignement scolaire, dans l'enseignement supérieur et par la formation continue, et au cadre de référence des compétences numériques, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000039005162. The *Cadre de Référence des Compétences Numériques* is an official framework adopted in France that has been in effect since 2019, defining essential digital skills for students from primary school to university, as well as adults in vocational training. The CRCN, which is based on DigComp framework, organises 16 digital skills into five thematic areas (information and data; communication and collaboration; content creation; protection and security; digital environment), each with eight levels of proficiency. These skills are certified using the Pix platform, with certifications given at the end of cycle 4 (*collège*) and the final cycle of high school (*lycée*).

ISSN 2281-5147

Although Italy, the United Kingdom, and France all include digital citizenship within their educational agendas, notable differences persist in the ways these countries structure their school systems and design governance models for digital education. These divergences influence how policies are implemented, the degree of institutional coordination involved, and the extent to which schools are empowered to act as agents of digital transformation.

In Italy, despite the release of a Digital Civic Education Curriculum in 2018[137], digital education is integrated into the transversal teaching of civic education, which remains strongly linked to the legal-pedagogical importance of teaching the constitution and its principles. Furthermore, civic education instruction in Italian schools remains uneven: there is a lack of structured and common tools for monitoring and evaluating the courses offered, as well as a coordinated and systematic strategy for teacher training[138].

---

[137] MIUR-Ministero dell'Istruzione, dell'Università e della Ricerca, Curriculum di Educazione Civica Digitale, Roma, 2018, https://scuoladigitale.istruzione.it/iniziative-competenz/sillabo-sulleducazione-civica-digitale/. The Curriculum suggests creating "positive strategies" that will allow students to "appropriate digital media, moving from passive consumers to critical consumers and responsible producers of content and new architectures" (MIUR, 2018, p. 5). The 2018 syllabus emphasises critical thinking and responsibility education, which are defined as awareness of the consequences of one's actions in the digital world, in promoting skill development.

[138] The law introducing civic education into the Italian education system requires the implementation of an integrated approach to this curricular area. At the same time, the law and the Guidelines for Implementation are ambiguous. On the one hand, this document seems to support the transversal nature of civic education. This approach is supported by statements in the Guidelines (Cf. note n. 106; https://www.istruzione.it/educazione_civica/norme.html) that describe its relationship to other subjects in the curriculum, as well as an encouragement to avoid the simple juxtaposition of content from different subjects.

According to the teaching organisation, the number of hours dedicated to teaching civic education will be jointly assigned to multiple teachers from the same class council, one of whom will serve as coordinator.

On the other hand, in other passages, this choice appears to be partially questioned, such as when it is explicitly stated that teaching activities can be carried out "by one or more teachers" and, in secondary schools, when it is decided to assign teaching to the teacher of "legal subjects" (if such subjects are included in the curriculum), albeit in collaboration with other members of the class council. Article 11 of the law explicitly mentions the "prospect of a possible modification to the timetable that would add an hour of civic education," implying that the transversal approach could be replaced by the introduction of a "separate" subject. Furthermore, the established number of hours is "derived" from the timetable of the subjects and areas already included in the curriculum.

The decision to take a "transversal" approach appears to be more influenced by organisational and contingent needs (such as maintaining staff and timetables and the unavailability of specific resources) than by a clear conceptual and methodological choice. These fundamental ambiguities give rise to a number of issues regarding

ISSN 2281-5147

In the United Kingdom, digital citizenship education is more operational and regulatory, with a strong emphasis on minors' online safety (duty of care) and the role of digital platforms as co-responsible.

In France, a long-term strategic approach is taken, based on multilevel governance and the development of a shared public policy, with a broad vision that includes training, infrastructure, territorial equity, and sustainability.

The differences that emerged, particularly between the UK's regulatory-operational approach and France's strategic-systemic vision, enabled us to identify complementary elements to Italy's critical issues. On the one hand, the UK experience has demonstrated the value of a clear regulatory framework that defines shared responsibilities among educational institutions, digital platforms, and families[139]. On the other hand, the French approach has demonstrated the importance of multilevel governance, which can organically integrate teacher training, equal access, and digital infrastructure[140]. The comparative perspective has influenced the development of common policy proposals in terms of coherence, monitoring, and systematicity, with

planning, teaching methodology selection, and assessment. For example, on the one hand, the possibility of organising and managing the minimum 33 hours of teaching hours in a modular manner, rather than distributing them throughout the school year, is increasing. On the other hand, it is expected that a separate civic education assessment will be formally administered on a regular basis (at the end of each term or four-month period) and at the conclusion of each term. Actually, in the name of autonomy, schools are supposed to address and resolve these problems, but there are no guarantees that they will be able to do so.

[139] In the United Kingdom, for example, the adoption of the *Online Safety Act* 2023 imposes specific protection duties on digital platforms, and the development of a clear media literacy strategy has begun, expanding Ofcom's mandate. According to *Online Safety Act* 2023, Chapter 6 - Codes of Practice and Guidance, Ofcom is now responsible for enforcing the new legislation, as well as developing and overseeing mandatory codes of conduct for online platforms. Ofcom seeks to maintain a balance between freedom of expression and child protection by implementing the Protection of Children Codes (April 2025, https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/statement-protecting-children-from-harms-online) and holding public consultations.

[140] In France, the *Cadre de Référence des Compétences Numériques* oversees the development of digital skills across the board, with a progression of levels and standardised certification. is more than just a technical framework; it is also a pedagogical framework aimed at developing informed, autonomous, and responsible digital citizens. Its significance lies in the strengthening of four critical dimensions: - Inclusion: It helps to bridge the digital divide by providing a gradual path to skill acquisition. - Formative assessment: It enables the transparent and continuous observation and measurement of progress. - Integrated education: It encourages transversal teaching, which links digital skills to all disciplines. - Active citizenship: It teaches young people not only how to use digital tools, but also about their ethical, social, and political implications.

ISSN 2281-5147

the goal of promoting and disseminating digital civic education as a tool for informed participation by children and all stakeholders in digital society.

9. Bridging the digital divide: empowering online safety through digital education

Digital education is an effective tool for youth empowerment and social inclusion, capable of closing educational gaps and encouraging active and informed citizenship.

Schools and community learning centres play an important role in developing these competencies by using digital technologies as tools for creativity and active learning[141]. They also help foster critical thinking, resilience, and support families in guiding children's use of technology. Expanding school access and investing in teacher training can better connect internet use with educational opportunities, helping address the significant digital skill gaps among younger students[142]. As early as 2014, the UN Committee on the Rights of the Child recommended that member governments incorporate digital literacy into their national school curricula[143].

In light of this, principles underpinning in all previous considerations could make a significant contribution to addressing the current gaps and areas of disadvantage within the Italian system, particularly in the fields of digital education and online child protection, as highlighted through comparative analysis with approaches taken in Italy, the United Kingdom and France.

Such a proposal would advocate for a more relational approach to digital literacy, raise awareness, and provide adequate psychosocial support for minors who are especially vulnerable in digital contexts[144].

---

[141] S. Chaudron, R. Di Gioia, M. Gemo, *Young Children (0-8) and Digital Technology: A qualitative study across Europe,* EUR 29070 EN, Publications Office of the European Union, Luxembourg, 2017.

[142] J. Byrne, D. Kardefelt-Winther, S. Livingstone, M. Stoilova, *Global Kids Online research synthesis, 2015–2016*, Research Report, UNICEF Office of Research–Innocenti and London School of Economics and Political Science, 2016.

[143] Committee on the Rights of the Child Report of the 2014 day of General Discussion on "*Digital Media and Children's Rights*", par. N. 109, https://www.ohchr.org/sites/default/files/Documents/HRBodies/CRC/Discussions/2014/DGD_report.pdf.

[144] *CURA Blueprint Guidelines*, *cit.*, pp. 9-11.

ISSN 2281-5147

Strengthening a relational perspective in digital literacy and awareness promotion appears to be critical for making interventions more effective and meaningful. This approach fosters family engagement and supports the development of critical awareness of digital technologies through structured communication strategies and attention to emotional well-being.

The implementation of educational programmes that teach children, parents, and educators about online risks, ethical considerations, and responsible digital citizenship has the potential to close the educational gap. To be truly effective, such programmes should be integrated into both school curricula and broader societal contexts, and include modules on topics such as the attention economy, content creation, peer pressure, and the ethical implications of online sharing. These programmes, if integrated into school curricula and promoted at the EU level, have the potential to standardise digital education, making it more accessible and mandatory. For example, implementing a standardised certification programme for adolescents that is flexible based on their developmental maturity could ensure that all students acquire essential digital skills, thereby reducing regional and socioeconomic disparities.

This includes not only teaching critical and responsible technology use, but also strengthening educational relationships and promoting parental involvement to foster a shared understanding of the collaborative role families play in developing critical awareness of digital technologies. Supporting families through training opportunities, emotional resources, and structured dialogue, such as workshops and targeted materials, can enhance trust and communication between parents and children, encouraging more effective and authoritative parenting practices in the digital sphere.

Promoting greater parental involvement in their children's digital technology use, as well as encouraging authoritative parenting practices, can help families communicate and trust more effectively. In contexts where engaging the most vulnerable families presents a challenge, initiatives such as interactive workshops and accessible educational resources can foster open dialogue on online safety, digital ethics, and responsible behaviour. Adopting a relational approach can support adolescents in developing a digital safe base, enabling them to navigate the online environment with greater confidence and security[145].

[145] *CURA Blueprint Guidelines*, *cit.*, p. 11.

ISSN 2281-5147

Finally, it is critical to implement psychosocial support that addresses the unique needs of minors as

Providing mental health, psychological, and sociological support services to children exposed to online risks represents a fundamental step in mitigating the adverse effects associated with digital technologies. Specialised services aimed at supporting vulnerable users can play a critical role in addressing phenomena such as cyberbullying, online abuse, and exposure to harmful content. To ensure broad and equitable access, these services should be systematically integrated into educational institutions and community settings, thereby reaching all students irrespective of their socioeconomic background[146].

Consequently, promoting the development of children's rights impact assessments as part of broader fundamental rights monitoring represents a critical step toward ensuring that digital products and services are safe, appropriate, and responsive to the specific needs of minors. Embedding such assessments within product conformity and safety evaluation processes can assist economic operators in aligning with child protection standards, particularly in regulatory environments where dedicated online safety legislation remains under development.

10. Conclusions

In today's digital environment, where children's presence is both pervasive and yet often rendered invisible, the challenge of developing tools capable of recognising and addressing their vulnerabilities has become inescapable. To respond to this challenge, not by offering definitive solutions, but by outlining a coherent, multisectoral, and child-centred operational path resulted a first attempt towards a safer and child-friendly approach to digitalization of services and product.

The ultimate goal is not merely to shield children from digital risks, but to contribute to the construction of an environment that embraces childhood and adolescence in all their complexity, supporting their emotional, relational, cognitive, and identity-related needs. From this perspective, protection is not conceived as a defensive or

[146] *CURA Blueprint Guidelines*, cit., pp. 11-12.

ISSN 2281-5147

restrictive measure, but rather as an enabling condition for meaningful and informed participation in digital society.

The adopted approach, combining legal frameworks, technical safeguards and educational initiatives, allows us to move beyond the traditional dichotomy between protection and participation. Such integration is essential not only to address the layered nature of children's vulnerabilities, as discussed in the first part, but also to counteract the fragmentation of interventions, institutional inertia, and the tendency to shift responsibility solely onto parents or the children themselves. The underlying logic is that of shared responsibility: between adults and minors, between public and private actors, between central institutions and local communities.

The educational dimension highlights how achieving a truly inclusive form of digital citizenship requires the joint commitment of schools, families, and broader communities, working together to develop coherent, accessible learning pathways that build upon existing resources. In this light, digital education emerges not as a secondary or optional competence, but as a structural prerequisite for exercising rights in the digital realm, for building meaningful relationships, for safeguarding personal integrity, and for developing a critical understanding of digital languages and dynamics.

A particularly emblematic case is that of adopted children searching for their origins: a growing phenomenon that illustrates the potential of the digital sphere as a space of knowledge and self-affirmation, but also its profound risks when not accompanied by emotional support, adequate digital skills, and institutional oversight. In this regard, the blueprint policies aim to fill a normative and practical gap, by proposing a reconsideration of access thresholds and service interactions, and by promoting relational and educational frameworks capable of combining self-determination with protection.

Ultimately, a model of digital childhood governance that is actionable, sustainable and, above all, attuned to the lived realities of children and adolescents will contribute to building a digital ecosystem that is more equitable, inclusive, and respectful of minors' dignity and fundamental rights. At a time when the rapid pace of technological innovation threatens to produce new forms of exclusion and fragility, these guidelines serve as instruments of guidance and collective responsibility. They invite all stakeholders (institutions, professionals, families and platforms) to recognise

ISSN 2281-5147

the complexity at hand and to transform it into an opportunity for shared growth and care.

ISSN 2281-5147

ISSN 2281-5147

YES, WE CAN…AND WE MUST! CHANGING THE NARRATIVE OF CHILDREN'S RIGHTS PROTECTION IN THE DIGITAL ENVIRONMENT THROUGH A CHILD-CENTERED APPROACH. THE LESSON FROM THE U.K. CHILDREN'S CODE

Sara Rigazio*

Abstract

In the face of empirical data confirming that children and young people spend a great deal of time online, today's reality delivers an equally alarming result: the Internet was not conceived and designed with the idea that users could also be minors. This represents a serious shortcoming that could, however, be remedied where a genuinely child-centered approach is chosen, that is, an approach based on the founding principles of the UN Convention on the Rights of the Child (CRC): the best interests, the evolving capacities and the right to be heard. Together with the essential contribution and role played by family, institutions and stakeholders, the narrative on the protection of children online could take on a different and more appropriate direction, focusing on the fundamental dimension of the *promotion* of children's rights and their agency.

The UK Children's Code represents, in this regard, a concrete model to look at with extreme interest. Its circulation, influence and success – with different nuances - proves, in fact, that one of the key elements in this topic is represented by the *empowerment* – both of the single minor and of the collectivity – in order to maintain and preserve what makes and builds our identity: human dignity.

* Assistant Professor of Comparative Law, Department of Political Sciences and International Relations, University of Palermo. Double blind peer reviewed contribution.

ISSN 2281-5147

Table of contents

Keywords

U.K. Children's Code – Empowerment – Convention on the Rights of the Child (CRC) – design discourse – Human Dignity

1. Introduction

Among the global challenges of our time, the protection of children in the digital environment represents one of the most urgent and complex tasks ever addressed in the present time, from a legal, social, economic and ethical point of view. According to recent data collected in research conducted by UNICEF, in fact, one-third of online users in Europe are under the age of 18 and numbers are destined to increase

ISSN 2281-5147

in the coming years, in consideration of the long-term effects resulting from the Covid-19 pandemic[1].

At the same time, it is a fact that the Internet "was not designed with kids in mind"[2]. The result is right in front of our eyes with countless new episodes where minors are daily victims of a distorted use of the web[3]. It should be noted, however, that in the last few years the awareness by the international institutions – in particular the European ones – and by the civil society as well, has increased evidently, leading to a series of initiatives launched to promote greater protection for minors and a better understanding of their rights[4]. In addition to representatives of institutions - national and international - a number of debaters were involved such as, among others,

[1] See, "Child rights and the 2030 Agenda for Sustainable Development in the context of the COVID-19 pandemic", in https://www.ohchr.org/sites/default/files/Documents/Issues/Children/ChildRights_2030Agenda.pdf.

[2] See, European Digital Rights, Age against the machine: the race to make online spaces age-appropriate, in https://edri.org/our-work/age-against-the-machine-the-race-to-make-online-spaces-age-appropriate/, September 4, 2024.

[3] See, National Society for the Prevention of Cruelty to Children (NSPCC), in collaboration with leading experts in academia on online child protection, published in November 2023, which outlines and exposes evidence on the risks and dangers present online for children and that emerged during the period 2017-2023 in the UK. The report focuses on the dissemination and use of child pornography as well as, more generally, the distorted use by platforms of the design features of websites frequented by children. Consider, among others, so-called dark patterns. The report can be found at https://learning.nspcc.org.uk/media/ezjg0pjb/online-risks-children-evidence-review-main-report.pdf; J. Bryce, S. Livingstone, J. Davidson, B. Hall, J. Smith, *Online risks to children: evidence review*, November 2023.

[4] Among the numerous ones, see EU Kids Online. This is an international research network whose goal is to improve the degree of knowledge and awareness among European children about opportunities, risks and safety in the digital environment. Through the use of a multidisciplinary approach, the project aims to map the online experience of children and parents, in constant dialogue with national and European policymakers and stakeholders. On this point, see D. Smahel, H. Machackova, G. Mascheroni, L. Dedkova, E. Staksrud, K. Ólafsson, S. Livingstone, U. Hasebrink, EU Kids Online 2020: Survey results from 19 countries. EU Kids Online, at https://www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online/eu-kids-online-2020. Similarly, also in the European context, in May 2021 as part of the Better Internet for Kids initiative, a guide was published regarding best practices identified in some member states, Children's rights in the digital environment: moving from theory to practice, available at https://www.betterinternetforkids.eu/documents/167024/200055/Best-practice+guideline+-+Childrens+rights+in+the+digital+environment+-+May+2021++v2+FINAL+CC+BY.pdf/f947d4f9-4ec4-49ae-5e2e-b6e9402c5fa2?t=1624532196598. Most recently, on September 24, 2024, the United Nations approved the Global Digital Compact, in which fundamental rights are also reaffirmed in the digital dimension, with special attention given to children's rights. The overriding goal of the Global Digital Compact is to "strengthen legal and policy frameworks to protect the rights of the child in the digital space," in https://www.un.org/sites/un2.un.org/files/sotf-the-pact-for-the-future.pdf.

ISSN 2281-5147

organizations in defense of children, representatives of the academic world and, in part, also the digital industry (so-called stakeholders).

The core issue regarding the empowerment of children in the digital environment necessary implies a series of considerations about: parental responsibility, institutions' involvement, stakeholders' role and, mainly, the minors' voices.

While all these elements are specifically regulated in the Convention on the Rights of the Child (CRC) – which represents at present the most ratified international convention in the matter of children's rights and the legal framework of reference[5] – nevertheless, neither the international community and the others actors involved, seem to take the CRC into serious and concrete consideration when it comes to implement actual policies in favor of the minors' empowerment.

Moreover, the evident contrast between the law in the books and the law in action[6] - that is between the established rule and the operational rule[7] - is particularly sharp in the matter of the digital dimension. Even though the CRC Committee has clearly pointed out that children's rights fully apply also in the digital environment, resistances and oppositions of various nature make the goal of protecting and promoting children's rights very difficult to achieve[8].

This article explores the benefits of adopting a child-centered approach in addressing the topic here presented, through the concrete example of the U.K. Age –

[5] The Convention on the Rights of the Child (CRC) was approved by the United Nations General Assembly in New York on November 20, 1989, and entered into force on September 2, 1990. To date, it is the international document that has received the highest number of ratifications by states, with the sole exception of the United States of America.

[6] J.L. Halperin, *Law in books and law in action: the problem of legal change*, 64 Me. L. Rev. 2011, p. 45; R. Pound, *Law in books and law in action*, 44 Am. L. Rev. 1910, p. 12; D. Nelken, *Law in action or living law? Back to the beginning in sociology of law* 1, 42 Legal studies 1984, pp. 157-174.

[7] Comparative law makes extensive use of this methodological approach. See, P.G. Monateri, *Morfologia, Storia e Comparazione. La nascita dei "sistemi" e la modernità politica*, in *Diritto: storia e comparazione. Nuovi propositi per un binomio antico*, Frankfurt, 2018, 267-290; R. Scarciglia, *L'Oggetto Della Comparazione Giuridica (Objects and Legal Comparison)*, in R. Scarciglia (edited by), *Introduzione al diritto pubblico comparato*, Bologna, 1966, pp. 47-68; G. Ajani – B. Pasa – D. Francavilla. *Diritto comparato: lezioni e materiali,* Torino, 2018; A. Somma, *Giochi senza frontiere: Diritto comparato e tradizione giuridica*, 37:109 *Boletín mexicano de derecho comparado*, 2004, pp. 169-205.

[8] See, General Comment n. 25, https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation, CRC/C/GC/25, 2 March, 2021, "Children's rights in relation to the digital environment".

ISSN 2281-5147

Appropriate Design Code, better known as the U.K. Children's Code[9]. The paper analyses the structure of the Code showing its strict connection with the CRC, also underlining how the way the Code's drafting process was developed and defined, contributed to its success. It then advances the argument that adopting a child-centered perspective means fully respecting the roles and prerogatives of all the actors involved, ultimately conveying to the empowerment of the minors and, therefore, of the whole collectivity.

2. The U.K. Children's Code in the prism of the CRC and of the design discourse

The U.K. Children's Code is a code of conduct, consisting of 15 standards, mainly aimed at digital platforms offering online services targeting minors, which came into effect in September 2020 in the United Kingdom, drafted by the Information Commissioner's Office (ICO), the UK's independent data protection authority. The ICO is competent in "upholding information rights in the public interest, promoting openness by public bodies and data privacy for individuals and empowering people through information"[10].

The Children's Code is a statute and, therefore, in the system of the English legal sources, it is part of the so-called legislation, or "the law created by the competent organs of the state and condensed into precepts expressed in written formulas"[11] .

[9] See, the U.K. Age Appropriate Design Code, known as Children'd Code, enacted by the Information Commissioner Office in 2020, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/introduction-to-the-childrens-code/. See, infra, par. 2.

[10] https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/ico25-plan/.

[11] G. Criscuoli, *Introduzione allo studio del diritto inglese: le fonti*, 2014, Torino, p. 411 ff. Although they are not as numerous as sources of judicial origin, as the A. notes, legislative sources also play a function "of primary importance, not only because of the original normative content they can have, but especially because of the sometimes decisive impact they can have on the life of the normative principles of case law." On the role statutes have occupied and still occupy in the hierarchy of English sources, see also, among others, T. Plucknett, *A Concise History of the Common Law*, 5th ed., Boston, 1956; M.S. Arnolds, *Statutes as Judgements: The Natural Law Theory of Parliamentary Activity in Medieval England*, 126 U. Pa. L. Rev., 1977, p. 329; C.K. Allen, *Law in the Making*, 7th ed., Oxford, 1964: U. Mattei. E. Ariano, *The common law model*, Turin, 2018, p. 233 ff.

ISSN 2281-5147

With specific reference to the expression 'code,' a clarification should be made: indeed, this is not the same concept as the 'code' typical of civil law systems. As it is well known, in fact, there is no use in English law of the code in the same way as a general system of norms. However, just as in Italy not all law is codified, even in England some specific issues have been the object of a specific regulation, such as in the case of the UK Age-Appropriate Design Code[12].

The Children's Code, therefore, will work as a reference for the courts - as, indeed, specified by the Code itself in the Executive Summary - when it comes to the protection and promotion of the rights of the child online, in a position, however, that is interstitial and of specialty with respect to common law in general.

As legal scholars remarked, "Despite the enormous amount of legislation produced, the most important part of our law remains common law [...]. Statutes are nothing more than addenda and errata to the book of common law and would have no meaning except in reference to common law [...]"[13].

The Code is aimed at all companies offering online services (information society services - ISS) to which, potentially, minors could also have access (likely to be accessed), such as video games, entertainment applications, smart toys, etc. As expressly stated, the ultimate goal is to ensure protection for under-age users through proper design of the systems underlying the services offered and appropriate use of the data entered and circulating on the network.

[12] More generally, this can be traced to that activity of collection and arrangement which, technically, is called consolidation. On the distinction between codification and consolidation, see G. Criscuoli, cit., p. 16 ss., who points out, among the most typical aspects of the difference between these two techniques, that whereby "consolidation does not affect the binding value of judgments issued prior to the act of consolidation, as opposed to codification, which, on the other hand, eliminates the binding effect to judgments related to reformed rules."

[13] W. Geldart, *Elements of English Law*, 1975, 8o ed., p.2. Geldart's words are also mentioned by A. Guarneri, *Lineamenti di diritto comparato*, 2022, p. 348. F. Pollock wrote «The best and most rational portion of English law is in the judge made law», *The Law Quarterly Review*, 1893, p. 106. On the historical relationship between common law and statutes, see also, C.K. Allen, *Law in the Making*, 7th ed., Oxford, 1964, *passim*, and more recently, A. Miranda, *Smoke gets in Euro-eyes: fusione e fissione del diritto comunitario*, in Liber Amicorum Luigi Moccia, edited by E. Calzolaio, R. Torino, L. Vagni, Roma TrE press, Roma, 2021, p. 389 ss.

ISSN 2281-5147

More generally, the Code stems from the need to protect minors *within* the digital dimension, and not, instead, from the need to prevent them *from* accessing it[14].

As previously mentioned, it consists of 15 standards, which are not merely technical requirements, but parameters to be used to design an adequate protection of the minors' data. The standards are: best interests, data protection impact assessments, age-appropriate application, transparency, detrimental use of data, policies and community standards, default settings, data minimization, data sharing, geo location, parental controls, profiling, nudge techniques (also known as dark patterns), connected toys and devices, online tools[15].

In order to understand how a standard works, it is worth to analyze, as an example, the one related to the default settings in order to realize how each standard is the result of the balance between the enhancement of the child, the parental responsibility, the (preventive) control of the company offering the service, and the (eventual) later control of the sanctioning authority.

Standard number 7 on default settings imposes an obligation on the company offering the service, to define and guarantee - from the beginning - the most restrictive level of privacy, unless it can be demonstrated that a different, lower-level approach is necessary in order to pursue the best interests of the minor.

In the case, for example, of a video game, minors will start using the product without the need for a change, on their part, to obtain a more restrictive level of privacy (so that their data will not, for example, be used by third parties) because the platform has already done so, in this respect. Rather, and with an entirely reversed perspective, minors may be given the opportunity to change the default choice, for a less restrictive level, provided that, as clarified in the Code itself, they are put in a position to exercise their rights consciously, and are provided with all the information they need to

[14]See, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/about-this-code/#code1.

[15] For the specific of each standard, see https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/code-standards/.

ISSN 2281-5147

understand what the consequences of any change in these settings are, in terms of the use and circulation of their data[16].

As it becomes quite clear, there is a strong connection between the standards and the CRC, connection also underlined by the same Executive Summary of the Code, when it explicitly declares that the Code is "rooted in the United Nation Convention on the rights of the child". As a matter of fact, the entire structure of the Code responds to the logic that is proper to the Convention, namely that of the protection of the child as a *subject* fully entitled to rights, who is recognized, depending on the maturity and on the context, a progressive acquisition of autonomy in the decisions that affect him or her, according to the principle of the evolving capacities.

As it is well known, indeed, the CRC formally establishes the transition from a paternalistic conception, traditionally oriented towards the idea of the minor as an "object" of law, to a vision in which, on the contrary, as mentioned, the minor becomes a full "subject" of law. This change in perspective, specifically, is achieved, on the one hand, through the recognition of the individual traditional freedoms in terms of fundamental rights, granted to every human being by international treaties and here adapted to the specific situation of minors; on the other hand, through the introduction of a series of "new" rights closely linked to the peculiarities of the condition of minors, both within and outside the family unit.

Thus, with regard to the first aspect, the provisions of Articles 13 to 17 recognize the child's right to freedom of expression and thought, as well as freedom of religion, association, and the right to privacy. The Convention also emphasizes the right of access to information and the need for minors to have a variety of information

[16] "You can also use privacy settings to support the exercise of children's data protection rights (such as the rights to object to or restrict processing). And they can give children and parents confidence in their interactions with your online service, and help them explore the implications of allowing you to use their personal data in different ways". See, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/7-default-settings/.

ISSN 2281-5147

sources at both the national and international levels, especially those aimed at promoting their physical and spiritual well-being[17].

The rights concerning the second aspect are more specific. They are aimed at protecting minors in certain situations (such as removal from their parents against their will, unless such removal is not in the best interests of the child)[18], to ensure the principle of parental responsibility in the education and upbringing of the child[19], and finally to protect the child from all forms of violence, throughout the period of custody by one or both parents or the legal representative[20].

The Convention on the Rights of the Child, therefore, has opted for a reversal of the traditional view of minors as individuals, incapable of providing for themselves and, consequently, perpetually dependent on the decisions of others, elevating minors from a context of immobility and subjugation to a dynamic context in which, on the contrary, they can become protagonists of their own choices.

It is indeed in this perspective that Appendix B of the Code concretely refers to the principle of the evolving capacities. As a matter of fact, it expressly provides for the so-called *developmental stages*, indications addressed to online operators, that have the precise intent of guiding companies that offer services to minors, in the application of the standards themselves, according to the age ranges of the users they address.

[17] Artt. 13, 14, 15, 16 and 17 of the CRC about: freedom of expression, freedom of thought and conscience, religion, privacy, access to information and material from a diversity of national and international sources.

[18] See, art. 9 (1): "States Parties shall ensure that a child shall not be separated from his or her parents against their will, except when competent authorities subject to judicial review determine, in accordance with applicable law and procedures, that such separation is necessary for the best interests of the child. Such determination may be necessary in a particular case such as one involving abuse or neglect of the child by the parents, or one where the parents are living separately and a decision must be made as to the child's place of residence".

[19] See, art. 18 (1): "States Parties shall use their best efforts to ensure recognition of the principle that both parents have common responsibilities for the upbringing and development of the child. Parents or, as the case may be, legal guardians, have the primary responsibility for the upbringing and development of the child. The best interests of the child will be their basic concern".

[20] Art. 20 (1): "States Parties shall take all appropriate legislative, administrative, social and educational measures to protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse, while in the care of parent(s), legal guardian(s) or any other person who has the care of the child".

ISSN 2281-5147

Specifically, the Code identifies five age ranges: the pre-literate and early literacy (up to 5 years of age); that corresponding to the primary school years (6 to 9 years of age); the so-called transition years (10 to 12 years of age); early adolescence (13 to 15 years of age); and the so-called approaching adulthood (16 to 17 years of age). These are, however, indicative ranges since, as it says, "Children are individuals, and age ranges are not a perfect guide to the interests, needs and evolving capacity of an individual child. However, you can use age ranges as a guide to skills and behaviors a child might be expected to display at each stage of their development"[21].

The Code's link to the Convention is further confirmed when it recalls firmly and explicitly the role of parents and family members in general, as well as the role of institutions.

As a matter of fact, the Code expressly states that the standards represent a support and help for parents to clarify and, possibly, solve a number of issues that arise whenever a child uses a digital tool such as, for example, in the so-called by default settings concerning privacy. Similarly, the standards also address the need for institutions to comply with the requirements of the Data Protection Act (DPA) of 2018[22], which in turn transposes the European GDPR, and in particular from Recital No. 38.

Furthermore, the Code reinforces the so-called participatory rights[23] - that characterize the entire Convention - in the digital dimension, where it recognizes

[21]See, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/3-age-appropriate-application/ .

[22] https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted. The Data Protection Act, which was finally approved on May 23, 2018, implements the European General Data Protection Regulation (GDPR). It is an updated version of the previous 1998 legislation, specifically drafted to address the challenges of the digital age. In particular, the new version focuses on the protection of so-called sensitive data and their greater protection, such as, among others, race, ethnic background, political opinions, religious beliefs, trade union membership, genetics, biometrics, health, sex life, or orientation.

[23] The use of the expression "participatory rights" can be ascribed to the Committee on the Rights of the Child, which has the task to monitor and promote the implementation of the Convention on the Rights of the Child in the legislation of member states. In particular, see Concluding observations Spain UN Doc. CRC/C/15/Add.28, 1995; Nicaragua UN Doc. CRC/C/15/Add.36, 1995; Germany U.N. Doc. CRC/C/15/Add.43, 1995, available on the official website of the United Nations. For a multidisciplinary analysis of participation rights, see A.B. Smith, *Interpreting and supporting participation rights: Contribution from socio-*

ISSN 2281-5147

freedom of expression, thought, and religion; of privacy; of association; of access to information in the mass media (of course in the terms in which the Code operates); of gaming and entertainment (again, dropped into digital reality); of protection from economic, sexual, or other exploitation, as well as pertaining to the web . The key elements of the relationship between the standards and the UN Convention are, therefore, to be found in the *evolving capacities* of the child, the central role of the family and the equally indispensable role of institutions and stakeholders[24].

In this perspective, another aspect which played a fundamental role in the success of the Code, pertains to the modalities chosen for the drafting of the Code itself. As a matter of fact, it is the result of a shared action between institutions, third sector organizations and representatives of the digital industry. It all started from the nongovernmental organization *5RightsFoundation*, founded by Baroness Beeban Keedron, a successful film producer and member of the House of Lords, in collaboration with academics and various stakeholders, who, in 2018, launched a strong campaign aimed at verifying, in concrete terms, the state of the art regarding the use, by minors, of digital tools and, at the same time, the (possible) measures taken by platforms for the access to the online contents by minors themselves.

The survey, part of an ongoing project, highlighted the real impact of the digital dimension on minors, particularly in the aftermath of the COVID 19 pandemic, under different profiles including, the relationships within the family unit, between the minors themselves inside and outside the school context, between the individual minor and the digital tool in relation to the use of social networks. The data collected shows a high level of datafication in the daily lives of children, and the substantial

cultural theory, in 10 The International Journal of Children's Rights, 2002, 1, 74. See, also E. Munro, *Empowering looked-after children*, in 6 Child and family social work, 2002, 1, 74. More recently, see

[24] M. Couzens, *Autonomy rights versus Parental Autonomy*, in AA.VV., The U.N. Children's Rights Convention: Theory meets Practice. Proceedings of the International Interdisciplinary Conference on Children's Rights, Intersentia, Oxford, 2007, pp. 420 ss. See, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/about-this-code/.

ISSN 2281-5147

absence of measures aimed at effective protection in accordance with the principles set out in the UN Convention on the Rights of the Child[25].

These findings represented the starting point for undertaking intensive lobbying - by 5Rights, child protection associations and representatives of the major digital industries, vis-à-vis Parliament - which led to the goal of drafting and approving, the Code.

3. The impact of the Code: concrete results

The most immediate objection that could be made, and in fact is very often made, is that little or nothing has changed or will be able to change for minors accessing the net, despite the intentions and interventions put in place by the states or the international organizations. In this respect, it is useful to recall the report, published in May 2024 and compiled by 5Rights in collaboration with the London School of Economics (LSE) and the association Digital Futures for Children, entitled "Impact of regulation on children's digital lives," which analyzes the changes made by some digital platforms, mainly in Europe and U.K, in the period between 2017 and 2024, in the direction outlined by the Code[26].

The report is the result of an investigation that involved an initial phase of data collection, through requests made directly to the platforms to provide the data; a second phase of reprocessing, referring to both the type of change and the period in which it was made.

The report focuses on the UK and European context and specifically considers the impact that the UK Age Appropriate Design Code, in particular, and to a much lesser extent the Digital Services Act, have had in terms of protecting minors in relation to privacy, security, and data protection.

---

[25] Research Report, Impact of regulation on children's digital lives, May 2024, https://eprints.lse.ac.uk/123522/1/Impact_of_regulation_on_children_DFC_Research_report_May_2024.pdf.

[26] Impact of regulation on children's digital lives, Research report, May 2024. V. https://eprints.lse.ac.uk/123522/1/Impact_of_regulation_on_children_DFC_Research_report_May_2024.pdf.

ISSN 2281-5147

It should also be noted that the document also considers a series of other non-EU regulatory measures; however, as highlighted in the report itself, the data show that the majority of changes made by platforms occurred following the approval of the UK Code and, to a lesser extent, the EU directive[27].

The most relevant changes seem to be concentrated in the 'by default' category, where there are the highest number of changes, made in 2021, to coincide with the Code's entry into force.

For example, Instagram (part of the Meta group) changed the initial setting of under-16 accounts from 'public' to 'private' as pre-defined; Google disabled, again as pre-defined, the application related to the history tracking feature.

Other changes affected, again in the by default category, the very management of the account on the platform: for example, Tik Tok disabled automatic notifications after 9 and 10 p.m. for minor users, and set 60 minutes per day as the maximum limit of video exposure for minors.

Changes are likewise recorded in the area of advertising, where, for example, Tik Tok provides a set of disclosures for users between 16 and 17 years old with regard to the operation of advertisement alerts, while it has disabled, by default, personalized alerts for all minor users.

Changes are likewise recorded in the area of advertising, where, for example, Tik Tok provides a set of disclosures for users between 16 and 17 years old with regard to the operation of advertisements, while it has disabled, by default, personalized alerts for all minor users.

In terms of security, the Tik Tok platform also shows that it is among the most active. In fact, for users under the age of 16, the option to send private messages with stranger users has been disabled, by default, while Instagram places an alert -

[27] Ofcom's *Children and parents: Media use and attitudes report* (2023) (www. ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-and-parents-media-use-and-attitudes-report-2023); Pew Centre's *Teens, social media and technology 2023* (https://www.pewresearch.org/internet/2023/12/11/teens-social-media-and-technology-2023/); and YPulse's 'These are European Gen Z's top social media platforms' (www.ypulse.com/article/2023/06/13/ we-these-are-european-gen-zs-top-social-media-platforms).

ISSN 2281-5147

"suspicious behavior" - next to the account of adult users for whom there is unusual interaction activity with accounts of underage users.

Another example worth mentioning is concerning a British platform offering online games with 60 million users, called Poki.

In early 2023, an investigation conducted by the 5Rights Foundation revealed that, despite being accessed by millions of users in the UK, many of whom were under the age of six, the Poki platform continued to commit a series of violations: it tracked children's activities by default; it geolocated and monitored users without their consent; it shared children's data with third parties, often for "unspecified purposes"; it used 'nudge techniques' (dark patterns), manipulating children and inducing them to reduce their privacy settings. Children's profiles, their precise geolocation, and detailed information about their gaming practices and habits were shared directly with more than 300 external companies, advertising and marketing companies, analytics companies, and data brokers located in the United Kingdom, the United States, and China.

Following a formal communication sent by 5Rights in March 2023, and eight months of subsequent consultations, the platform radically revised the design of its system to comply with the Age Appropriate Design Code.

The changes made include: changing the default settings to ensure the highest level of privacy; limiting cookies; replacing profiling-based advertising with contextual ads; disabling the geolocation feature; and revising the privacy policy to make it more understandable and accessible. It is worth noting that the company has decided to implement these measures for *all users*, without distinction between adults and minors, as required by standard no. 3 on age-appropriate application.

While we are aware that a key role has also been played by investigations and, at times, sanctions imposed by the relevant national privacy authorities, nevertheless, the emerging data appear comforting and seem to confirm that the path indicated by the UK Code is appropriate.

A further observation should be made with regard to the fact that the examples given- although they constitute a huge step forward, rarely represent the rule and, above all,

ISSN 2281-5147

do not imply that all 15 standards are complied with and applied simultaneously by all the actors involved.

On this point, it should be remembered that one of the distinguishing traits of the Code, is precisely the fact that it has envisaged and constructed a mechanism that does not end with mere compliance with the standards by the companies, but provides for the active involvement, at the same time, of the child and the family, as well as, more generally, of the institutions. This ensures that all these actors contribute to its implementation, each for their own role and responsibility, so that the goal is achieved.

In this way, that much-feared "digital tsunami" Stefano Rodotà was talking about, is averted and, instead, a personal protection network is implemented, which, however, needs the involvement of all stakeholders[28] .

4. Imitation and circulation of the Code: does it work?

The affirmation of the UK Age-Appropriate Design Code in the United Kingdom has sparked particular interest also overseas, both in Europe and in North America. In fact, since 2021, there has been a significant spread of the British Code, along with scattered instances - mainly in Europe and the US - of imitation, prompting some brief considerations on the circulation, imitation, and reception of models.

Without any claim to delve into a topic that has been addressed by leading scholars[29], one wonders whether – in fact – the hypothesis of the English Code could fall within

[28] S. Rodotà, *Il Diritto di avere diritti*, Bari, 2014, p. 337, who underlines how data, particularly personal data, are "attratti nell'orbita onnivora del sistema delle imprese e degli organismi di sicurezza".

[29] A. Watson, *Legal transplants: an approach to comparative law*, Edinburgh, 1974; Id., *Law and legal change*, 38 Camb. L. J., 1978, p. 313.; Id., *TwoTier Law, an approach to law making*, Int. & Comp. L. Q., 1978, p. 552; Id., *Legal change: sources of law and legal culture*, 131 Un. of Pennsylvania L. Rev., 1983, p. 1121. On some critics to Alan Watson's work, see O. Kahn-Freund, *Book Review, Legal Transplants*, 91 L.Q.R., 1975, p. 292; W. Twining, *Diffusion of law: a global perspective*, Journal of Legal Pluralism, 2004, p. 49; Id., *General jurisprudence: understanding law from a global perspective*, London, 2009; P.G. Monateri, *The 'Weak Law': Contaminations and Legal Cultures (Borrowing of Legal and Political Forms*), 2008, on line https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1300298. On formants and circulation of models, R. Sacco, *Legal Formants: A Dynamic Approach to Comparative Law*, I, *The American Journal of Comparative Law,* 1991, pp. 39, e 34 and II, p. 343; R. Sacco, A. Gambaro, *Sistemi Giuridici Comparati*, Torino, 1996, 4; R. Sacco, Circolazione e mutazione dei modelli giuridici, Digesto civ., II, Utet, Torino, 365.

ISSN 2281-5147

the phenomenon whereby, in sectors that present very similar issues and problems to be resolved. The acquisition of models already tested in other contexts would facilitate a 'virtuous' process of reforms[30] and, in a certain way, could convince national and international actors to adopt such similar models[31]; thus also achieve a certain level of 'spontaneous harmonization' of protection standards and fundamental principles[32], obviously on the condition that the phenomenon is framed taking into account the historical and evolutionary differences and the context of the individual systems and, therefore, their legal traditions.

As it has been observed, in fact, '*the circulation and imitation of the model does not depend so much on the intrinsic qualities of the legal system or the model being imitated, but rather on the strategies and problems of the system that is imitating*'[33].

In this regard, the drafting of the English Code has certainly helped to rekindle the interest of the international community and, consequently, of national legislators, on the matter of child protection in the digital world, offering a new perspective to address the issue, considering, on the one hand, the concrete profile that characterizes

---

On the dialogue between Sacco and Watson, see S. Ferreri, *Assonanze transoceaniche. Tendenze a confronto*, in 1, Quadrimestre, rivista di diritto privato, 1993, p. 179; U. Mattei, *Why the wind changed. Intellectual leadership in western law*, 42, Am. J. Comp. Law, 1994, p. 195; A. Watson, *From legal transplants to legal formants*, 43 *American Law Journal of Comparative Law*, 1995, 3, 469; P.G. Monateri, *Black Gaius*, 51 *Hastings L.J.*, 2000, p. 510; M. Graziadei, *Comparative Law, Transplants, and Receptions*, in M. Reimann e R. Zimmermann (edited by), The Oxford Handbook of Comparative Law, 2. ed., Oxford, 2019, p. 442 ss; AA.VV., *Esperienze giuridiche in dialogo. Il ruolo della comparazione*, M. Graziadei and A. Somma (eds), Roma, 2024, passim.

[30] A. Dondi, *Comparazione oggi. Brevi (e molto limitate) impressioni dal côté processuale*, in A. Somma, V. Zeno-Zencovich (edited by), Comparazione e diritto positivo. Un dialogo tra saperi giuridici, Roma, 2020, p. 333 ss.

[31] M. Graziadei, *Legal Transplants and the Frontiers of Legal Knowledge*, in Theoretical Inquiries in Law, 2009, (10) 2, p. 693. See, also, in the matter of environmental protection, B. Pozzo, *Modelli notevoli e circolazione dei modelli giuridici tra in campo ambientale: tra imitazione e innovazione*, in Studi in Onore di Antonio Gambaro. Un giurista di successo, Milano, 2017, p. 351.

[32] G. Benacchio, *Diritto privato della Unione Europea*, Milano, 2016, p. 131 ss, regarding the phenomenon of the circulation of rules and legal models in Europe. Specifically in the European legal context, the Author underlines that this analysis represents a very useful tool in order to understand the role exercised by the so called 'competition among models' in the legislative process. See, also, A. Plaia, (edited by), *La competizione tra ordinamenti giuridici. Mutuo riconoscimento e scelta della norma più favorevole nello spazio giuridico europeo*, Milano, 2007; A. Zoppini, *La concorrenza tra ordinamenti giuridici*, Roma, 2004.

[33] A. Miranda, *Trapianti giuridici, circolazione dei modelli e persistenza della norma: l'insegnamento di Alan Watson*, in A. Miranda, *Diritto e tradizione. Circolazione, decodificazione e persistenza delle norme giuridiche*, Palermo, 2004, p.17.

ISSN 2281-5147

the standards and, on the other, the involvement of the many actors directly affected by this issue. If we look at what has happened since the Code was issued in the United Kingdom, we can see a series of related or influenced initiatives, such as the approval of similar Codes in the state of California and other US states, as well as in the Netherlands, the publication of the UN General Comment n. 25 specifically referring to the rights of children in the digital dimension – directly inspired by the English Code – together with similar initiatives by the EU institutions on the subject.

On the other hand, despite the general agreement on the rationale and intentions of the original English model, an overview of these initiatives also reveals a series of differences and difficulties related, among other things, to environmental, political, and cultural factors which, to varying degrees, affect the reception of the Code model.

It is the case of the California Age-Appropriate Design Code (CAADC), approved on September 15th 2022 by the state Assembly. The CAADC is inspired by the UK Age-Appropriate Design Code and is primarily aimed at all companies that offer online services that are likely to be accessed and used by minors.

This is the first piece of legislation in the United States that is directly inspired by the *by design* approach; it shares the general structure of the UK Children's Code, from which it borrows the indication of the standards in a similar way, but at the same time differs from it in some respects.

The analysis of the Californian legislation must necessarily take into account two areas of investigation: the first with respect to the federal legislation on the privacy of minors currently in force; the second with respect to the British Code. Both are significant in order to fully understand the main characteristics of the CAADC.

Regarding the federal legislation, the Children's Online Privacy Protection Act (COPPA) which regulates the protection of the privacy of minors, has been recently amended after an intense debate in Parliament, aimed at strengthening the protection of minors in relation to the introduction of new technologies. In this regard, a number of proposals for reforming COPPA – known and ultimately conveyed in the amendments known as COPPA 2.0 – have been put forward, starting in 2023, which

ISSN 2281-5147

aim to extend the protection of minors online, particularly concerning the processing of their data by digital platforms[34].

At the same time, another bill has been introduced (but still not passed into legislation) — the Kids Online Safety Act (KOSA) — which requires digital platforms to exercise a so-called duty of care, i.e., the obligation to implement a series of reasonable measures, mainly in terms of protecting minor users from the now very frequent phenomenon of cyberbullying. Moreover, it has to be observed that at the moment this paper is written, a comprehensive package has been introduced to the Senate – namely KOSPA (Kids Online Safety and privacy Act)[35] which includes both KOSA and COPPA 2.0. The bill, tough, languished for quite some time in the House of Representatives, due to the reservations of the Republican party and has not been approved yet. The main debate being around the notion of 'duty of care' and the recipients of this duty, also in consideration of the numerous 'interventions' by the actual administration aimed – *de facto* – at diminishing the duty of the (big tech) companies to protect minors online.

In the meantime, it is worth noting that, with regard to the subjective scope of application, while the text of the federal legislation previously in force (COPPA) considered only persons under the age of 13 to be minors, a limit also provided for in the European General Data Protection Regulation (GDPR), the new COPPA 2.0 (but not the KOSA proposal neither the KOSPA) adopts – albeit limited to the case of targeted advertising – a broader concept of a minor, even if not yet in line with that provided for by the UN Convention and the English Children's Code – *i.e.*, an individual under the age of 18 – which in turn is also provided for by the text of the California Code.

The new COPPA 2.0 amendments, in fact, sets the limit at 16 years of age, with a view to also including the adolescent age group that was previously excluded. Moreover, the new name of COPPA 2.0, namely the Children and Teens' Online Privacy Protection Act, would seem to confirm this choice.

[34] On June 23, 2025 the amendments went into effect, while the Federal Trade Commission finalised them in April 2025. The compliance deadline for companies is April, 2026. See the FTC official web page.

[35] See, https://www.congress.gov/bill/118th-congress/senate-bill/2073.

ISSN 2281-5147

Another important issue that will have to be addressed, and which is likely to be the subject of heated debate, especially between more conservative and more progressive groups, is that of parental consent.

While the federal texts both of COPPA and of COPPA 2.0 are based precisely on the latter, *i.e.*, the necessary authorization of parents for minors to use online services (with poor results, however), the Californian text, adopting the rationale of its British counterpart, which in turn refers to the principles of the UN Convention on the Rights of the Child, embraces a different idea of 'protection', aiming at pursuing the best interests of minors through a series of requirements intended primarily for commercial operators and only secondarily for family members, with a view to gradually empowering all those involved.

With respect to the analysis of the British Code, it is necessary to reflect on the general structure of the two codes of conduct and, in particular, on the premise from which each of them originates and develops.

While the British Code, as previously mentioned, is based on and refers to the principles and rights contained in the UN Convention on the Rights of the Child (it is rooted in the UN Convention), the CAADC is a separate piece of legislation that, in general terms, refers to the best interests of the child. The CAADC obviously lacks any link to the Convention, given that the United States is the only country in the world that has never ratified it. This shortcoming gives rise to two considerations.

On the one hand, it indicates that the CAADC lacks the foundation and set of principles which, when interpreted as a whole, represent some of the key elements for a new and different conception of the child, which underpins the Convention itself and which play an important role, as seen in the English case, in the implementation of the standards contained in the Code. The notion of best interests, as regulated by Article 3 of the Convention, is, in fact, a tool that must be coordinated with the rest of the provisions in order to affirm the other principles, including that of evolving capacities.

On the other hand, it prompts reflection on the interpretation of the concept of best interest in the US legal framework. In this regard, it should be noted that this principle became established in American family law during the 19th century, in the context of

ISSN 2281-5147

custody cases in divorces. Outside its original scope — in which it has been repeatedly criticized for its vagueness — it has found effective recognition in state legislation, especially in matters of adoption, but not the same clarity in the jurisprudence of the Supreme Court, which has shown a fluctuating orientation on several occasions[36].

In fact, in 2015, in the well-known case of *Hobergefell v. Hodges*[37], the judges recognized the right to marriage for same-sex couples, also in consideration of the need to safeguard the best interests of minors within the family unit, at the same time, in a series of other cases, the Court gave priority to the concrete assessment of the best interests of the child over other absolute legal presumptions, *i.e.*, it considered that the best interests must in any case be weighed and considered in relation to other responsibilities, primarily those of parents and public authorities[38].

In this respect, it is once again necessary to 'read' the issue taking into account the context in which it arises and, certainly, in the case of the United States, the constitutional balance between federal and state power in matters of family relations has a considerable impact on the limits and connotations of this principle.

In relation to the concept of 'best interests', it is therefore appropriate to refer to the report drawn up by the 5Rights Foundation (the association that promoted the UK Children's Code) and the London School of Economics, published in March 2024[39],

---

[36] L.M. Kohn, *Tracing the foundations of the of the best interests of the child standard in American jurisprudence*, in *Journal of Law and Family Studies*, 2008, p. 358 ss.; C. Breen, *The Standard of the best interests of the child: a western tradition in international and comparative law*, The Hague, 2002.

[37] *Hobergefell v. Hodges*, 35 S.Ct. 2584 (2015) in https://supreme.justia.com/cases/federal/us/576/14-556/case.pdf.

[38] *Flores v. Reno*, 507 US 292 (1993), in https://supreme.justia.com/ cases/federal/us/507/292/case.pdf, in the matter of foreign unaccompanied minors, it was stated that "a venerable phrase familiar from divorce proceedings», is a proper and feasible criterion for making the decision as to which of two parents will be accorded custody. But it is not traditionally the sole criterion – much less the sole *constitutional* criterion – for other, less narrowly channeled judgments involving children, where their interests conflict in varying degrees with the interests of others. […] So long as certain minimum requirements of child care are met, the interests of the child may be subordinated to the interests of other children, or indeed even to the interests of the parents or guardians themselves. […] The best interest of the child is likewise not an absolute and exclusive constitutional criterion for the government's exercise of the custodial responsibilities that it undertakes, which must be reconciled with many other responsibilities».

[39] S. Livingstone, N. Cantwell, D. Özkul, G. Shekhawat, B. Kidron, *The best interest of the child in the digital environment*, March 2024, in https://www.digital-futures-for-children.net/best-interests.

ISSN 2281-5147

entitled 'The best interests of the child in the digital environment', which clarifies the scope and meaning of this expression, which is often abused and misused by companies offering online services to minors.

The research, in fact, reiterates that the continuous development of legislation and regulations on the protection of children's rights, both nationally and internationally, must be matched by equal caution and attention on the part of states and commercial operators in the use of the 'language' of children's rights. In other words, it is not enough to include the expression 'best interests' in order to have fulfilled and effectively followed through on the pursuit of the best interests and protection of the child. The reference to best interests, as well as to other rights, implies, as has been expressly and repeatedly stated, a reference to the entire Convention and, therefore, to the principles on which it is based.

A key passage concerns the United States: the report acknowledges that most tech companies are based in this country, the only one that has not ratified the UN Convention on the Rights of the Child.

However, the US remains a signatory to the Convention, which means that it is still obliged not to act in contravention of it. This becomes particularly important when one considers that the digital services offered by US companies have an impact on the lives of minors all over the world, or almost all over the world.

In this sense, the CAADC seems to have taken on board the message contained in the report, effectively placing itself at the forefront of both the federal Children's Online Privacy Protection Act (COPPA and the amendments) and the failure of the U.S. to ratify the CRC. The CAADC has clearly chosen the British Code as its model: the structure, the identification of standards, and even the name of the code of conduct are direct imitations. Curiously, however, the CAADC refers at the outset to the UN Convention in relation to the need to protect minors in all aspects of their lives.

However, as has been repeatedly pointed out, the federal government's failure to transpose the directive means that for this legal system, of reference to a context – that in which the Convention matured and developed – which represents a more complex and composite reality, made up of legal, cultural, and social elements, of a

ISSN 2281-5147

sensitivity built up over time by the doctrine and the jurisprudence, which have evolved and cannot be replaced simply by inserting the expression 'best interests.' One need only think of the General Comments drafted annually by the UN, which have, from the outset, addressed issues that are crucial to the affirmation of children's rights.

This overview would seem to reveal a tension between the concept of best interest, which has become established over the years, particularly in the case law of the Supreme Court, and that expressed in both the Californian Code and the English Code. In the case of the Code approved in California, in particular, there is a clear need and, at the same time, a difficulty for the state legislator to reconcile the British view, which considers this principle as 'paramount', in line with the UN Convention, with the more 'relativized' view expressed by the courts, as mentioned above. The outcome is not yet clear, as it will be the judges who determine its limits and content.

Other differences between the English Code and the CAADC concern the processing of children's data and the data protection impact assessment, which in the case of the English Code are influenced by the requirements of the GDPR, in the matter of possible harms to rights and freedoms, while in the Californian text are generally referred to as 'material detrimental'.

In light of the above, when comparing the federal legislation on the one hand and the English model on the other, from a more general point of view, it is clear that, unlike the English Code, the Californian text is part of a regulatory and institutional context which seems more complex in certain respects. This is not only because of the presence of the federal level of legislation on the subject but also, and above all, because of the difficulty of balancing the protection of minors with other constitutionally protected freedoms. In particular, as far as we are concerned here, freedom of expression, which, as is well known, is protected at the constitutional level by the First Amendment, emerges in this specific case in its 'multi-directional' nature. The difficulty lies precisely in finding a balance between freedom of expression and self-determination of minors, freedom of expression of platforms and their users, and the duty of control and possible intervention by public authorities.

ISSN 2281-5147

In the specific case of the California Age-Appropriate Design Code, it should be noted that in September 2023, the Federal District Court for the Northern District of California issued a preliminary injunction suspending the Code, as it was deemed contrary to and detrimental to the First Amendment. In turn, the California Attorney General filed an appeal arguing that the content of the law concerns the protection of minors online and does not infringe on freedom of expression or, even less so, free enterprise. Meanwhile, academics, politicians, representatives of child protection organizations, and attorneys general (bipartisan) have filed a document in support of the CAADC text (amicus brief)[40], taking a clear stance in favor of the Code. To date, the decision of the 9th Circuit is pending.

A detail that should not be overlooked in this case is that the district court's injunction was issued in response to an appeal filed by Net Choice[41], a national association that brings together some of the most influential online platforms. To get an idea of the organizations represented, among them are TikTok, Amazon, Meta, Yahoo, Google, and Airbnb, to name just the best known. As is easy to imagine, the interests protected and pursued by Net Choice are certainly different (if not in conflict) with those set out in the CAADC.

In this regard, there is another significant difference with the English Code. As has been mentioned before, the latter is the result of a shared process – from the outset and throughout the drafting process itself – between numerous and diverse stakeholders, including representatives of the digital industry. This does not mean that the conflicts in terms of interests pursued have been completely resolved, but certainly the involvement of all stakeholders from the outset has made it possible to better understand their respective positions and demands.

---

[40] V. Amicus Brief, https://accountabletech.org/statements/broad-group-of-advocates-and-experts-file-amicus-briefs-countering-big-techs-attack-on-landmark-california-law-protecting-kids-online/?cn-reloaded=1. See, also, the remarks by Daniel Solove, one of the leading experts in privacy, https:// teachprivacy.com/first-amendment-expansionism-and-californias-age-appropriate-design-code/.

[41] *NetChoice, LLC, v. Rob Bonta*, Attorney General of the State of California. Order Granting motion for preliminary injunction. V. https://storage.courtlistener.com/recap/gov.uscourts.cand.406140/gov.uscourts.cand.406140.74.0.pdf#page=2.

ISSN 2281-5147

In this respect, the provisions of the Children's Advisory Panel (CAP)[42] and periodic monitoring by the UK Information Commissioner's Office have proved particularly appropriate, as they help to create a more collaborative climate and, above all, ensure that the actual recipients of the regulation are involved in the regulatory process. Perhaps a similar strategy could have been implemented in the case of the Californian legislation.

However, the setback experienced by the CAADC has not discouraged other states, which, following California's example, are approving very similar codes. Following California's legislative initiative, other state assemblies have begun a similar process, approving texts more or less inspired by the California Age-Appropriate Design Code. Each of these has highlighted different aspects in their final or pending versions. An emblematic example of what has been said previously, is offered by the state of Utah, where the legislator's choice is characterized by an approach that is opposite to the British and Californian ones.

In fact, the state government has opted for so-called 'parental consent': this means that minors under the age of 18 must obtain parental authorization to use any social media. The initiative has raised more than one concern: firstly, because there is already federal legislation (the Children's Online Privacy Protection Act – COPPA) which, as mentioned, requires parental consent, and which has not produced the desired effects (given the amendments); secondly, because this choice confirms the evident desire to move away from the English Code model, which, as mentioned, is based on the idea of gradually recognizing a growing level of autonomy for minors. In this way, any decision is left to the parents, effectively nullifying the original idea behind the Code.

From this point of view, the distinctly conservative cultural tradition that characterizes this state's approach to family law, including parent-child relationships, probably plays a role. As is well known, the state of Utah is traditionally linked to the religious

[42] Starting with the first draft of the UK Children's Code drawn up in 2019, the Children's Advisory Panel (CAP) was established to coordinate the various 'souls' of the Code: minors, families, non-governmental organizations, and representatives of the digital industry. For example, UKIE, the association that brings together online game providers, is part of this panel. By holding regular sessions, the aim is to create and maintain genuine engagement and ensure that the Code is a successful outcome. See https://ico.org.uk/about-the-ico/what-we-do/background-to-the-children-s-code/children-s-advisory-panel-cap/.

ISSN 2281-5147

doctrine of the Mormon group, a clear example of the hegemony of religious tradition as a model of social organization[43].

In the case of Vermont and Minnesota, instead, the choice has been to align, generally, to the CAADC and, therefore, to the UK Code[44].

One consideration that can be drawn from the above is that the English Code model is certainly circulating in the United States, albeit with different methods, nuances, and applications. The failure of the US to ratify the UN Convention plays a role in these different modes of reception, but it must be said that, in the case of the North American states, the framework of approved regulations shows a strong dependence on cultural factors, traditions, and, in particular, the role (*rectius* influence) of various stakeholders, as the Net Choice case has clearly highlighted.

While this paper does not focus specifically on the international and the European initiatives on this matter, that require an investigation *ad hoc*, it is of course worth remembering that the UK Code's influence is clearly evident in the General Comment n. 25 issued by the CRC Committee. Without going into details, it is very well known that this Comment is the result of a series of consultations among different groups of actors among which the 5Rights Foundation. Useless to say that the vision embedded by this association played a significant role in the drafting process of the Comment[45].

Among the EU initiatives, the BIK+ strategy and of course the project for a European Age-Appropriate Design Code, represent an important step by EU institutions in the desired direction, as already seen in the British and US experiences, of protecting and promoting children's rights in the digital world.

---

[43] The reference here is to the very well-known classification in legal families by U. Mattei and P. Monateri, *Introduzione breve al diritto comparato*, Padova, 1997.

[44] V. https://mgaleg.maryland.gov/2024RS/bills/hb/hb0603T.pdf; https://www.house.mn.gov/comm/docs/2hIcmA4QN0K9KVMGRvzBpw.pdf.

[45] «The Comment is a culmination of three years of work during which 5Rights Foundation, supported the Committee on the Rights of the Child», in https://5rightsfoundation.com/our-work/childrens-rights/uncrc-general-comment.html.

ISSN 2281-5147

Presumably, the EU Code should be supported by the rules contained in the GDPR and the principles contained in the UN Convention. Given that all EU member states have ratified it, this should – hopefully – be the legal framework of reference.

On the other hand, it should also be remembered that, in the meantime, there have been numerous legislative interventions by EU institutions in the field of digital technology (in the broad sense of the term), from the best-known regulation on artificial intelligence to the approval of the Digital Services Act[46]. All these pay particular attention to the more general protection of fundamental individual rights, with references to the European Charter of Rights, and this is a feature that has generally characterized the process of discussion, drafting, and approval in this specific area[47].

Therefore, the future EU Code of conduct should have the task of providing concrete protection (in the sense intended by the Convention) and, at the same time, promoting the rights of minors online, bringing as much uniformity as possible to a framework which, although rich in valuable initiatives, still appears to be very fragmented and uneven overall. It is worth remembering that The Netherlands has already approved, in 2021, the *Code voor Kinderrechten*[48], expressly referring to the British Children's Code. The Dutch text contains guidelines for companies offering online services that are also accessible to minors, which refer to the principles of the UN Convention and require the adoption of a series of behaviors inspired by the by design approach.

---

[46] https://data.consilium.europa.eu/doc/document/PE- 49-2023-INIT/it/pdf, par. 8, 56 and 101.

[47] This is not the place to examine the stages that led to the approval of the final text of the regulation on artificial intelligence, but it should be noted that many of the difficulties encountered concerned precisely the relationship between fundamental rights and artificial intelligence and the limits – if any – that should be set. There have been many recent contributions published on the subject. I will limit myself to citing the reflections of V. Zeno-Zenchovic, *Artificial intelligence, natural stupidity and other legal idiocies*, *MediaLaws*, 2024, in https://www.medialaws.eu/rivista/artificial-intelligence-natural-stupidity-and-other-legal-idiocies/, who reminds us, if we had ever forgotten, that, regardless of all possible considerations about which approach is best for regulating technology, it is always and only human beings who enter data into the machine and decide what data to enter.

[48] https://codevoorkinderrechten.nl/wp-content/uploads/2021/03/20210311_ Code-voor-Kinderrechten_v1-1.pdf.

ISSN 2281-5147

More generally, the success of a (possible) European Age-Appropriate Design Code seems to be linked to the ability of EU institutions to create - as it has been the case in the UK since the drafting process - the optimal conditions for the various stakeholders to participate in its drafting. From this perspective, a bottom-up approach, as was the case with the Common Core project[49], would be preferable.

This approach, indeed, aims to identify possible common responses and to exclude, instead, intervention imposed from above, could in fact prove to be more suitable for interpreting the needs of the community context.

Otherwise, the project would remain a dead letter or, worse still, could be relegated - like other initiatives - to a purely stylistic-doctrinal exercise.

[49] Originally, as is well known, the *Common Core* project was inspired by an idea of Rudolph Schlesinger, who conducted research on contracts at Cornell University in 1960. V.R. Schlesinger, *Formation of Contracts: a Study of the Common Core of Legal Systems,* New York, 1969, *passim*. The Common Core of European Private Law initiative, led by professors Mauro Bussani and Ugo Mattei as editors of the project, draws inspiration from this research and, in particular, from the methodology on which it is based: the so-called factual approach. The two editors combine this with Rodolfo Sacco's theory of formants, thus arriving at the so-called 'common core method', whose purpose is 'to unearth the common core of the bulk of European Private Law [...] The search is for what is different and what is already common behind the various private laws of European Union Member States [...] Such a common core is to be revealed in order to obtain at least the main lines of one reliable geographical map of the law of Europe." On this point, see M. Bussani, U. Mattei, The Common Core Approach to European Private Law, in 3 Columbia Journal of European Law, 1997-1998, p. 339; M. Bussani, U. Mattei, Preface: the Context, in Bussani and Mattei, The Common Core of European Private Law, 2002, pp. 1–8. The Common Core project has developed along multiple lines, including that relating to the area of family law. The operational unit that carried out the research in this area applied this methodology to some of the most relevant aspects of family law, such as those relating to the division of assets between partners; *support rights and duties; administration and disposition of joint estate; dissolution of joint estate; dissolution of the relationship; family house.* The questionnaires submitted to the national rapporteurs, in fact, drawing directly on Schlesinger's project, are in no way intended to favor one system over another or, worse still, to hide the differences between the various legal systems, but rather to "map eventual common practical solutions, despite the letter of a civil code or statute's rule could provide differently." In the Common Core perspective, the scenario for the transnational lawyer, who approaches family law of different European legal systems, is that of a traveler compelled to use a number of different State's maps, each one containing (quite often) misleading information. The CC method tries to correct those misleading pieces of information, not forcing the actual diverse reality of the law within one single map to attain uniformity, but presenting a complex situation in a reliable way. A. Pera, *Searching for a common core of family law in Europe*, 1 *Opinio Juris in Comparatione*, 2018, p. 58 ff.

ISSN 2281-5147

4. A child centered approach: preserving human dignity as a paramount principle

This brief analysis reveals a fact worth considering: a system where the responsibility for the use of a service or product likely to be accessed by minors is shared between the minors themselves, the family, the institutions, and the company offering the service, it is a system that guarantees not only the protection of minors, but, as we have seen with the Code standards, the promotion of their rights, since it fits fully into the concept of the evolving capacities contained in the CRC. Therefore, this system provides the minor with the tools to deal with the digital dimension, in a conscious and healthy way, in order to benefit from it as much as possible. The premise, let's remember, is to *encourage* aware use, not prohibit it.

From this perspective, therefore, precisely the empowerment we mentioned at the beginning is realized. This approach, authentically based on the principles of the CRC, clearly expresses another fundamental choice: the commitment to protect the *dignity* of the person, a prerequisite for any legal system, even more so considering vulnerable subjects as minors. As a matter of fact, the lesson we can draw from the UK Code is that a child-centered approach can be realized only if, at the same time, we take into consideration the value of human dignity.

This concept, as a matter of fact, in the context of the so-called disruptive technologies, proves to be decisive in preserving the autonomy of the individuals who make up the family unit. As it has been highlighted, *dignity* becomes the guiding principle and the criterion in the relationships between parents and children, between the family and institutions, and even with stakeholders themselves. The protection of human dignity is pragmatically oriented shaping the relationship between the minor and the parents and the duality parental responsibility /control *versus* the self determination of the minor.

In the analysis carried out with reference to the English model, the principle of dignity, in its various forms, certainly represents a recurring, shared, and therefore paramount value. More than any other, dignity is capable of overcoming the undeniable differences between the legal systems, since it is, on closer inspection, a value common to the Western legal tradition and which, therefore, from the point of view of the circulation of models, could also facilitate the acceptance of similar solutions in a future perspective of spontaneous harmonization.

ISSN 2281-5147

Only doing so, we will truly protect the *person*, made of – as Stefano Rodotà reminded us of – a "corpo elettronico" and of a "corpo fisico": two faces of the same medal, complementary, but without the first prevailing on the other[50].

[50] S. Rodotà, cit., 2014.

ISSN 2281-5147

ISSN 2281-5147

MINORS' CONTRACTUAL AUTONOMY IN THE DIGITAL ECOSYSTEM: LEGAL PROTECTION AND SELF-DETERMINATION IN PRIVATE LAW

Alberto Jaci*

Abstract

This paper examines the contractual autonomy of minors in the digital ecosystem through the lens of private law. As children increasingly engage with algorithm-driven platforms and standardised digital contracts, traditional legal doctrines—such as legal capacity, consent, and fairness—face new challenges. The study investigates how private law can respond to the structural vulnerabilities of minors without undermining their evolving autonomy. It proposes enhanced protective mechanisms, including simplified disclosures, assisted validation, and withdrawal rights. At the same time, it calls for a rethinking of core contractual categories in light of technological realities. The analysis supports the development of a digital private law framework that ensures effective protection while enabling minors' responsible participation in online markets.

Table of contents

* PhD Candidate in Private Law at the Department of Political and Legal Sciences at University of Messina. Double blind peer-reviewed contribution.

ISSN 2281-5147

Keywords

Contractual Capacity – Digital Private Law – Minors' Autonomy – Consumer Protection – Algorithmic Contracting

1. Minors, Contracts and Technology: at the Origins of a New Systemic Conflict

The convergence between contract law, digital technologies and the evolving status of minors generates a structural tension within private law: traditional civil law categories are confronted in markets designed to bypass awareness and negotiation. This tension is not merely doctrinal but systemic, calling for an ontological redefinition of the contract in the digital age.

The issue of contractual autonomy for minors in the digital environment raises a dual normative concern: on the one hand, there is a clear need to ensure effective protection against abuse[1], manipulation[2], and excessive commercial exposure[3]; on the other hand, it is equally important to recognise and promote a gradual legal self-

[1] Sonia Livingstone and Amanda Third, 'Children and young people's rights in the digital age: An emerging agenda' (2017) 19 (5) NMS 657.

[2] Queennette Odudu, 'Technological Solutions for Protecting Children From Online Predators: Current Trends and Future Directions' (2024) SSRN 2, 11.

[3] Jenny Radesky, Yolanda Reid Chassiakos, Nusheen Ameenuddin and Dipesh Navsaria, 'Digital Advertising to Children' (2020) 146 (1) AAP 1, 3.

ISSN 2281-5147

determination of minors[4], in line with the evolving capacities principle set forth in the United Nations Convention on the Rights of the Child[5]. Private law is thus confronted with the task of reassessing its traditional categories—such as legal capacity, consent validity, and contractual liability[6]—in light of the specificities of digital interactions and the increasingly active role of minors within the digital ecosystem[7].

This convergence reveals a structural misalignment between the normative premises of classical private law—such as informed consent, symmetrical negotiation, and relational reciprocity—and the realities of algorithmically mediated, opaque, and unilaterally imposed digital contracting. When these dynamics intersect with the specific vulnerabilities of minors, the contract becomes a site of systemic legal conflict: not merely an exception or anomaly, but a disruptive phenomenon that calls for an ontological redefinition of key civil law categories.

2. Capacity and Contractual Autonomy of Minors

In civil law systems such as the Italian and German ones, legal capacity constitutes a fundamental prerequisite to be able to fully exercise own private autonomy.

Article 2 of the Italian Civil Code establishes that full legal and contractual capacity is acquired upon reaching the age of majority, subject to specific exceptions for acts of ordinary administration or for emancipated minors[8]. This framework reflects a

[4] Yves Poullet, 'e-Youth before its judges – Legal protection of minors in cyberspace' (2011) 27 (1) CLSR 6, 10.

[5] UN General Assembly, *Convention on the Rights of the Child* (20 November 1989) UNTS vol 1577, 3, art 5 and art 12 / Srishti Virat, 'Child Rights in the Digital Environment' (2023) V (1) IJLLR 1 / John Tobin, *The UN Convention on the Rights of the Child: A Commentary* (OUP 2019).

[6] Reiner Schulze and Dirk Staudenmayer, *Digital Revolution: Challenges for Contract Law in Practice* (1st edn, Nomos 2016).

[7] Halla Holmarsdottir, Idunn Seland and Christer Hyggen, 'How Can We Understand the Everyday Digital Lives of Children and Young People?' in Halla Holmarsdottir, Idunn Seland, Christer Hyggen and Maria Roth (eds), *Understanding The Everyday Digital Lives of Children and Young People* (PM 2024).

[8] Francesco Rossi, *Capacità e incapacità* (ESI 2018).

ISSN 2281-5147

protective model that assumes minors lack the maturity and awareness needed to undertake binding obligations. This approach finds parallels in German civil law jurisdiction, where §104 BGB provides that minors under the age of seven lack legal capacity entirely, and where contracts entered into by minors over seven are only valid with prior consent or subsequent approval by their legal representatives under §§107–109 BGB. This model, while conceptually aligned with the Italian system, enshrines a stricter mechanism of formal parental control.

As a general rule, minors are not entitled to validly conclude contracts except through their legal representatives or, where expressly provided, with judicial or parental authorisation[9]. However, this traditional model is increasingly challenged by the realities of digital interaction, in which minors regularly engage in activities that involve contractual relationships: accepting standard terms and conditions, making microtransactions, purchasing virtual goods, or subscribing to online services[10].

Against this backdrop, one must question whether the codified approach to contractual capacity remains adequate to address the diffuse, low-value, and high-frequency contractual practices that characterise the digital economy[11]. The rigidity of the current legal regime may lead to dysfunctional outcomes, such as the systematic denial of contractual autonomy even in instances where the minor demonstrates sufficient understanding of the nature and consequences of the act. This calls for a reinterpretation of contractual capacity, not merely as a formal, age-based requirement, but rather as a functional competence to self-determine responsibly in specific contexts[12].

[9] Guido Alpa, *Il contratto in generale. Principi e problema* (2nd edn, Giuffrè 2021).

[10] Fabio Bravo, 'I contratti a distanza e il mercato digitale' in Guido Alpa and Antonio Catricalà (eds), *Diritto dei consumatori* (IM 2016).

[11] Sandra Calvert, 'Children as Consumers: Advertising and Marketing' (2008) 18 (1) TFC 205.

[12] By analogy, the partition between *petits enfants* and *grands enfants*, relevant to health, self-determination and parental responsibility, would be applicable. See: Pasquale Stanzione, 'Persona minore di età e salute, diritto all'autodeterminazione, responsabilità genitoriale' (2013) CDC 21.

ISSN 2281-5147

This perspective aligns with the CRC's principle of "evolving capacity", which calls for respecting minors' autonomy in proportion to their maturity[13].

Private law reveals a tension between protectionist and enabling models, the former focused on vulnerability, the latter on graduated autonomy[14].

A further dimension that requires analysis concerns the relationship between contractual capacity and the meritoriousness of interests pursued[15]. Pursuant to Article 1322 c.c., contractual autonomy may depend on whether the transaction serves a meritorious purpose[16].

3. The Digital Contract: New Challenges

The emergence of the digital contract marks a paradigmatic shift in the architecture of contractual relations[17]. Rather than serving as a negotiated exchange between parties of equal standing, the contract is increasingly embedded in digital infrastructures that automate consent, obfuscate content, and preclude authentic deliberation[18].

Civil law has historically developed the architecture of contract on the basis of principles such as freedom of contract, equality between the parties, and the

[13] Sara Rigazio, 'A Dynamic Perspective on the Minor's Right to Self Determination: the Lesson from the Convention on the Rights of the Child (Crc) and Some Practical Insights from the Entertainment Industry' (2019) C.E.L.B. 3.

[14] Lucilla Gatt and Ilaria Amelia Caggiano, 'Consumers and Digital Environments as a Structural Vulnerability Relationship' (2022) 2 EJPLT 13 / Samuel Issacharoff, 'Disclosure, Agents, and Consumer Protection' (2011) 167 (1) JITE 65.

[15] Rosmawani Che Hashim and Farah Nini Dusuki, 'Minors and Their Incapacity to Contract: A Revisit' (2023) 14 (1) UUMJLS 269.

[16] Mariella Lamicela, 'La riscoperta del giudizio di meritevolezza ex art. 1322,co.2, c.c. tra squilibrio e irrazionalità dello scambio contrattuale' (2016) 5 (2) RG 195.

[17] Tatyana Skvortsova et al., 'Development of Digitization in Contractual Relations' (2019) 87 LNNS 1025.

[18] Nancy Kim, 'Digital Contracts' (2019) 75 TBL 1683.

ISSN 2281-5147

significance of informed consent[19]. Yet, in the digital environment, these principles are often stripped of their substantive content. Consent is often expressed by clicking pre-ticked boxes, without individual negotiation[20]; general terms and conditions are unilaterally drafted, typically lengthy and technical, thereby rendering comprehension difficult even for the average adult user[21]; recommendation algorithms and personalised targeting mechanisms shape user choices, undermining the authenticity of contractual will[22].

These criticalities become exponentially more pronounced when minors are involved. Their increased cognitive, emotional, and relational vulnerability exposes them to the risk of entering into binding obligations without a full awareness of the attendant legal and economic consequences[23]. In such cases, the digital contract risks degenerating into an instrument that constrains, rather than expresses, individual autonomy[24]. Private law must thus confront the adequacy of digital contracts in satisfying the requirements of conscious formation of consent, pre-contractual good faith, and equity in the performance of obligations[25].

Moreover, the mass and serial nature of digital contracts introduces a structural tension between the individual dimension of contractual responsibility and the collective nature of digital market practices[26]. Online platforms do not operate on a relational basis but rather through automated and replicable models, in which

[19] Enrico Gabrielli, *I contratti in generale* (UTET 2006).

[20] Neil Richards and Woodrow Hartzog, 'The Pathologies of Digital Consent' (2018) 96 WULR 1461.

[21] Florian Möslein, 'Digitized Terms: The Regulation of Standard Contract Terms in the Digital Age' (2023) 19 (4) ERCL 300.

[22] Mireia Artigot Golobardes, 'Algorithmic Personalisation of Consumer Transactions and the Limits of Contract Law' (2022) 1 JLMI 18.

[23] James Chang and Farnaz Alemi, 'Gaming the System: A Critique of Minors' Privilege to Disaffirm Online Contracts' (2012) 2 (2) UCILR 627, 642.

[24] Simona Tiribelli, 'Moral and Legal Autonomy in the Era of Artificial Intelligence' (2022) S&F 166.

[25] Martijn W Hesselink, *The Politics of the European Civil Code* (KLI 2006).

[26] Zeynep Ayata, 'European Union Contracts in Digital Environments' in David Ramiro Troitiño (ed) *E-Governance in the European Union* (Springer 2024) 173.

ISSN 2281-5147

contractual content is unilaterally determined and the individual user has virtually no room for influence[27].

This context calls into question the actual applicability of traditional civil law remedies—such as annulment for mistake or coercion, invalidity due to lack of form, or termination for breach—to scenarios that diverge markedly from the classical paradigm of deliberate and informed agreement.

Finally, the increasing integration of artificial intelligence into contractual processes—through chatbots, smart contracts, and dynamically personalised terms—raises novel questions concerning the legal attribution of will, the characterisation of offers, and the validity of consent expressed through automated interactions[28]. This debate must also be read in light of recent European legislation. The Digital Services Act[29] (Regulation EU 2022/2065) expressly prohibits certain manipulative practices—commonly referred to as 'dark patterns'—and reinforces transparency duties, particularly where minors are concerned (art. 28). Similarly, the AI Act proposal prohibits systems that exploit the vulnerabilities of specific groups, such as children, by materially distorting their behaviour (art. 5). These measures show that the European legislator is moving towards a broader recognition of contractual vulnerability in digital contexts.

While these structural transformations raise concerns for all consumers, they become particularly problematic in the case of minors[30]. Here, the systemic opacity and automation of the digital contract intersect with specific legal and cognitive vulnerabilities, giving rise to compounded risks that private law must address with

---

[27] Antonio Orti Vallejo, 'Contractual Relationships in Collaborative Economy Platforms' (2019) 27 (5) ERPL 995.

[28] Norhafiza Awang, 'Contract Law and Artificial Intelligence: Examine the Implications of AI on Contract Negotiation and Execution, Including the Challenges of Automated Contracting' (2024) 7 IJARBSS 93.

[29] Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) [2022] OJ L277/1. / Caroline Cauffman and Catalina Goanta, 'A New Order: The Digital Services Act and Consumer Protection' (2021) 12 (4) EJRR 758.

[30] Oleksandr Omelchuk, Olena Cherniak and Nataliia Tyshcuk, 'Protection of the rights of children and minors in their transactions in the information society' (2020) 9 (2) IH 25.

ISSN 2281-5147

heightened sensitivity. It should be emphasised that vulnerability in digital contracting is not confined to minors. Situational vulnerabilities—such as impulsive behaviours induced by algorithmic recommendation systems or persuasive design techniques—may affect adult users as well. The European debate thus increasingly conceptualises vulnerability as a relative condition, not only linked to age, but also to the cognitive and relational context in which contractual decisions are made.

4. The Minor in the Digital Contracts: Critical Issues

Once minors enter this transformed contractual landscape, the criticalities described above become exponentially more severe. Their position as legally and cognitively unprepared subjects makes them particularly susceptible to contractual mechanisms that bypass understanding, inhibit negotiation, and impose obligations through design rather than dialogue[31]. The interaction between rules governing minors' legal capacity and the structural features of digital transactions necessitates a critical reassessment of the traditional mechanisms underpinning contractual obligation[32].

First and foremost, digital contracts frequently lack any effective *ex ante* mechanism for verifying the user's legal status. This undermines the coherence of the protective legal framework, which is largely premised on the invalidity or voidability of acts entered into by those lacking capacity, while simultaneously exposing minors to obligations they may not fully understand or evaluate[33].

The standardised nature of contractual terms on digital platforms further reduces minors' ability to comprehend and critically assess the content of contracts. This issue becomes even more acute in the presence of dark patterns or implicit persuasive

[31] Antonio Landi, 'I fornitori di servizi di intermediazione molto grandi' in Luca Bolognini, Enrico Pelino and Marco Sciadone (eds) *Digital Services Act e Digital Markets Act. Definizioni e prime applicazioni dei nuovi regolamenti europei* (TAL 2023).

[32] Irene Longo, 'Capacità e incapacità delle persone di età minore : alcuni spunti sul contratto telematico' (2016) 3 RIIG 391.

[33] Guido Alpa, 'I contratti del minore. Appunti di diritto comparato' (2004) 5 IC 517.

ISSN 2281-5147

techniques, which may induce the minor to perform dispositive acts without an authentic manifestation of contractual intent[34].

Another critical issue concerns the liability arising from contract performance. At the same time, the ability of legal representatives to invoke annulment under Article 1425 or appeal of the contract under Article 1426 of the Italian Civil Code may generate uncertainty in contractual relations, especially where the act in question has already produced significant economic effects or has been partially or fully executed[35]. Interestingly, German law adopts a more structured *ex-ante* approach: under §110 BGB (the so-called "Taschengeldparagraph"), minors may enter into contracts without parental consent only when the consideration is fully paid with means provided for that purpose. While this provision offers a narrow window of autonomy, it also implies a presumption of informed consent linked to financial limitation, which is absent in the Italian framework.

Additional concerns arise from evidentiary difficulties in proving minority status and lack of parental authorisation, particularly in digital environments that lack traceable or authenticated records[36].

Finally, from an axiological perspective, a fundamental tension emerges between the principle of contractual freedom and the imperative of legal protection for minors[37]. On the one hand, minors are increasingly active participants in the digital economy, demonstrating growing relational and decision-making capabilities[38]; on the other

[34] Katri Nousiainen and Catalina Perdomo Ortega, 'Dark Patterns in Law and Economics Framework' (2024) 36 (1) LCLR 90.

[35] Francesco Rossi, 'Contratti del minore e responsabilità per i danni prodotti alla controparte' (2021) 1 Familia 3.

[36] If it is proved that the parents failed to exercise control and that the other party was harmed, the principle of *culpa in educando* may abstractly apply. See: Court of Cassation, Section 3, Civil, Judgment February 19, 2014 No. 3964.

[37] Eleonora Grossi, *La tutela del minore nel commercio elettronico e nella rete internet* (LIUC 2003).

[38] Anna Gambaro, 'Il bambino consumatore: il suo diritto ad una appropriata informazione' (2010) 12 SSF 221.

ISSN 2281-5147

hand, there remains a pressing need for legal safeguards that cannot be wholly delegated to the logic of the free market[39].

5. Protection and Empowerment

A first set of instruments comprises *ex ante* control mechanisms, aimed at preventing minors from entering into contractual relationships in conditions of unawareness or without supervision[40]. In this regard, the implementation of effective age verification systems represents a fundamental technical and legal requirement[41]. However, such systems must be carefully designed to strike a balance between legal certainty and the protection of minors' digital rights and privacy, avoiding disproportionate forms of profiling or surveillance[42].

A further remedy lies in the adoption of enhanced contractual disclosures, drafted in simplified, comprehensible, and visually accessible language tailored to users in developmental stages[43]. In this sense, the imposition of a heightened duty of transparency upon digital service providers towards minor users is proposed, as a specific application of the general principle of pre-contractual good faith[44].

---

[39] Novriyanto Nusi, 'Electronic Legality Of Employment Contracts On Minor Children' (2020) 2 (2) ESLAW 293.

[40] Shilpa Das, 'Ex-Ante Regulation: An Evolving Need in Digital Markets' (2024) 5 (1) CCIJOCLP 55.

[41] Simone Van Der Hof and Sanne Ouburg, 'We Take Your Word for It' - A Review of Methods of Age Verification and Parental Consent in Digital Services' (2022) 8 EDPLR 61.

[42] Karolina La Fors-Owczynik, 'Prevention strategies, vulnerable positions and risking the 'identity trap': digitalized risk assessments and their legal and socio-technical implications on children and migrants' (2016) 25 (2) ICTL 71.

[43] Natali Helberger et al., 'Digital Content Contracts for Consumers' (2013) 36 JCP 37.

[44] Virginia Portillo et al., 'A call to action: Designing a more transparent online world for children and young people' (2024) 19 JRT 1.

ISSN 2281-5147

A third area of intervention concerns assisted validation or subsequent ratification mechanisms, whereby a contract entered into by a minor may acquire legal effect upon authorisation by a legal representative, potentially subject to judicial oversight[45].

In Germany, a similar mechanism operates through §§108 and 109 BGB, which render the effectiveness of a contract concluded by a minor contingent upon the timely approval or rejection by their legal guardian. This institutionalised ratification system could inform future Italian reforms aiming to balance autonomy and protection in a predictable framework.

Particularly significant is the provision of a right of withdrawal without penalty[46], exercisable within a reasonable period, as a post-contractual safeguard for acts undertaken without sufficient deliberation[47]. This remedy operates as an ex-post corrective, capable of neutralising detrimental effects without undermining the stability of legal transactions.

Lastly, it is essential to promote educational instruments grounded in private law. The dissemination of a culture of informed contracting, beginning at the school level, may constitute a structural measure of legal empowerment[48]. Digital contractual literacy should be understood not merely as a technical skill, but as the progressive exercise of individual autonomy, linked to the capacity to evaluate risks, consequences, and obligations. The inclusion of these safeguards finds further support in European legislation: while the DSA strengthens duties of transparency and limits on manipulative design towards minors, the AI Act[49] (EU Regulation n. 2024/1689) introduces a horizontal prohibition against exploiting users' vulnerabilities. Taken

[45] Jasper Verstappen, *Legal Agreements on Smart Contract Platforms in European Systems of Private Law* (LGTS 56, 2023) 55.

[46] Directive 2011/83/EU of the European Parliament and of the Council on consumer rights [2011] OJ L304/64, art 9.

[47] Reinhard Steennot, 'The right of withdrawal under the Consumer Rights Directive as a tool to protect consumers concluding a distance contract' (2013) 29 (2) CLSR 105.

[48] Catherine M. Lemieux, 'Learning contracts in the classroom: Tools for empowerment and accountability' (2001) 20 (2) SWE 263.

[49] Regulation (EU) 2024/1689 (Artificial Intelligence Act) [2024] OJ L. / Celso Cancela-Outeda, 'The EU's AI act: A framework for collaborative governance' (2024) 27 IoT 2.

ISSN 2281-5147

together, these provisions anticipate a model of digital private law in which contractual fairness is no longer measured exclusively by formal consent, but also by the substantive protection of vulnerable users.

6. Prospective Outlook: What Role for Private Law?

Yet, the centrality of contract as a mechanism for the voluntary regulation of legal relationships—especially in digital contexts—restores to private law a crucial role in constructing a legal order capable of reconciling liberty with protection. Regulating digital contracts demands an intelligent and selective adaptation of traditional legal institutions, without relinquishing the protective and axiological function of private law[50].

In this light, private law must operate as a "second-generation" legal order, mediating between the individualistic logic of private autonomy and the imperative to protect vulnerable subjects, particularly minors[51]. The challenge, however, is not merely legal, but also institutional and cultural. A dialogical and intersystemic private law is needed—capable of engaging constructively with EU law (notably the AI Act, the DSA and the GDPR[52]), and with the pedagogical and constitutional dimensions of minor protection.

In this regard, private law cannot ignore the impact of the AI Act, which, alongside the DSA, shapes a European framework of digital fairness. Both instruments acknowledge that the manipulation of vulnerable individuals, whether minors or adults, constitutes a systemic threat to autonomy. These developments suggest a gradual convergence between consumer protection law, data regulation, and private law principles.

---

[50] Guido Alpa, 'Il mercato unico digitale' (2021) 1 CIE 1.

[51] Martha Albertson Fineman, *Equality, Autonomy, and the Vulnerable Subject in Law and Politics* (1st edn, Routledge 2013).

[52] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1. / Felix Zopf, 'Two Worlds Colliding - The GDPR in between Public and Private Law' (2022) 8 EDPLR 210 / Ilaria Amelia Caggiano, 'Protecting Minors as Technologically Vulnerable Persons through Data Protection: An Analysis on the Effectiveness of Law' (2022) 1 EJPLT 27.

ISSN 2281-5147

7. Towards a Digital Private Law for Childhood

The concept of contractual capacity, the principle of private autonomy, and the disciplines of information and liability must be reinterpreted in an adaptive manner—without abandoning doctrinal rigour but embracing a functional and dynamic reading[53]. In this respect, the proposal for a digital private law for childhood is not merely a theoretical aspiration; it is a systemic necessity. It calls for a legal space capable of articulating protection and empowerment, recognising the progressive maturation of the minor subject, and providing legal instruments that safeguard without excluding[54].

The path forward is twofold: the elaboration of normative, jurisprudential, and doctrinal solutions that are consistent with the complexity of the digital environment; the promotion of basic legal education that enables minors to acquire awareness of their rights and obligations. From this perspective, private law is not merely a technical discipline, but a fundamental component of the democratic project, capable of contributing to a more just, transparent, and inclusive digital society. Looking ahead, the development of a digital private law framework for minors may contribute to building a more just, inclusive, and proportionate legal system—one in which minors' participation in economic life is not relegated to a regulatory grey area, but governed by principles of shared responsibility, graduated autonomy, and effective protection[55].

[53] Mark Tunick, 'State Authority, Parental Authority, and the Rights of Mature Minors' (2023) 27 TJE 7 / Grzegorz J. Blicharz, 'Consumers as Unassisted Minors: Asymmetrical Sanction for Unfair Contract Terms' (2022) 11 (6) Laws 87.

[54] Liat Franco and Shulamit Almog, 'Precarious Childhood: Law and its (IR)Relevance in the Digital Lives of Children' (2019) 7 (1) PSJLIA 53.

[55] Charles Alves de Castro, Aiden Carthy and Isobel OReilly Dr, 'An Ethical Discussion About the Responsibility for Protection of Minors in the Digital Environment: A State-of-the-art review' (2022) 9 (5) ASSRJ 343.

ISSN 2281-5147

ISSN 2281-5147

LET'S PLAY TOGETHER: FAIR RULES FOR MINOR VIDEO GAMERS A RESEARCH AGENDA

Federica Casarosa* and Lavinia Vizzoni*

Abstract

This short paper provides for a research agenda dedicated to the critical position of minors as video game players in the EU scenario. Firstly, minors are contextualized in the digital scenario as primary users of several applications, also AI-based, but at the same time exposed to the consequent risks. Then, the specific case of young video gamers is considered, with its implications related to crucial issues like the processing of minors' personal data, unfair business practices and the nature of the video game itself.

In the EU legal framework, few solutions emerge, however, along with some confusion and overlapping rules. The contribution aims at highlighting such challenges, providing initial indications to be further discussed in academic literature on how to protect minor gamers, with the objective of finding effective solutions without, at the same time, excluding children from entertainment.

Table of contents

* Federica Casarosa is a Research Affiliate at the Scuola Superiore Sant'Anna and Lavinia Vizzoni is a Tenure-track Assistant Professor at the University of Pisa. Double blind peer reviewed contribution.

ISSN 2281-5147

Keywords

Minors – Video games – Data protection – Artificial intelligence – Capacity of discernment

1. Introduction. Minors in the digital context between risks and opportunities

The rapid development and consequent massive diffusion of scientific and technical knowledge and applications[1] has affected all areas of individuals' activities, and specifically, it has prompted a profound debate concerning the role and protection of the person under the age of 18 years. Among the different perspectives, an interesting dimension emerges, giving rise to a new chapter in the regulation of juvenile and family law:[2] Gaming and virtual reality played by minors.[3]

In general, minors commonly make use of applications that employ digital technologies, sometimes supervised and/or supported by their parents and relatives, sometimes, instead, in complete autonomy.[4] Statistics show that minors are the users

[1] On the relationship between law and science, see Giorgio Oppo, 'Scienza, diritto, vita umana', in Riv. dir. civ. (2002) I, 11 who points out that applied science, and thus technology, is ontologically destined to be regulated by law. See also, Guido Alpa, 'Tecnologie e diritto privato, in Riv. it. sc. giur. (2017) 205.

[2] Talks about new "dimension" of family law Amalia Chiara Di Landro, 'Best interest of the child e tutela dei minori nel dialogo tra legislazione e giurisprudenza, giurisprudenza' in Nuove leggi civ. comm. (2020) 2, 452. On the relationship between new technologies and family law and the theorization of a kind of "cyberfamily," see Sandro Nardi, *La famiglia e gli affetti nell'era digitale*, Naples, 2020, 7 ff. and with specific regard to children, 39 ff.

[3] M. V. Birk, S. van der Hof, and A. van Rooij, 'Behavioral design in video games' in Games: Research And Practice (2024) 2(2), 1-3; E. Fosch Villaronga, et al., 'Toy story or children story?: Putting children and their rights at the forefront of the artificial intelligence revolution' in Ai & Society (2021) 38(1), 133-152.

[4] Francesco Di Ciommo, *Evoluzione tecnologica e regole di responsabilità civile* (ESI, 2003) 32 ff. On the massive diffusion of new technologies in the daily lives of minors as well, see also Emanuela Andreola, *Minori e incapaci in Internet* (ESI, 2019) 22 ff.

ISSN 2281-5147

par excellence of certain content:[5] from accessing and surfing the Net, to browsing social networks, usually through smartphones. These activities exploit devices whose operation maybe also based on Artificial Intelligence systems, interconnected within Internet of Things,[6] such as wearables,[7] smart home speakers[8] or smart toys, as well as video games consoles. However, such high diffusion is not always coupled with knowledge and awareness of the risks emerging from such an environment.[9] An example of the possible risks comes from the affair of the "Hello Barbie" smart toy: the Mattel doll released in 2015 was equipped with a microphone and software able to interact with children. However, the conversations were not just a trigger for the reactions of the doll but were recorded and stored on cloud, after the interaction. Then, the recordings were transmitted to a California company specialized in the development of AI systems, with the aim of improving the relevance and quality of the interaction the toy has with its young owner.[10] When this process was uncovered, issues regarding data protection and security were raised along with claims regarding bias and discrimination in the speech interactions provided, leading to the discontinuation of the smart toy production.

The example shows that minors, more candid and willing to engage in imaginative play, are less conscious of the risks, and may become victims of offences perpetrated through smart technologies.[11] Thus, the potential fragility of minors demands special

[5] Unicef, The State of the Children in the European Union in 2024. In particular, the statistics show that in 2023 in the EU, 97 % of people under 15 have access to Internet". See the Digital technology policy brief at https://www.unicef.org/eu/media/2826/file/Digital%20technologies%20policy%20brief.pdf.pdf.

[6] See Rolf H. Weber, 'Internet of Things - Need for a New Legal Environment?', in Computer Law & Security Review (2009) 521. On the potential of the IoT, see Amedeo Santosuosso, *Intelligenza artificiale e diritto* (Giuffrè, 2020) 180 ff.

[7] See Italian Data Protection Authority Order No. 179 of March 26, 2015, Launching the Public Consultation on the Internet of Things.

[8] Lavinia Vizzoni, *Domotica e diritto*. La *Smart Home tra regole e responsabilità* (Giuffrè, 2021) 72 ff.

[9] For an overview of the digital risks see UNICEF (n. 5), p. 4. See also Ronny Bogani and Burkhard Schafer, 'Artificial Intelligence and Children's Rights', in Marcello Ienca et al. (eds), The Cambridge Handbook of Information Technology, Life Sciences and Human Rights (Cambridge University press, 2022), 217 ff.

[10] On the matter, see Irina D. Manta, David S. Olson, 'Hello Barbie: First They Will Monitor You, Then They Will Discriminate Against You. Perfectly' 67 *Alabama Law Review* (2015)135.

[11] See also Bogani and Schafer (n. 9) who underline that children are more vulnerable than adults due to their developmental psychology and in particular to "*their emotional volatility and impulsiveness, which provides a unique opportunity for online marketers to reach a particularly vulnerable target customer market*", 218.

ISSN 2281-5147

attention.[12] Indeed, the consequences of uncontrolled exposure to the risks of the digital ecosystem can become devastating with respect to subjects who, being physiologically in a psycho-physical condition of vulnerability, it is easily influenced in their capacity for self-determination.[13]

However, the aforementioned risks must not outweigh the benefits springing from the use of technologies. The use of various digital tools by minors represents a form of manifestation of their personal and digital identity, integrating a decisive moment in the formation of their personality, in a context in which the physical world and the virtual world represent two articulations of the same space of relationship.[14] This is confirmed by fundamental rights principles and declarations both at the supranational and at the national levels: first, the UN Convention on the Rights of the Child (hereafter UN CRC)[15] recognizes that the welfare and development of children should be protected, allocating a set of rights to children; then, Art. 24 of the EU Charter of Fundamental Rights affirms that children's well-being entails protection and care, as well as recognition of their opinions and choices.[16] In more general terms, finally, Article 2 of the Italian Constitution implies that the minor can freely express and develop his or her personality, which means that the minor can freely move in that direction for the realisation of their identity interests.[17]

---

[12] The delicate relationship between young users and the Internet is investigated, among others, by Alessandro Mantelero, 'Teens online and data protection in Europe' in Contr. impr. Europa (2014) 442., Id, 'Children online and the future EU data protection framework: empirical evidences and legal analysis' in Int. J. Technology Policy and Law (2016) 169, Carolina Perlingieri, 'La tutela dei minori di età nei social networks' in Rass. dir. civ. (2016) 1324.

[13] Talks about the "vulnerability" of the "electronic body" of "digital native minors", Antonina Astone, *I dati personali dei minori in rete. Dall'internet delle persone all'internet delle cose* (Giuffrè, 2019) 5 ff; Ilaria Garaci, 'Il "superiore interesse del minore" nel quadro di uno sviluppo sostenibile dell'ambiente digitale' in Nuova giur. civ. comm. (2021) 801.

[14] See Arianna Thiene, 'I diritti della personalità dei minori nello spazio virtuale', in Annali online did. e form. doc. (2017) 13/2017, 26.

[15] Convention on the Rights of the Child, adopted on 20 November 1989, by General Assembly resolution 44/25.

[16] M. Kellerbauer, M. Klamert, and J. Tomkin (eds), 'Article 24 CFR', in Manuel Kellerbauer, Marcus Klamert, and Jonathan Tomkin (eds), *The EU Treaties and Charter of Fundamental Rights: A Commentary*, 2nd Edition (Oxford Law Pro, 2024) 520.

[17] Roberto Senigaglia, *Minore età e contratto. Contributo alla teoria della capacità* (Giappichelli, 2020), 75; Id, 'L'identità personale del minore di età nel cyberspazio tra autodeterminazione e parental control system', in Nuove leggi civ. comm. (2024) 6, 1568. And formerly, see Francesco D. Busnelli, 'Immagini vecchi e nuove della tutela della salute del minore', in Andrea Bucelli (ed.), *Identità e salute del minore* (Pisa University Press, 2021) 3. More recently,

ISSN 2281-5147

Within this context, this contribution aims to provide a research agenda that considers two main challenges emerging from the policy perspective and from the academic perspective. On the one hand, the contribution aims at identifying the risks and problems that result from the restrictive approach adopted in some countries as regards the use of technology by minors: imposing a ban, or strict limitation, for minors in general, such as, for instance, in the Italian draft bill on Protection of minors in the digital environment,[18] is in clear contrast with the evolving capacity of discernment that minors acquire throughout the years. Such development is acknowledged by international treaties, such as the abovementioned UN CRC. How has the evolving capacity of discernment of minors been taken into consideration by the legislator so far? Is there a difference between the approach adopted at the European and national levels? Which are the criteria that the legislator has identified to show the development in the capacity of discernment?

On the other hand, the analysis of the academic literature on the protection of minors has so far approached this topic from a sectoral perspective, for instance, looking specifically at the specific rules applicable to protect minors' personal data,[19] or discussing the risks of cyberbullying,[20] etc. Few are the occasions in which the analysis is full-fledged and encompasses the overall activity of the minor in the digital realm.[21]

Daniela Marcello, *Circolazione dei dati del minore tra autonomia e controllo. Norme e prassi nel mercato digitale europeo* (ESI, 2023) 51.

[18] The draft bill in question was presented to the Chamber of Deputies and the Senate on 13 May 2024 and is currently under examination in committee. On its main contents and critical issues see Lavinia Vizzoni, *I "minori digitali" tra doveri educativi e tutele* (Bari, 95 ff.)

[19] With specific regard to the processing of a child's personal data, see Antonina Astone, *I dati personali dei minori in rete. Dall'Internet delle cose all'Internet delle persone* (Milano, 2019) *passim*, Daniela Marcello, *Circolazione dei dati del minore tra autonomia e controllo. Norme e prassi nel mercato digitale europeo* (Napoli, 2023) *passim*. See also I. A. Caggiano, 'Protecting Minors as Technologically Vulnerable Persons Through Data Protection: An Analysis on the Effectiveness of Law' (2022) *European Journal of Privacy Law & Technologies*.

[20] On the phenomenon of cyberbullying and strategies for its counteraction, see Carolina Perlingieri, *Profili civilistici dei social networks* (Napoli, 2014) 33 ff., Anna Carla Nazzaro, 'Cyberbullismo' in *Tecnol. e dir.*, 2020, n° 2, 465 ff., Ettore Battelli, 'Minori e social network: cyberbullismo e limiti della parental responsibility' in *Corr. giur.*, 2021, n° 10, 1269 ff., Francesca Zanovello, 'Prevenzione e contrasto del bullismo e del cyberbullismo. Tra novità e criticità della l. n. 70/24' in *Nuove leggi comm.*, 2024, n° 4, 826 ff. For an analysis of cyberbullying and online abuse from a criminological and legal perspective, proposing strategies to improve the digital environment see also F. Ahmed, F. Chaudhary, & S. Shahzad, *Cyberbullying and Online Harassment: A Criminological and Legal Perspective. Policy Research Journal*, (2025) 3(2) *Policy Research Journal* 52–59.

[21] See the attempt to outline a comprehensive legal framework for the digital minors by Vizzoni (n. 18) at 57 ff., and with specific regard to the position of parents, at 121 ff.

ISSN 2281-5147

The present contribution will instead adopt a different methodology in order to identify the several legal dimensions that the use of technology may trigger. This will allow not only to have a clear picture of the emerging risks that the minor will face, but also identify if and how the legislative interventions may coordinate and provide for synergies in order to solve or mitigate the risks, or vice versa may overlap and contradict potentially imposing additional burdens to manufactures of ICT that, indirectly, impact on the abilities of minors to fully exercise their rights.

According to the above-mentioned objectives, the role of minors in the digital environment will be investigated, focusing on the use of (online) video games. This will allow us to highlight the importance of such increasingly sophisticated applications and devices for the lives of minors, as well as the related risks, especially when AI-based tools and services are embedded. Special attention will be devoted to the balance between the legislative framework, still anchored to an age-based definition of minors, vis-à-vis the expanding autonomy of minors in the practices, able to show evolving capabilities. Special attention will be paid to the Italian legal system implementing and integrating with the EU legislation.

The results of this initial exploration, which will consider some practical cases too, will then provide some tentative interim conclusions in order to delineate a conceptual foundation for further scholarly inquiry and legislative consideration.

2. An underestimated risk: the use of video games by minors

Video games are a daily feature in minors' lives.[22] Many options are available for individual play, that engage the minor in a solitary challenge that can either require an Internet connection or not, but also multiplayer games, where the added value is provided by the possibility to play online with other users, which may or may not be known by the minor. Additionally, virtual reality games are also available, where simulated experiences require additional devices in order to enhance immersion in virtual reality.

[22] J. Gottfried and O. Sidoti, *Teens and Video Games Today* (Pew Research Centre, 2024), available at https://www.pewresearch.org/internet/2024/05/09/teens-and-video-games-today/

ISSN 2281-5147

The use of video games by minors is not only a means of entertainment, but also, depending on the type of interaction and features available, video games become a tool to engage with friends, connect with people with the same interests, experiment with personal identity, and enhance imagination.[23] The positive effects of video games do not exclude the risks that emerge from prolonged and assiduous use, affecting the ability to restrain and engage in social interactions,[24] or the risks of exposure to harmful or unlawful content.[25]

Such risks may be enhanced by the design choices of video game manufacturers. If, in the early days of video games, the business models adopted by manufacturers were based on direct micro-payments, through the availability of consoles in arcades, or on the purchase of the entire games on a physical support that allowed the gamers to play at home, nowadays manufacturers has widened their business models through advertisement and/or user-data driven models.[26] As a matter of fact, in order to generate profit, video games are designed in a way to enhance the participation and engagement; although, in principle, this is legitimate from the manufacturer's perspective, it becomes problematic as soon as the design choices lead to economic

[23] The importance of play in the development of minors is also recognised by the UN Committee on the Rights of the Child, 'General comment No. 14 2013 on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1) (2013), available at: https://www2.ohchr.org/English/bodies/crc/docs/GC/CRC_C_GC_14_ENG.pdf. The document affirms that "*Play and recreation are essential to the health and well-being of children and promote the development of creativity, imagination, self-confidence, self-efficacy, as well as physical, social, cognitive and emotional strength and skills. They contribute to all aspects of learning; they are a form of participation in everyday life and are of intrinsic value to the child, purely in terms of the enjoyment and pleasure they afford. [...] Play and recreation facilitate children's capacities to negotiate, regain emotional balance, resolve conflicts and make decisions.*" (at p. 4). See also Simone van der Hof et al., "Don't Gamble With Children's Rights"—How Behavioral Design Impacts the Right of Children to a Playful and Healthy Game Environment' *Front. Digit. Health* (2022) 4:822933, 5, where several examples of healthy games are presented.

[24] The psycho-social literature has long highlighted the substantial risks inherent in the use of video games by infants and adolescents, which may also result in addiction. Cfr. P. Ghezzo and G. M. Pirone, 'Videogiochi e minori, le questioni aperte', in Difesa sociale (2007) 1, 11; F. Romano and M. Conti, 'La dipendenza da videogiochi', in Psicologia di comunità (2014) 1, 71. More in general, on the anxiety that affects Gen-Z people, see Jonathan Haidt, *The Anxious Generation: How the Great Rewiring of Childhood Is Causing an Epidemic of Mental Illness* (Penguin Books Ltd, 2025) 20 ff. The author identifies two trends: overprotection in the real world and underprotection in the virtual world as the major reasons why children born after 1995 became the so-called anxious generation.

[25] See Van der Hof et al (n. 23) who distinguish among different types of harm: social harm (e.g., invasion of privacy, hate speech or cyberbullying), mental harm (e.g., sexual abuse or aggression from playing violent games), physical harm (lack of exercise, obesity, poor sleep), at 6.

[26] See Max V. Birk, Simone van der Hof, and Antonius J. van Rooij 'Behavioral Design in Video Games', ACM Games 2, 2, Article 16 (August 2024).

ISSN 2281-5147

exploitation of gamers, and in particular minors. Such an exploitation can emerge through different forms: unlawful personal data processing,[27] manipulation of economic choices, and a push towards harmful activities.[28]

These are not only theoretical risks, as a recent U.S. case has uncovered a real "Pandora's box". In 2022, Epic Games, the company that owns the famous video game Fortnite, was the recipient of a substantial fine following a settlement with the Federal Trade Commission.[29] The challenged conduct pertained to the collection of personal data of users under the age of thirteen[30] - such as their names, email addresses, identifiers used to track players' progress, purchases made, game settings, and friends lists – without the consent neither of the minor, nor of the parent. The investigation uncover that such activity was malicious as the company's data controller was perfectly aware of the data collection.

Additionally, the Federal Trade Commission imposed a sanction for the manipulation of minors put in place by Epic Games: the company in order to push underage users to purchase virtual goods used dark patterns, essentially carrying out unfair business practices, inducing underage players to make purchases that could take place without parental consent.[31]

Although the case was solved based on the U.S. legal framework, it highlights a set of problems that may also be translated into the European context. Which are the legal provisions that may be applicable to video games? The following sections will try to identify an initial overview of the problems taking the perspective of the minor user. Given that different (and overlapping) pieces of legislation apply, the following

[27] Not only is the creation of children profiles, without their (or their parents') consent is unlawful but it may also be exploited directly and indirectly: for instance, the video game manufacturer can send reminders to the email account of the player to rejoin the game; or can share or sell the personal data to third parties.

[28] Van der Hof at al. (n. 23) at 7.

[29] See Fulvio Sarzana di S. Ippolito, 'Fortnite viola la privacy di minori e li inganna: così la super sanzione da 520 milioni di dollari', in *cybersecurity360.it*, 20 dicembre 2022

[30] The thirteen-year limit arises from the U.S. *Children's Online Privacy Protection Act* (COPPA) of 1998. See Sasha Grandison, 'The Child Online Privacy Protection Act: The Relationship Between Constitutional Rights and The Protection of Children', in University of the District of Columbia Law Review (2011) 14(1) 209.

[31] See Tommaso Crepax and Jan Tobias Muehlberg, 'Upgrading the Protection of Children from Manipulative and Addictive Strategies in Online Games: Legal and Technical Solutions Beyond Privacy Regulation', in International Review of Information Ethics, 31(1), 1 ff. (2022): the authors analyse manipulative and addictive strategies in online games for children and proposes legal and technical solutions to enhance their protection.

ISSN 2281-5147

analysis will look upon the practical steps that the minor will follow when deciding to engage with video games: from the moment of the purchase or download of the video game, where national contractual rules apply; to the moment of play, where the recent European legislation on Digital Services Act and AI act apply, as well as the provisions on unfair commercial practices; and the possibility to communicate and engage with other players, triggering the application of the General Data Protection Regulation.

3. Buying and downloading options for video games

Although minors are the users par excellence of video games, their act of purchase or download of such video games raises some doubts about the validity of the relevant contract of sale/supply. In the Italian legal system, minors are considered to be structurally fragile, vulnerable people, who raise protective needs, which are centred essentially on the dogma of the minor's absolute incapacity to act, pursuant Article 2 of the Italian Civil Code. But of course, a static solution, where the minor, regardless of their age and effective capacity, is prevented from carrying out any legally relevant act, does not grasp the complexity of the present and the variety of dynamics in which the underage person is the leading actor.

Therefore, there are several instances that enhance the autonomy of the minor. Still, in the Italian civil code, there are so called "exceptions" to the incapacity rule. For example, under some conditions and over a certain age, a minor can work and recognise a child born out of wedlock. And the emancipated minor has a partial capacity. The real change is due to the already mentioned international charters of rights, especially the UN CRC, which adopted for the first time at the international level the well-known principle of the best interest of the child.[32] This principle, which has to drive every decision in which an underage person is involved, and the two other

[32] See Arianna Thiene, 'I diritti della personalità dei minori nello spazio virtuale', in Annali online did. e form. doc. (2017) 13/2017, 26.

[32] On the best interest of the child see, among others, Enrico Quadri, 'L'interesse del minore nel sistema della legge civile', in Famiglia e dir. (1999) 80, Leonardo Lenti, '«Best interests of the child» o «best interests of children»?', in Nuova giur. comm. (2010) 157, Vincenzo Scalisi, 'Il superiore interesse del minore, ovvero il fatto come diritto', in Rivista di diritto civile (2018) 405, Michele Sesta, 'La prospettiva paidocentrica quale fil rouge dell'attuale disciplina giuridica della famiglia', in Famiglia e dir. (2021), 763 ff., Elisabetta Lamarque, 'Pesare le parole. Il principio dei best interests of the child come principio del miglior interesse del minore', in Famiglia e dir. (2023), 365 ff.

ISSN 2281-5147

principles that derive from it, that is to say, the right of the minor to be heard,[33] and the capacity to discern,[34] build the new value triad of juvenile law.

The capacity to discern is presumed to have been acquired at the age of twelve, although its existence can be proved even before. The evaluation of discernment is an assessment of the single minor and requires a careful, concrete investigation, a specific analysis to be carried out case-by-case in order to prove the real maturity of the individual.[35] The reference to an age threshold other than the eighteenth year, which has always traditionally worked as a border between incapacity and capacity to act, is particularly meaningful. Another "dogma" seems this way to be shattered, the undifferentiated category of the minor, inclusive of individuals from zero to eighteen years,[36] expressive of what has been called a «uniform and flattened view of reality».[37] And yet, the doctrine's reflection has gone further. As already said on the side of personal acts, a wide area of autonomy has long been recognized for the minor. Some openings are now shown even toward a contractual capacity of the minor, recognizing the minor capable of discernment, the ability to perform even those acts that, although expression of the exercise of patrimonial rights, are functional to the implementation of personal rights, in accordance with the constitutional right to pursue the development of their personality.

[33] On the minors' right to be haerd, see Cesare Massimo Bianca, 'Il diritto del minore all'ascolto', in Nuove leggi civ. comm., 2013, 546 ff., Pietro Virgadamo, 'L'ascolto del minore in famiglia e nelle procedure che lo riguardano', in Dir. fam. pers. (2014) 1656 ff.

[34] See, also from a critical perspective, Giovanni De Cristofaro, 'Il diritto del minore capace di discernimento di esprimere le sue opinioni e il c.d. ascolto fra c.p.c. riformato, convenzioni internazionali e diritto UE', in Familia, (2023), 363.

[35] On the different capacities and abilitites of minors, see Grace Icenogle et al. 'Adolescents' cognitive capacity reaches adult levels prior to their psychosocial maturity: Evidence for a "maturity gap" in a multinational, cross-sectional sample', in Law and human behavior (2019) 73. In particular, the authors distinguish between "cold" cognition and "hot" cognition, the former refers to "mental processes (such as working memory or response inhibition) employed in situations calling for deliberation in the absence of high levels of emotion", where young adults perform comparably to older individuals; while the latter "involves mental processes in affectively charged situations where deliberation is unlikely or difficult", where instead the young adults show striking differences with older individuals.

[36] Francesco Donato Busnelli, 'Capacità ed incapacità di agire del minore', in *Persona e famiglia. Scritti di Francesco D. Busnelli*, Pisa, (Giappichelli, 2017), 216.

[37] The suggestive words are from Pietro Rescigno, 'Una ricerca sui minori', in Marcello De Cristofaro, Belvedere (eds) *L'autonomia dei minori tra famiglia e società*, (Giuffrè 1980), XI.

ISSN 2281-5147

The General Data Protection Regulation (GDPR)[38] highly contributed to consolidating a new role for minors. According to the GDPR framework, minors require special protection regarding the processing of their personal data, as they may not be fully aware of the risks, consequences, and security measures related to such processing. In particular, Article 8 establishes that the processing of minors' personal data is lawful only if the minor is at least sixteen years old; otherwise, parental or guardian consent is required. Member states can lower this threshold, not under thirteen years, as Italy has done, setting the age at fourteen.[39]

So, minors who are at least fourteen years old can provide their consent personally for the processing of data, in relation to information society services, such as registering on social networks. This recognition of the capacity to give consent is closely linked to the possibility of recognizing the minor's capacity to enter into contracts, related to the provision of such services.

In the video games field, it has to be highlighted, though, that first of all, there is no control, so the purchase of the video game is limited to those indicated as suitable for the age group to which the young user belongs.[40] Sometimes, in fact, users are anything but great minors capable of self-determination and of making autonomous and wise choices in function of the development of their personality, assuming that such a function can be configured regarding the purchase of such a product/service.

As regards giving consent to the processing of the user's personal data in the context of an information society service, often the minor data subject is well below the age limit of fourteen, relevant in the Italian legal system, as well as in other EU legal systems, to provide a valid, autonomous consent. Besides, the capacity to give personal consent is not necessarily symmetrical to the capacity to enter into the

[38] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[39] See C. Caglar, 'Children's Right to Privacy and Data Protection: Does the Article on Conditions Applicable to Child's Consent Under the GDPR Tackle the Challenges of the Digital Era or Create Further Confusion?' (2022) *European Journal of Privacy Law & Technologies*, where the author examines whether the provision on the conditions applicable to a child's consent under the GDPR addresses the challenges of the digital age or merely adds complexity, L Jialin, 'Reflection on Data Right Protection for Minors in the Digital Age' (2025) *Children and Youth Services Review*, in which the author proposes an expansion of the protection of minors' sensitive information, emphasising the responsibilities of data controllers.

[40] Giovanni Ziccardi, 'I minori online tra videogiochi e metaverso, in Ciberspazio e dir. (2023) 3, 325.

ISSN 2281-5147

connected contract. The main underlying issue is whether the contract of purchase/download of a video game can be considered as functional to the development of the minor's personality, in the digital environment. This specific answer actually depends greatly on the age of the minor and on the circumstances of the case.

Even if the underage user is above the fourteen years threshold, and the related contract is considered to contribute to the development of the minor, there are still several matters to solve: regarding the category of "older" users, first of all there is the need not to the exclude them from entertainment, but also to correctly identify the applicable rules, in order to protect them properly, in a multi-level perspective.

4. AI-based systems embedded in video games

The "digital issues" arising from the use of AI-based technologies, also with regard to minors, have recently been addressed by the so-called Artificial Intelligence Act,[41] having the objective of improving the functioning of the internal market and promoting the adoption of reliable and human-centred Artificial Intelligence, while ensuring a high level of protection of the fundamental rights enshrined in the Charter of Fundamental Rights.

The Regulation, adopting a risk base approach that now dominates the regulation of new technologies, is strongly focused on the categorisation of AI systems according to the risk they generate[42]. This ranges from unacceptable risk, which makes the use of the AI systems prohibited, to high risk, so that the AI systems defined as such are required to meet stringent requirements under the Regulations, including risk mitigation measures, to minimal risk, which does not require the fulfillment of any

[41] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).
[42] Giusella Finocchiaro, 'La regolazione dell'intelligenza artificiale', in Riv. trim dir. pubbl. (2022) 4, 1085, part. 1093 ff.

ISSN 2281-5147

obligations under the AI Act,[43] but providers are encouraged to voluntarily adopt additional codes of conduct.

There is also a limited, "specific transparency" risk: as clarified by the European Commission itself in a statement, the official communiqué of August 1st 2024, on the entry into force of the AI Act,[44] systems that fall under it, such as chatbots, must clearly inform users that they are interacting with a machine, while some content generated by AI must be explicitly labelled as such.

The category of the minimum risk of AI-based systems, when compared to their use by minors, arouses immediate perplexity, especially when the Commission, in its communiqué, refers to AI systems characterised by a minimum risk, by way of example, "video games that exploit AI". The risks of such a qualification may enhance the possibilities of exploitation against minors, as video games already exploit several algorithmic or AI-based tools. The (slightly) less worrisome ones relate to, for instance, the use of dynamic difficult adjustments,[45] which allow the possibility to reduce the difficulty of the game every time the player fails to reach the conclusion of the game. Although this technical adjustment aims at keeping the player interested in the game from the beginning to the end, it may also affect the player's ability to disengage, resulting in an infinite game duration. Other cases instead are more problematic, as for instance, the case of monetized matchmaking which is based on the possibility of linking players (with different levels of expertise) in such a way as to trigger the less expert player to purchase items or goods (internal to the game) used by the more expert one. It is clear that in this case, the AI-based system allocates the linked players based on players' data, including not only game-based data (such as skill level items used, amount of time dedicated to the game, etc.) but also personal data. Clearly, this type of application results in encouraging microtransactions rather than increasing the actual quality or playability of the game.[46]

[43] Note that apart from the general obligation regarding AI literacy envisaged in Art. 4, no additional requirements in the design, development and deployment of the AI system are applicable.

[44] See https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_it#:~:text=Il%201%C2%BA%20agosto%202024%20%C3%A8,'intelligenza%20artificiale%20nell'UE.

[45] See more at https://en.wikipedia.org/wiki/Dynamic_game_difficulty_balancing.

[46] Van Der Lot et al. (n. 23) at 10.

ISSN 2281-5147

5. Communication tools and platform regulation

Coming specifically to the potentially underestimated risks that the use of video games can produce on underage users, firstly, it is rare that video games do not avail themselves of solutions declined in terms of chatbots: the configuration of a "customer service" answering FAQs is sufficient for this purpose; and furthermore, in narrative video games, it is precisely a chatbot that appears by default, perhaps with human features, to answer the player's questions.

So, in this way, the video game *tout court* has already trespassed into the category of limited risk of the AI Act mentioned above, which nevertheless requires the fulfilment of mere transparency obligations, so that, as mentioned, the user is informed that he or she is interacting with a machine.

Along with chatbots, another feature available on video games is the possibility of interacting with other players through messaging systems or directly with conversations that take place through headsets equipped with a microphone. This feature is not without issues too: a first question emerging is the classification of the messaging service according to the legal framework. This qualification depends upon the level of integration within the game itself, in some cases it is fully integrated (and therefore operated by the same manufacturer of the video game), in other cases it may be provided by third party service providers, as exemplified by widely used platforms Discord.[47] This element is not without relevance, as the classification of the service may, in turn, bear on the legal nature of the video game itself. Indeed, one might contend that enabling interpersonal communication among players effectively transforms the video game into a digital platform, thereby rendering it subject to the regulatory obligations imposed by the Digital Services Act[48] and giving rise to a complex interplay of applicable normative frameworks.

[47] See Jeevan Joseph, Akshara Anilkumar, Treesa Thomas, Binny S, 'Discord: An all in one messaging application (Case Study)', International Journal of Engineering Technology and Management Sciences, Issue: 5 Volume No.6 August-September 2022).

[48] 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.

ISSN 2281-5147

From the application of the DSA would derive, among other things, the prohibition of profiling minors in art. 28(2) DSA,[49] which would be difficult to comply with where the video game records the conversations of minors and consequently proposes targeted advertising to them, intercepting their consumption needs, as occurred precisely in the aforementioned Fortnite case.

The attention is bound to return to the protection of personal data collected in the context of conversations, which could be recorded: it is no coincidence that in 2020, Sony announced that the PlayStation 5, to be released shortly, would record conversations between players for the purposes of moderating them within gaming groups.[50] Conversations, written or audio, could in fact be recorded or saved by many video games, without them being provided with complete information, which clarifies, for example, the recording methods and retention times, as well as specific, compliant with the more stringent requirements already provided for by the GDPR.

Moreover, the game-based advertising aimed at minors could further integrate an unfair business practice; for that reason alone, it is prohibited and sanctioned. This has also been confirmed by the recent intervention of the European Commission, which has announced an action aimed at probing alleged unfair practices in the video game "Star Stable Online", targeting in-game purchases aimed at children.[51] Star Stable is a children's video game where players explore an online world by riding horses and competing with friends in obstacle races. However, players who spend real money gain advantages within the game. To acquire items, players must exchange real money for in-game currency, known as "star coins".

Therefore, the Commission, in collaboration with the Consumer Protection Cooperation Network, has requested information from the Swedish game developer of Star Stable to understand its commercial practices. As highlighted in the EC statement, the upcoming Digital Fairness Act may include stricter rules on virtual

[49] Although the formulation of this provision is not that clear. See Guido Scorza, 'Digital services act. Le luci e le poche ma gravi ombre delle nuove regole UE', in *agendadigitale.it*, April 28 2022.

[50] See the news released on October 17, 2020 on the website https://gaming.hwupgrade.it/, and the official statement, dated October 16, 2020, by Catherine Jensen, President of the "Global Consumer Experience" Division https://blog.playstation.com/2020/10/16/details-on-new-voice-chat-functionality-coming-to-ps5/, which does not deny the activation of the functionality in question and, indeed, even highlights the technical impossibility of deactivating it, while declaring it generically compliant with the regulations on privacy.

[51] See at https://ec.europa.eu/commission/presscorner/detail/en/ip_25_831.

ISSN 2281-5147

currency transparency and fairness, and a crucial goal is "to ensure a safe online environment for consumers, particularly children, so they can enjoy gaming without facing unfair practices".[52]

And last but not least, there are serious dangers of grooming for the minor when interfacing with other users, even adults, who may come into possession of important information relating to the minor, as well as the risks of becoming a victim of conduct that can be classified as cyberbullying.

In this regard, the EU Directive 2011/93 on combating the sexual abuse and sexual exploitation of children and child pornography[53] should therefore come into play, also in combination, in the Italian legal system, with Law No. 71 of 2017, aimed at preventing and combating the phenomenon of cyberbullying specifically, as well as the recent Law No. 70/2024, which also contains provisions aimed at preventing and combating the phenomena of both bullying and cyberbullying.

6. Tentative conclusions

In seeking to articulate some necessarily provisional conclusions, it must be acknowledged that, in the context of minor users of video games, the constellation of legal issues emerging is both multifaceted and conceptually intricate. The foundational premise is that minors constitute a structurally vulnerable category of users vis-à-vis smart technologies that may use AI-based applications, including but not limited to interactive entertainment systems. The spectrum of protective measures that may be envisaged is inherently differentiated and stratified.

At the outset, it should be observed that the existing regulatory landscape is characterised by a high degree of normative fragmentation. As the previous analysis has shown, the applicable framework at the European level is both complex and polycentric: multiple instruments converge, at times partially overlapping, thereby generating interpretative uncertainty and a consequent deficit in legal certainty.

[52] See the news published on March 21st 2025: https://www.euronews.com/next/2025/03/21/european-commission-targets-in-game-currency-in-childrens-video-games.

[53] This Directive should be overcome soon, considered the recent Proposal for a Directive on combating the sexual abuse and sexual exploitation of children and child sexual abuse material and replacing Council Framework Decision 2004/68/JHA.

ISSN 2281-5147

Although some specificities emerge from the national legislation, they cannot mitigate the complexity nor, obviously, detach from the European legislation.

What emerges clearly is the limited sensitivity of the European legislator to the specificities of the phenomenon. This does not mean that no rules are provided as regards the protection of minors, but rather that they still adopt a 'flattened view' of the minor. In particular, neither the AI Act nor the Digital Services Act takes into account the evolving capacity of a minor in relation to his or her degree of maturity. Some positive hints come from another set of interventions: the GDPR, as well as the Italian national legislation—albeit through interpretative approaches that are at times complex—allows for an assessment and recognition of a minor's capacity prior to reaching the age of majority. In particular, the GDPR proves instrumental from a contractual perspective, as it permits recognition of the ability to provide consent and, consequently, to enter into contractual obligations in the field of digital services, even for individuals who have attained the age of fourteen.

The true lever that enables the attribution of legal capacity to minors is therefore the notion of discernment, which is already firmly established as a principle at the international level. Yet, it must be observed that the capacity for discernment is conceptually distinct from the capacity to act. The former, in fact, is a principle whose primary foundation lies in the minor's freedom of expression, and which finds its principal application within the realm of public law, notably in procedural matters — as an expression of the right to be heard — and, more broadly, in all matters involving minors. What is required, however, is a rearticulation of the notion of discernment, primarily by applying it to intra-family relationships, wherein the minor should be able to express personal inclinations and aspirations, which ought to guide his or her upbringing.

Furthermore, the capacity for discernment constitutes a general principle that requires implementation through indicators and criteria laid down by the legislature. In this regard, some practical tools already available may become effective: the so-called Pan-European Game Information (PEGI) standard may serve as useful benchmark for industry operators willing to acknowledge varying levels of maturity and discernment among the minor user base, and to introduce corresponding distinctions regarding the suitability of video games. After all, the fundamental freedom of expression is also manifested in the recreational sphere, particularly through the use of video games.

ISSN 2281-5147

The PEGI system is, indeed, a method of rating video games based on age. Available guidelines classify video games into five age categories (+3, +7, +12, +16, +18) and eight content descriptors (bad language, discrimination, drugs, fear/horror, gambling, sex/nudity, violence, in-game purchases), in order to determine the games most suitable for minors. However, as noted, such indications often go largely unnoticed, resulting in the risk that minors may play video games unsuitable for their age, both in terms of content and visual elements.[54]

In parallel, recourse to soft law instruments, such as codes of conduct, has been explicitly endorsed at the European level as a regulatory modality of preference in this sector. This is exemplified by the Resolution adopted by the European Parliament on 18 January 2023, entitled "Consumer protection in online video games – a European Single Market approach", which advocates for the elaboration of harmonised governance strategies capable of reconciling market integration with the imperative of child protection.

Moreover, notwithstanding the aforementioned lack of attention to the evolving maturity of minors within the AI Act, a crucial element can nonetheless be discerned in the notion of "AI literacy" as enshrined in Article 4 thereof. According to this provision, providers and deployers of AI systems shall take measures to ensure not only a sufficient level of AI literacy among their staff and other persons involved in the operation and use of AI systems on their behalf, but also to consider the persons or groups of persons on whom the AI systems are to be used. Consequently, providers will need to specifically assess and, where appropriate, provide training tailored to the audience on which their system is intended to have an impact. Particular attention should be given to systems that are, or could be, intended for use by minors. In such cases, the literacy requirement should be significantly elevated, due to the increased risks associated with the inherent vulnerability of the individuals concerned.

If rigorously implemented, this normative apparatus could operate as a catalyst for the epistemic empowerment of minors in their interaction with technological ecosystems, thereby attenuating informational asymmetries and mitigating the

[54] See T. Casadei and C. Coniglione, *Patti educativi digitali: come indirizzare i ragazzi a un uso consapevole dei device*, in *www.agendadigitale.it*, November 13th 2023.

ISSN 2281-5147

manipulative potential of dark patterns. The correlative risk, however, concerns the distributive implications of such regulatory prescriptions, which risk engendering disproportionate compliance burdens for economic operators within the interactive entertainment industry.

Against this backdrop, an ancillary — yet significant — trajectory emerges: the systematic investment in training and awareness-raising initiatives, conceived not merely as auxiliary measures but as constitutive components of a governance architecture predicated upon inclusion rather than exclusion.

Such an approach would resonate with the foundational principle of proportionality, ensuring that minors — particularly those approaching the threshold of majority — are not unjustifiably marginalized from the digital entertainment sphere.

ISSN 2281-5147

ISSN 2281-5147

A STORY *OF* AND *FOR* CHILDREN: THE LIFECYCLE LOOP OF CHILD RIGHTS-BASED AI

Sara Tibidò, Nadia Spatari, Sara Lilli e Maria Vittoria Zucca*

Abstract

This paper traces the lifecycle loop of child rights-based AI - from the initial phase of design through development and deployment - while mapping the ethical and regulatory landscape surrounding AI technologies designed for, accessed by, or impacting children. Building on established frameworks, the study advocates for the implementation of regulatory sandboxes and risk assessment measures to protect children's rights and interests against threats and emerging cyber risks. This research argues for the essential integration of a child rights-based approach at every stage and phase of an AI system's lifecycle, asserting that this leads to the development and deployment of more secure, child-centered systems.

Table of Contents

* Sara Tibidò, Ph.D. Student in *Cybersecurity*, University of Bari "Aldo Moro" and IMT School for Advanced Studies Lucca, ORCID: 0009-0004-0646-0558.
Nadia Spatari, Ph.D. Student in *Cybersecurity*, National Inter University Consortium for Informatics (CINI) and IMT School for Advanced Studies Lucca. ORCID: 0009-0009-4935-7135.
Sara Lilli, Ph.D. Student in *Cybersecurity*, Sant'Anna School of Advanced Studies in Pisa and IMT School for Advanced Studies Lucca. ORCID: 0009-0000-2796-3067.
Maria Vittoria Zucca, Ph.D. Student in *Cybersecurity*, Sant'Anna School of Advanced Studies in Pisa and IMT School for Advanced Studies Lucca, ORCID: 0009-0004-0049-9611.
Double blind peer-reviewed contribution.

ISSN 2281-5147

Keywords

Artificial Intelligence - Children's rights - Children-centred AI - Digital Safety - Child Impact Assessment - Regulatory Sandbox

1. Starting the lifecycle loop of child rights-based AI

Once upon a time, there was a doll named Cayla[1], designed to be a friendly playmate for children. But behind her smiling face and sweet voice, she hides the potential of *listening* - and *sharing*. What was meant to be an AI embedded toy became a warning story of how innovation can overlook safety, privacy, and the fundamental rights of

[1]See the articles from BBC, 'German parents told to destroy Cayla dolls over hacking fears', (*BBC News* , 17 February 2017) https://www.bbc.com/news/world-europe-39002142 accessed 06 July 2025; and World Economic Forum (WEF), 'Generation AI: What happens when your child's friend is an AI toy that talks back?' (*World Economic Forum*, 22 May 2018) https://www.weforum.org/stories/2018/05/generation-ai-what-happens-when-your-childs-invisible-friend-is-an-ai-toy-that-talks-back/ accessed 06 July 2025; other relevant cases should also be considered, such as the chatbots Wysa and Woebot, for which reference can be made to the following article: Geoff White, 'Child advice chatbots fail to spot sexual abuse' *BBC* (London, 11 December 2018),https://www.bbc.com/news/technology-46507900 accessed 06 July 2025; and Karen Brown, 'Something Bothering You? Tell It to Woebot. When your therapist is a bot, you can reach it at 2 a.m. But will it really understand your problems?', *The New York Times* (New York, 01 June 2021), https://www.nytimes.com/2021/06/01/health/artificial-intelligence-therapy-woebot.html accessed 06 July 2025.

ISSN 2281-5147

the youngest users. Cayla's conversations have indeed been found vulnerable to hacking, allowing strangers to listen and communicate directly to children.

While significant steps have been undertaken to improve safety and protection from similar situations (for instance, the adoption of *privacy*- and *security*-by-design approaches) different international organizations and associations, like UNICEF'[2] and the Institute of Electrical and Electronics Engineers - IEEE[3], and international non-governmental organizations (NGOs), such as the 5Rights foundation[4'5], are calling for stronger, child-specific measures. These measures underscore the importance of integrating children's rights from the outset of the innovation process, ensuring their safety, protection, and participation.

While children should not be excluded from the digital world, as also stated by the UN General Comment No.25[6], they should be protected by the risks (both *old* and *new*) they may face when using digital products or services. To move towards a welcoming, as well as more safe and secure digital ecosystem for children, it is crucial to integrate children's rights - along with safety and security measures - from the very beginning of the innovation process. This approach is particularly important when developing AI systems[7]. Indeed, the interaction between children and AI systems is

[2] UNICEF - V. Dignum, M.Penagos, K.Pigmans and S.Vosloo, 'Policy Guidance on AI for Children (Version 2.0)' (November 2021). https://www.unicef.org/innocenti/reports/policy-guidance-ai-children accessed 12 May 2025.

[3] IEEE Std 2089-2021, 'IEEE Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children' (vol., no., pp.1-54, 30 Nov. 2021). DOI: https://doi.org/10.1109/IEEESTD.2021.9627644.

[4] Digital Futures Commission and and 5Rights Foundation, 'Child Rights by Design' (11 March 2023). https://5rightsfoundation.com/resource/child-rights-by-design/ accessed 04 July .2025.

[5] 5Rights Foundation, 'Children & AI Design Code' (March 2025). https://5rightsfoundation.com/children-and-ai-code-of-conduct/ accessed 04 July 2025.

[6] UN Committee on the Rights of the Child, 'General comment No. 25 (2021) on children's rights in relation to the digital environment' (02 March 2021) CRC/C/GC/25.

[7] Acknowledging that there is no internationally shared definition, for the purpose of this paper, we intend an "AI system" as defined by Article 3(1) of the EU AI Act and as further explained by the European Commission (February 2025) in its guidelines on AI systems definition (available online

ISSN 2281-5147

complex and not limited only to those systems designed *for* children to be the main end users (*e.g.*: AI-enabled toys or systems used in the EdTech field), but also to those systems not meant for them but with which they *interact* in everyday lives contexts (*e.g.:* smart home assistant or recommender systems in social media and streaming platforms), and systems that can directly or indirectly *impact* them (*e.g.:* AI systems used to support decision process of social workers dealing with case of child maltreatment[8])[9]. Attention should also be paid to factors that can influence AI's impact on children, such as socioeconomics, geographic and cultural context and norms, as well as other elements like children's developmental stages related to their physical, cognitive, emotional and psychological capacities.[10]

Accordingly, this story begins far back in the innovation process, from the discovery phase through the design and development phases, and it is grounded in the children's rights as defined by the UN Convention on the Rights of the Child (UNCRC). Indeed, since its adoption by the UN General Assembly in 1989 and its entry into force in September 1990, the UNCRC has become the world's most widely ratified human rights treaty[11]. With its ratification, States are legally bound to respect, protect, and fulfill the rights as outlined in the Convention[12]. Therefore, although the digital environment and new technologies may pose new challenges, the Convention (guided in its implementation in relation to the digital environment by the UN General Comment No.25) can still be considered an authoritative source on children's rights.

---

at: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application - accessed 14 March 2025).

[8] See, for example, A. Kawakami and V. Sivaraman, and L. Stapleton, and H.F. Cheng, and A. Perer, and Z.S. Wu, and H. Zhu, and K.Holstein, "'Why Do I Care What's Similar?" Probing Challenges in AI-Assisted Child Welfare Decision-Making through Worker-AI Interface Design Concepts' (ACM Designing Interactive Systems Conference, online, 13-17 June 2022).

[9] UNICEF - V. Dignum, M.Penagos, K.Pigmans and S.Vosloo (November 2021).

[10] *Ibidem*.

[11] UNICEF, 'How the Convention on the Rights of the Child works' https://www.unicef.org/child-rights-convention/how-convention-works accessed 12 May 2025.

[12] *Ibidem*.

ISSN 2281-5147

In 2011, the UN Human Rights Council endorsed the "Guided Principles on Business and Human Rights" (UNGPs)[13], implementing the 2008's UN "Protect, Respect and Remedy" framework for business and human rights and recognizing business's responsibility to respect also those rights as enshrined in the UNCRC[14]. The UNGPs '*are applied to the digital context through the UN Human Rights B-Tech Project*'[15] (*e.g.*: the briefing, conducted together with UNICEF and published in 2024, on "Taking a Child Rights-Based Approach to Implementing the UNGPs in the Digital Environment" unpacks core headlines on the implementation of UN principles with a child rights perspective[16]). A year later, in 2012, UNICEF, the UN Global Compact and Save the Children developed the "Children's Rights and Business Principles", a range of actions companies can undertake in different contexts to respect and support children's rights[17]. Although those Principles do not constitute a legally binding document, they are instruments of soft law that have been '*incorporated or referenced in legislation, industry codes of conduct, and market-entry requirements in various sectors of the economy, including the digital sector*'[18].

Unlike such voluntary approaches, the European Union has imposed some legal obligations to online intermediaries and platforms. In particular, first in 2018 with the "Audiovisual Media Services Directive" (AVMSD), coordinating national legislations and setting out responsibilities for media service providers (*e.g.:* protection of users, children in particular, from certain kinds of content or programs and establishment

[13] UN, 'Guided Principles on Business and Human Rights' (01 January 2012) 978-92-1-154201-1.

[14] *Ibidem*.

[15] OECD, 'Shaping a Rights-Oriented Digital Transformation' (28 June 2024), No. 368, OECD Digital Economy Papers (citing). https://www.oecd.org/en/publications/shaping-a-rights-oriented-digital-transformation_86ee84e2-en.html accessed 12 May 2025.

[16] UNICEF and UN Human Rights, 'Taking a Child Rights-Based Approach to Implementing the UNGPs in the Digital Environment' (November 2024) https://www.unicef.org/childrightsandbusiness/reports/b-tech-contribution accessed 05 July 2025.

[17] UNICEF, the UN Global Compact and Save the Children, 'Children's Rights and Business Principles' (2012) https://www.unicef.org/documents/childrens-rights-and-business-principles accessed 12 May 2025.

[18] OECD (28 June 2024), citing.

ISSN 2281-5147

of age verification systems in video-sharing platforms)[19], and then in 2022, with the "Digital Services Act" (DSA). The DSA, which refers to international standards (including the UNGPs)[20] and aims at regulating online platforms and intermediaries (to be specific: very large online platforms and search engine, online platforms, host services and intermediary services), contains some child-specific provisions (*e.g.*: Article 14 on comprehensible child-friendly explanations of conditions and terms of use, Article 28 on appropriate and proportionate measures to protect children's safety, security and privacy, and Articles 34 and 35 on mandatory annual fundamental rights risks' assessments and mitigation measures).[21]

Designing with children's rights in mind is no simple task, but retrofitting a product to comply with these rights after development can be both difficult and costly.[22] Accordingly, this paper proposes a children's rights-based approach to the entire AI system lifecycle, emphasizing the integration of children's rights, needs, and perspectives - alongside safety, security, and stakeholders inputs - at every phase. The aim is to ensure that systems are well-designed from the outset to be compliant with children's rights standards and obligations, thereby reducing the need for substantial post-deployment corrections. Therefore, the following sections will describe a story of innovation that begin from (i) the legal, policy and technical frameworks shaping the *design* and *development* phases of an AI system for/impacting/accessed by children, passing through (ii) the phases *of testing* and *validation* with the use of regulatory sandboxes, to (iii) the phases of *deployment* and *post-deployment*[23].

---

[19] *Ibidem*.

[20] *Ibidem*.

[21] OECD, 'Towards digital safety by design for children' (19 June 2024), No. 363, OECD Digital Economy Papers. https://www.oecd.org/en/publications/towards-digital-safety-by-design-for-children_c167b650-en.html accessed 05 July 2025.

[22] Digital Futures Commission and 5Rights (11 March 2023).

[23] For the division of the phases constituting the AI system lifecycle, we recall the work of D. De Silva and D. Alahakoon, 'An Artificial Intelligence Life Cycle: From Conception to Production' (2022) 3(6) Patterns, https://doi.org/10.1016/j.patter.2022.100489 accessed 12 May 2025. Indeed, the Authors consider an AI system's life cycle made of three main phases: "*design*", "*develop*" and "*deploy*", each of them made of different "*stages*". While the Authors do not consider a separate phase for testing and validation, in the "*deploy*" phase it is considered a "*post-deploy*" stage (stage no.16).

ISSN 2281-5147

2. *Design* and *develop*: towards clear and practical child rights-based guidelines for practitioners

State have the duty, under international human rights law, to protect people in their jurisdiction or/and their territory from human rights abuses, and corporate responsibility to respect human rights exists '*regardless of their size, sector, location, ownership and structure*'[24]. Therefore, States and businesses have different but complementary responsibilities[25]. Accordingly, since the exercise and protection of human rights can be affected by how '*digital technologies are designed, developed and deployed*', it is important to embed human rights in all the phases of an innovation process[26]. However, providing all stakeholders with clear, technically applicable and cross-cutting guidelines is challenging.

Before rights-specific considerations, ethical AI-related challenges have been a central topic of discussion among policy makers, professionals and academics. Indeed, ethical principles and guidelines have been found difficult to be integrated into the engineering process that power AI development: there is a critical gap between these principles, available guidelines and the realities of the engineering practice[27]. Moreover, the accountability gap, in terms of clarity about who should be ought accountable '*for the outcomes of technology use, to whom, and how*'[28], presents a major challenge for engineers (*e.g.:* hierarchies of power in the workplace that may limit their

[24] UN, 'Guided Principles on Business and Human Rights' (01 January 2012), citing.

[25] *Ibidem.*

[26] OECD (28 June 2024), citing.

[27] IEEE SA, 'Report: Addressing Ethical Dilemmas in AI: Listening to Engineers Report' (2021) https://standards.ieee.org/initiatives/autonomous-intelligence-systems/ethical-dilemmas-ai-report/ accessed 05 July 2025.

[28] *Ibidem*, citing.

ISSN 2281-5147

technical and organizational choices; absence of independent infrastructures to turn to in case of ethical concerns or to report cases of non-compliance)[29].

While various ethical principles have been proposed in relation to the rights of the child and AI systems, their effective implementations and practical applications are still mainly unexplored[30]. Children are different among them and from adults, accordingly AI principles concerning children should not be considered nor treated as a subcategory of other guidelines[31]. Accordingly, Wang *et al.* identify four main '*challenges in translating ethical AI principles into practice for children*'[32]:

1. '*Lack of consideration of the developmental aspect of childhood*'[33]: the vast number of technologies and their various applications make it difficult to provide consistent professional codes and norms for AI applications. Incorporating children introduces a new layer of complexity to this scenario. Their unique needs, diverse age ranges, development stages, backgrounds, physical and psychological traits necessitate special attention;

2. '*Lack of consideration of the role of guardians in childhood*'[34]: parent(s) or legal guardian(s) bear the ethical and legal primary responsibility for the upbringing and development of the child (Article 18 UNCRC) and for the children's provision of appropriate direction and guidance in the exercise of their rights (Article 5 UNCRC). Therefore, the role of parent(s) and legal guardian(s) must be considered and examined, but without falling in the traditional assumption that they possess superior expertise or skills to orient children in the digital landscape;

[29] *Ibidem*.

[30] G.Wang, J. Zhao, M.Van Kleek & N.hadbolt, 'Challenges and opportunities in translating ethical AI principles into practice for children' (2024) Nature Machine Intelligence 6, 265–270 https://doi.org/10.1038/s42256-024-00805-x accessed 04 July 2025.

[31] *Ibidem*.

[32] *Ibidem*, citing.

[33] *Ibidem*, citing.

[34] *Ibidem*, citing.

ISSN 2281-5147

3. '*Lack of child-centred evaluations considering children's best interests and rights*'[35]: relying solely on quantitative metrics and technical evaluation, while important, can present challenges. Translating ethical AI principles into practice for children requires a more balanced approach between both empirical variables and quantitative measurements, and, in general, a paradigm shift towards a more human-centred approach;

4. '*Lack of a coordinated, cross-sector and cross-disciplinary approach*'[36]: experts from other domains, dealing with analogous issues, often have different vocabularies and methodologies. One of the main challenges lies in their adaptability across different AI principles. Cross-sector and cross-disciplinary collaboration is essential to harmonize and encourage knowledge transfer while avoiding duplicate efforts.[37]

These challenges add other layers of difficulty in integrating children's rights in the design and development of a product or service. Smart toys like Cayla's doll, should not only be secure- and privacy-by-design, but should also *e.g.* take into account children developing language skills, by adopting a child friendly language in accordance of the maturity of the child, while also considering a system of blocking access to content children should not access without adults' supervision. Accordingly the difficulty is not just on how to make the system embedded in the toy technically robust and resilient, but it also concerns dealing with developmental theories, adaptability to different situations (*e.g.:* Is the system capable of adapting content and language according to the child's specificity? and how to make the system able to do that while following the principle of data minimization?), and definitions of concept like "appropriateness" (*e.g.:* What may be considered appropriate for a child of a certain age, maturity and background could not be necessarily considered appropriate for and by another child).

Given all these challenges, engineers and practitioners working on the design and development of AI systems for, accessed by or impacting children, are required to

[35] *Ibidem*, citing.

[36] *Ibidem*, citing.

[37] *Ibidem*.

ISSN 2281-5147

deal with more than technical problems and solutions. This is for those topics that are indeed '*socio-technical*'[38], meaning that '*social and technical aspects are interwoven in such a way that studying one without due consideration of the other makes for an incomplete investigation and understanding*'[39]. To guide practitioners in diving this scenario, some references are made to existing contributions from academia, industry, international organizations/associations and NGOs.

However, academic contributions on how to design, develop and deploy AI systems compliant with related existing standards and obligations are still few, and mainly summarized as "design implications" at the end of a paper. While literature reviews can offer a valid overview of a topic, few are the works[40] investigating children's rights coverage and inclusion in engineering and computer science' works, and even less are works trying to summarize all these "design implications" in one single and easy to use document. This sum up could be interesting and possibly useful in real life situations, since coming from in-the-field studies, and a service- or product-specific framework can be valuable to achieve precise applicable guidelines.

Nevertheless, industry-partnership projects and international organizations and associations have been mainly focusing on a broader approach, advocating for responsible innovation for children well- being (*e.g.:* LEGO and UNICEF[41]), a child-centered approach to AI system (*e.g.:* UNICEF[42]) and age appropriate services (*e.g.:*

[38] Rashina Hoda., *Qualitative Research with Socio-Technical Grounded Theory. A practical guide to qualitative data analysis and theory development in the digital world* (Springer Charm, 2024), https://doi.org/10.1007/978-3-031-60533-8 citing.

[39] *Ibidem*, citing.

[40] See, for example, G.Wang, J.Zhao, M.Van Kleek, and N.Shadbolt, 'Informing Age-Appropriate AI: Examining Principles and Practices of AI for Children' (CHI - Conference on Human Factors in Computing Systems, New Orleans, LA, April 30 – May 5 2022).

[41] UNICEF and LEGO, 'The Responsible Innovation in Technology for Children (RITEC) Project'. See UNICEF's webpage 'Responsible Innovation in Technology for Children. Project | Digital technology, play and child well-being' (*UNICEF*) https://www.unicef.org/innocenti/projects/responsible-innovation-technology-children accessed 06 July 2025.

[42] UNICEF - V. Dignum, M.Penagos, K.Pigmans and S.Vosloo (November 2021).

ISSN 2281-5147

IEEE[43]). These contributions are one of the most cited when it comes to children and AI.

Contributions coming from (or in collaboration with) businesses and industry are important for their ground on real life scenarios and interests, bridging the gap between academic research and industry actual needs. Integrating a children's rights approach and design for well-being into business strategies can have positive outcomes for both children (their rights, needs and desire with better products) and brands (boosting brand reputation and values, by differentiating themselves from their competitors and within their customers, and attracting possible investors)[44].

The "Responsible Innovation in Technology for Children" (RITEC) project is a collaboration between UNICEF and The LEGO Group, funded by The LEGO Foundation, aiming at investigating how the design of children's digital experiences affects their well-being, and provides guidance on design choices that can promote positive outcomes for children's well-being[45]. From the RITEC project a framework (the final "RITEC-8", updated and published in 2024) and a design toolbox (the "RITEC Design Toolbox") have been developed to provide an '*easy-to-use guidance for designers of digital play*'[46] by including a list of relevant features and examples[47].

The framework developed in the context of this project is called RITEC-8[48] because is grounded in 8 pillars: (i) autonomy (allow children to be in control and make decisions that matter for them and their play); (ii) competence (considering

[43] IEEE, Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children, 2021. DOI: https://doi.org/10.1109/IEEESTD.2021.9627644.

[44] *Ibidem*.

[45] UNICEF, The Business Case for Designing for Children's Well-Being in Digital Play Summary for Executives, 2024. https://www.unicef.org/childrightsandbusiness/reports/business-case-designing-childrens-well-being-digital-play accessed 06 July 2025.

[46] *Ibidem*, citing.

[47] *Ibidem*.

[48] UNICEF, Digital technology, play and child well-being. Responsible innovation in technology for children, 2024. https://www.unicef.org/innocenti/reports/responsible-innovation-technology-children accessed 06 July 2025.

ISSN 2281-5147

meaningful rewards for progress and allowing children to adjust and improve); (iii) emotions (experience positive as well as more challenging emotions); (iv) relationships (taking into account children's different needs and characteristics, allow them to make new friends and socialize while competing, creating, and/or collaborating with others); (v) creativity (encourage children's curiosity and imagination to invent and experiment); (vi) identities (while playing, allow children to explore and express facets of themselves and of others); (vii) diversity, equity & inclusion (experience intended for different children and needs); and (viii) safety and security (children feel and are kept safe while playing)[49]. The framework is also accompanied by a design toolbox (RDT) with the aim of providing design professionals in the online gaming industry (product, visual, UX, research, but also management levels, and safety professionals) with practical tools for incorporating the RITEC-8 for children's well-being into their design process[50].

UNICEF, before the RITEC Project, has already been focusing on AI systems in its "Policy Guidance on AI for Children"[51]. The document provides nine requirements for child-centered AI, and furnishes a set of '*complementary online resources*' and '*practical implementation tools*'[52]. The guidance is addressed to different stakeholders, from development teams to policymakers, and, while this is important, finding a common both understandable and practical language for all may be challenging. The risk is too high-level guidance, resulting difficult to fully implement into the actual work's duties (*e.g.*: The "transparency" principle does not specify how to explain AI decisions to a child of a certain age or background over a child of another age or background).

Meanwhile, the IEEE, as technical professional organization, elaborated the "Standard for an Age Appropriate Digital Services Framework Based on the 5Rights

[49] *Ibidem*.

[50]UNICEF, 'RITEC Design Toolbox. Designing for children's well-being in digital play' https://www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/online-gaming/ritec-design-toolbox accessed 06 July 2025.

[51] UNICEF - V. Dignum, M.Penagos, K.Pigmans and S.Vosloo (November 2021).

[52] *Ibidem,* citing.

ISSN 2281-5147

Principles for Children"[53] (IEEE 2089-2021)[54]. The IEEE 2089-2021 is practical in its formulation, being developed to be used in '*software engineering and digital services organizations*'[55], including but not limited to those '*providing services and products that engage with children or are likely to be accessed by or engage with children*'[56]. Although its technical nature, the document is informed by the UNCRC and the UN General Comment No.25, and it is based on the principle of the "*best interests*"[57] of the child[58]. The Document is an important attempt to combine a more technical approach with existing policies and regulations on the subject.

NGOs have also attempted '*bridging high-level principles and practical challenges*'[59] by defining what innovators need to know to realise children's rights in their product or service[60]. In 2023, the "5 Rights Foundation" (within the "Digital Future Commission" project) released the "Child Rights By Design": a guidance aiming to provide clear and practical indications to those figures involved in the process of

[53] IEEE Std 2089-2021(2021).

[54] In 2023, the IEEE 2089-2021 has been recognized to serve as the foundation for an *European Committee for Standardization (CEN)/European Committee for Electrotechnical Standardization (CENELEC)* Workshop Agreement (CWA 18016), helping to serve various EU regulations and policies, such as the the DSA and the 'European strategy for a Better Internet for Kids (BIK+)' (see: IEEE SA, 'IEEE 2089™ Provides Foundation for European Reference Document for Children's Protection & Well-being Online' (2023). https://standards.ieee.org/news/ieee-2089-european-reference-document/ accessed 13 May 2025).

[55] IEEE Std 2089-2021 (2021), citing.

[56] *Ibidem,* citing;

[57]The "best interest" principle refers to Article. 3 UNCRC and, according to S. Livingstone et al. (S. Livingstone, N. Cantwell, D.Özkul, G. Shekhawat and B. Kidron, 'The best interests of the child in the digital environment' (March 2024) https://www.digital-futures-for-children.net/our-work/best-interests accessed 14 May 2025), it implies that, when children's rights seem to be in tension or when other parties' interests (such as those of companies or organizations) may conflict with them, to identify "*which rights are to be given precedence*", an independent procedure of "*best interests' determination*" should be designed to avoid "*provide legitimation for whichever right a company may favour*".

[58] IEEE Std 2089-2021 (2021).

[59] Digital Futures Commission and 5Rights (11 March 2023).

[60]*Ibidem*.

ISSN 2281-5147

creation, design, development and deployment of a digital product or services likely to be used by or impacting on children[61]. Grounded on the UNCRC, the guidance calls for a "*by-design*" approach[62], that would mean including children's rights considerations in every phase of an AI system's lifecycle. By collecting inputs from innovators, practitioners, and children, the guide is structured around 11 high-level principles[63] and align with the main crucial phases of an innovation process[64]. Given the peculiar opportunities and challenges AI systems pose, the 5Rights Foundation also published the "Children and AI Design Code. A protocol for the development and use of AI systems that impact children"[65](2025). The Code is composed of distinct stages and developed so as to be applicable in each phase of an AI system's lifecycle[66]. Moreover, it is structured as an '*assessment process*' so that '*non-conformity is identified, evaluated, and mitigated*'[67] and progress are recorded in writing[68]. While recording can help keep track of both progress and risks, the "*requirement checklist*" provided at the end of the Code may be not sufficient to report and elaborate both of them. Here, integrating existing related initiatives can be a valuable asset and can avoid "reinventing the wheel" when other contributions or disciplines have already found a solution (as suggested by Wang et al. when calling for a cross-sector and

[61] *Ibidem*.

[62] As C. Djeffal highlights (in: C.Djeffal, 'Children's Rights by Design and Internet Governance: Revisiting General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment' (2022) 11(6) Laws https://doi.org/10.3390/laws11060084 accessed 05 July 2025), the "*by-design thinking*" has traditionally been applied in the area of privacy, data protection, and security, but it has begun to spread also throughout the legal system. The "*law-by-design norms*" take advantage of "*the law's binding nature and combine it with normative claims that are to be translated into technology*".

[63] 5Rights Foundation's "Child Rights by Design" principles: (i) equity and diversity, (ii) best interests, (iii) consultation, (iv) age appropriate, (v) responsible, (vi) participation, (vii) privacy, (viii) safety, (ix) wellbeing, (x) development, and (xi) agency.

[64] Digital Futures Commission and 5Rights (11 March 2023).

[65] 5Rights Foundation (March 2025).

[66] *Ibidem*.

[67] *Ibidem*, citing.

[68] *Ibidem*.

ISSN 2281-5147

cross-disciplinary approach). The IEEE 2089-2021[69], for example, foresees the creation of an '*Age Appropriate Register (AAR)*'[70]: a '*medium*'[71], used to document and communicate progressively, and '*handover*'[72] between the competences and responsibilities of the stakeholders involved in one phase to those involved in the subsequent phases[73]. Therefore, the AAR (or a similar tool), can be an important ally in monitoring and ensuring compliance with children's rights (and safety and security standards) throughout the whole AI system's lifecycle.

Whether the use of this or similar tools, in cases such as the doll Cayla, could have been found useful and successful in timely identifying, analysing, and mitigating risks and challenges remains an open question. Further research is needed in order to assess the practical outcomes of applying such frameworks and guidelines, so as to provide effective and actionable indications to practitioners. Retrofitting a product to comply with these rights after development can be equally (if not more) difficult and costly.[74] Accordingly, a child rights approach should be kept as a lighthouse since the pre-deployment phase of an AI system's lifecycle.

3. *Testing* and *validation*: regulatory sandbox environments to ensure safety and compliance

Testing AI systems intended for children within regulatory sandboxes is a crucial step in ensuring the protection of their rights. Children and preadolescents, as particularly vulnerable users, require special consideration from the earliest stages of technology

[69] IEEE Std 2089-2021(2021).

[70] *Ibidem*, citing.

[71] *Ibidem*, citing.

[72] *Ibidem*, citing.

[73] *Ibidem*.

[74] Digital Futures Commission and 5Rights (11 March 2023).

ISSN 2281-5147

design. It is essential to assess how these systems might affect their privacy, safety, and overall well-being from the outset.

Regulatory sandboxes provide a controlled environment in which innovative digital solutions can be tested, allowing technological development to be balanced with the need for protection. This approach makes it possible to identify and address potential issues before the product is released to the market and its compliance with standard and regulation children's rights by design. Several European States include the use of sandboxes as a means to build a comprehensive legal framework for AI. This trend is supported by the EU, which views regulatory sandboxes as facilitators of innovation and recognizes them as a crucial tool in future regulatory activities concerning AI. A regulatory intervention for the definition of this tool was provided by the AI Act, definitively approved on May 21, 2024, which in Article 57 defines AI sandboxes[75]. Regulatory sandboxes on AI, established by European or national competent authorities, provide a controlled environment to develop and test innovative AI systems before commercial deployment. These activities take place under the direct supervision of authorities to ensure compliance with EU and national regulations. When the systems involve the processing of personal data or fall under other regulated areas, data protection authorities and other relevant bodies must be involved in the sandbox's operation[76]. Regulatory sandboxes can help address these issues by providing regulatory certainty for technology companies and other stakeholders, fostering collaboration and capacity-building with and among regulators, and promoting regulatory clarity and compliance[77].

The use of regulatory sandboxes in Europe to test products aimed at minors is still limited and not yet systematized. However, there are some cases and emerging trends that indicate a growing interest in this area, particularly in relation to financial

[75]EU, 'Artificial Intelligence Act' (2024). Chapter VI: Measures in Support of Innovation. https://artificialintelligenceact.eu/chapter/6/ accessed 12 May 2025.

[76] S. Ranchordas, 'Experimental Regulations for AI: Sandboxes for Morals and Mores' (2021) 1(1) Morals & Machines 86 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3839744 accessed 12 May 2025.

[77] Datasphere Initiative, 'Sandboxes for data: creating spaces for agile solutions across Borders' (2022) https://www.thedatasphere.org/ accessed 12 May 2025.

ISSN 2281-5147

education for young people, the protection of personal data (including GDPR compliance and age of consent requirements), the responsible use of technology such as AI and digital platforms designed for minors, and the development of secure digital payment solutions for those under the age of 18.

Datasphere initiative[78] has published a case study on regulatory sandboxes, highlighting the inability of current laws and policies to keep pace with rapid technological developments. The study proposes regulatory sandboxes as tools to foster innovation while ensuring effective data governance - particularly when it comes to children's data. The sandbox model described in the study does not allow for temporary suspensions of legal constraints; instead, it promotes innovation within the existing regulatory framework, encouraging solutions that remain compliant with current rules, trends and better oversee foreign products that process children's data within their jurisdictions[79].

The Norwegian Police University College has tested a bot ("PrevBOT") within a regulatory privacy sandbox, aiming to explore the feasibility of developing a tool capable of automatically patrolling the open internet. The goal of this project is to detect and prevent the sexual exploitation of minors by identifying suspicious behavior and grooming attempts in real time. By combining AI-driven language analysis, behavioral profiling, and age estimation technologies, PrevBOT seeks to serve as a proactive digital safeguard, helping law enforcement intervene before harm occurs - while operating within strict privacy and ethical frameworks. PrevBOT is designed to protect minors online by addressing the growing issue of digital grooming. This crime involves adults who use psychological manipulation and digital communication to build trust with children, often with the intent of sexual exploitation. To effectively counter this threat, PrevBOT integrates advanced technologies capable of identifying risky interactions before they escalate. The system is trained to detect grooming language not only in explicit terms but also in the subtle

[78] The "Datasphere Initiative" is a non-profit dedicated to global collaboration on technical and policy solutions for the urgent, multidimensional, and cross-border challenges of data governance (see: https://www.thedatasphere.org//about-us/ accessed 14 May 2025).

[79] UNICEF, 'Regulatory sandboxes . Case study', 2025: https://www.unicef.org/innocenti/media/11091/file/UNICEF-Innocenti-Regulatory-Sandboxes-Case-Study-2025.pdf accessed 14 May 2025.

ISSN 2281-5147

and coded language often used in chats, including slang and emerging online expressions. It can analyze conversation patterns to recognize early signs of inappropriate behavior, even when the language appears innocent. In addition, PrevBOT estimates the age and gender of users based on their writing style and digital behavior. This allows it to identify potentially fake profiles, especially when adults pretend to be minors to gain access to youth-oriented spaces. Recognizing age discrepancies is important for detecting interactions where children may be at risk. The bot also performs sentiment and behavioral analysis by monitoring response times, typing speed, emotional tone, and interaction patterns. This helps identify users who, despite maintaining a calm or friendly appearance, may be displaying signs of persistence, or manipulation - indicators that their intentions might not align with their words. Together, these capabilities enable PrevBOT to provide proactive protection for minors, flagging dangerous behavior early while respecting privacy regulations and promoting safer digital environments for young users[80]. PrevBOT project is still in its early stages, and it will be interesting to see how it manages to strike a balance between the need for freedom and the need for safety. Minors have a right to agency and privacy, but without an adequate level of online protection, they would not be able to fully exercise those rights. Trust is a key element for a project that aims to comply with both current regulations and the principles of ethical and responsible AI. In this regard, emphasizing transparency and actively involving stakeholders throughout the research process provides a strong foundation.

An important experimentation to make in consideration is the case of the UK's ICO Regulatory Sandbox. The United Kingdom's Information Commissioner's Office (ICO) established the ICO Sandbox program in 2019 to support organizations developing innovative data-based products and services, ensuring compliance with privacy regulations. Since 2020, the program has focused particularly on two areas: protecting children's online privacy through the Children's Code and managing the complex sharing of personal data in sensitive sectors such as health, education, finance, and public administration.

[80] The Norwegian Police University College, exit report: PrevBOT (20 September 2024) https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/reports/the-norwegian-police-university-college-exit-report-prevbot/ accessed 14 May 2025.

ISSN 2281-5147

A notable example is the Lookafterme project by FlyingBinary Limited[81], a digital service based on AI designed to support mental health issues such as anorexia and bulimia, including for children from the age of eight. The system monitors online content in real time and alerts users to potentially harmful material, providing integrated clinical support. During its participation in the Sandbox, FlyingBinary ensured full compliance with UK GDPR, the Data Protection Act 2018, and the Children's Code. The company focused particularly on secure and age-appropriate authentication methods for children, the principle of data minimization, and data protection by design. Special attention was given to the protection of health data, considered sensitive, and ensuring that data processing always took place in the best interest of the child, using the "Best Interests Framework", an ICO tool inspired by the UNCRC. The project serves as a replicable model demonstrating how technological innovation and the protection of fundamental rights can be effectively integrated, especially in sensitive fields like health and education.

Lessons learned from various sandbox experiences highlight both their potential and the challenges they pose - especially concerning children's data. Sandboxes can play a crucial role in helping stakeholders balance the benefits of using minors' data with the need to fully safeguard their rights: testing the doll Cayla in such an environment could have helped experts identify those vulnerabilities and issues before its deployment into the market, and possibly avoid children's harm and company's reputational damage. Encouraging tech companies to participate in sandboxes is a key factor in their success. While some sandboxes provide financial support to cover legal, technical, or operational costs, the most valuable incentive is often the regulatory clarity and compliance assurance they offer.

Sandboxes have demonstrated global relevance and potential for cross-border replication. In particular, international sandboxes can enhance regulatory capacity, improve cooperation, foster innovation and compliance, and promote the availability and accessibility of data across jurisdictions and sectors. By engaging directly with emerging technologies - including those developed abroad regulators, especially in countries without a strong domestic tech sector, can stay informed on global trends

[81] Information Commissioner's Office, 'Regulatory sandbox final report: Flyingbinary'(Tech. Rep., 2022). https://ico.org.uk/media2/migrated/4021302/flyingbinary-exit-report-202208.pdf accessed 15 May 2025.

ISSN 2281-5147

and better oversee foreign products that process children's data within their territory[82].

4. *Deployment* (and *post-deployment*): cyber-threats and risk-driven mitigation

The deployment of AI-based technologies designed for/interacting with/impacting children does not mark the end of the innovation lifecycle but initiates a new phase - one that requires ongoing oversight, responsiveness and ethical commitment. Indeed, ensuring that these systems uphold children's rights over time requires a structured post-deployment framework of assessment, monitoring, and risk mitigation.

interference and, in fact, prove to be particularly vulnerable to a wide range of cyber-threats.[83] Common risks include data breaches that can compromise sensitive personal information (*e.g.*: names, locations and voice recording) or even adversarial attacks that can manipulate system inputs to trigger inappropriate or unsafe outputs, distorting educational content or conversational responses.

As concerns data breaches, particular attention should be paid to the real case of the Smart Toy produced by Fisher-Price[84]. This product represents one of the earliest and most emblematic examples of an Internet-connected smart toy, designed to establish personalized interaction with the child through the use of a rudimentary form of AI[85]. Manufactured by the American company Fisher-Price, a subsidiary of Mattel, the toy was available in three versions - a bear, a monkey, and a panda - and relied on Wi-Fi connectivity and a mobile application managed by parents to oversee its functions. The Smart Toy was capable of gradually learning the child's preferences, customizing

[82] *Ibidem*.

[83] For further reading, S. Shasha et al, 'Playing with Danger: A Taxonomy and Evaluation of Threats to Smart Toys' (2018) 6 IEEE Internet of Things Journal 2986, 2996.

[84] Description of the Fisher-Price Smart Toy Bear, see: http://fisher-price.mattel.com/shop/en-us/fp/smart-toy/smart-toy-bear-dnv31.

[85] For a more in-depth look at the case, refer to: M.C. Gaeta, 'Smart toys and minors' protection in the context of the Internet of everything' (2020) 11(2) Eur J Privacy L & Tech 118.

ISSN 2281-5147

its content and responses through the use of physical smart cards[86]. However, a technical analysis conducted at the hardware, software and network levels[87] revealed critical vulnerabilities in the system's APIs - the *Application Programming Interfaces* that enable communication between applications and services. These vulnerabilities involved the lack of proper identity verification for message senders, thereby allowing unauthorized third parties to gain access to sensitive personal data, such as the child's name, date of birth, language, activity history, and similar information. More concerning was the demonstrated possibility of modifying or deleting user profiles and even altering the toy's functionality, potentially exposing children to physical and psychological harm. This case highlights how, even in the absence of immediate damage, a cyberattack can deeply compromise a child's private and relational sphere, emphasizing the risks posed by the aggregation of seemingly innocuous data, which can be utilized to construct a detailed and exploitable personal profile.

As for the cyber-risks of manipulation, some smart toys have begun incorporating generative AI systems such as ChatGPT - one notable example is Grok[88]. Grok is a conversational toy designed to engage children through verbal interaction powered by a LLM, and it is among the first toys to feature a voice interface connected to ChatGPT. While the toy's goal is to promote natural dialogue, integrating LLMs into children's products raises significant concerns around safety and control. In Grok's case, researchers conducted an experiment[89] that demonstrated the toy continuously streams audio to external servers without requiring a wake word. It records not only

[86] Fisher-Price described the toy as "*an interactive learning friend with all the brains of a computer, without the screen*", thus emphasising its educational and innovative intent to combine technology and learning in a playful and non-invasive format.

[87] Rapid7, *R7-2015-27 and R7-2015-24: Fisher-Price Smart Toy and HereO GPS Platform Vulnerabilities (FIXED)* (Rapid7 Blog, 2 February 2016), online at: https://community.rapid7.com/community/infosec/blog/2016/02/02/security-vulnerabilitieswithin-fisher-price-smart-toy-hereo-gps-platform).

[88] Shaped like a plush rocket, Grok contains an embedded "voice box" inside a zippered compartment and requires Wi-Fi connection via a companion app. To see the product: Curio Interactive Inc. 2024. Curio - AI Toys, https://heycurio.com/. accessed 05-07-2025.

[89] V. Pavliv, N. Akbari and I Wagner, 'AI-powered smart toys: interactive friends or surveillance devices?' in Proceedings of the 14th International Conference on the Internet of Things (IoT '24, ACM 2025) 172.

ISSN 2281-5147

intentional commands but also background conversations, including external audio sources or nearby people. This raises privacy concerns, as sensitive information can be captured and transmitted without the user's knowledge. Furthermore, the toy's responses revealed vulnerabilities: although the experiment was not designed to elicit inappropriate content, some replies contained double meanings - for example, "*it's about spirit not size*". This suggests it may be possible to bypass or break out of the system prompt, allowing the toy to produce inappropriate or unsafe statements, representing a child safety risk and a potential avenue for manipulation.

Given the outlined and - not merely theoretical - cyber risks[90] the post-deployment phase must prioritize the implementation of robust cybersecurity safeguards[91].

Article 15 of the AI Act mandates that high-risk systems - including those used in educational and play-based contexts[92]- be developed with a high degree of robustness and cybersecurity, aligned with the state of the art. This includes encryption, anomaly detection and protection against tampering. At a broader level, Article 5(1)(b) of the AI Act explicitly prohibits the use of AI systems that exploit vulnerabilities linked to age, thereby shielding children from manipulative or coercive behaviors.

Nevertheless, ensuring a secure post-deployment environment for children requires more than technical safeguards; it demands ongoing, structured monitoring and accountability throughout the system's lifecycle. As required by Article 71 of the AI

[90] See the BBC News article related to the Cayla doll case: https://www.bbc.com/news/world-europe-39002142 (*BBC,* 2017), accessed 10 May 2025. Consider also that, where children's rights may be compromised, predefined sunsetting or withdrawal protocols should be established to ensure the safe decommissioning of harmful or outdated AI systems.

[91] In this context, it is important to consider that during the negotiations of the AI Act, numerous child rights organizations called for greater attention to the specific needs of children. In particular, they urged the inclusion of educational systems in the list of "*high-risk*" applications, the prohibition of AI practices that exploit vulnerabilities related to age and the development of clear guidelines to ensure transparency and comprehensibility of AI systems for children. While the final text of the AI Act has partially addressed these demands - by, for instance, including educational AI systems in Annex III and banning the use of AI that exploits age-related vulnerabilities - it has fallen short of explicitly recognizing children as a protected group in all provisions and it lacks specific instructions on how to communicate with child users. European Commission, "Commission Seeks Feedback on Guidelines on the Protection of Minors Online under the Digital Services Act" (11 March 2024).

[92] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, OJ L1689/1, Annex III.

ISSN 2281-5147

Act, providers of high-risk AI must implement a post-market monitoring system to collect and assess performance data over time. Rather than a one-off evaluation, this should be seen as a living framework - one integrating technical vigilance with a sustained ethical responsibility to act in the best interests of the child.

Moreover, post-deployment oversight must be equipped to address adversarial threats, such as input manipulation or the covert reprogramming of educational agents for *non*-educational - or harmful - purposes[93]. To mitigate these risks, real-time monitoring systems must be capable of identifying not only technical malfunctions but also indicators of deliberate misuse, unauthorized alterations or manipulation, as these safeguards are essential to ensuring the long-term safety, reliability and trustworthiness of AI systems - provided they are effectively integrated within a continuous risk assessment framework[94].

Central to this evaluation is the integration of the "Child Rights Impact Assessment" (hereinafter, CRIA): a methodology, applied from the design phase, that examines the potential impacts on children of laws, policies, programmes and services, and that can also be applied to assess both the potential and actual effects of AI systems on children's rights[95]. The CRIA process begins with a screening stage to determine whether a policy, service or technology warrants a full assessment. Where significant impacts are identified, a full CRIA follows, starting with an analysis of the proposal's scope and the relevant Articles of the UNCRC. This stage is backed by qualitative and quantitative evidence, including direct consultation feedback with children to ensure their views are considered and to identify recurring themes and priority concerns. The assessment then evaluates general and disproportionate impacts on specific groups of children and outlines corresponding mitigation strategies (*e.g.:* reduction in exposure to harmful content by X%). The process concludes with a set of findings, including

[93] For an in-depth investigation, see B. Guembe et al., 'The Emerging Threat of AI-Driven Cyber Attacks: A Review' (2022) 36(1) Applied Artificial Intelligence 2037254.

[94] NIST AI, Artificial Intelligence Risk Management Framework *(AI RMF 1.0)* (2023); URL: https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf.

[95] *Ex multis*, J. H. and M.A. Stephenson, 'Human Rights Impact Assessment: Review and Practice Guidance for Future Assessments' (2010) Scottish Human Rights Commission Report; L. Payne, 'Child Rights Impact Assessment as a Policy Improvement Tool' in K. Roberts Lyer (ed), Human Rights Monitoring and Implementation (Routledge 2020) 91.

ISSN 2281-5147

recommendations and monitoring mechanisms. Publishing the CRIA enhances transparency and accountability, ensuring that AI systems are developed in a manner that upholds children's rights and delivers long-term, positive outcomes. Alongside this risk assessment approach, periodic impact reports should be mandated for high-risk AI systems, modeled after the "Data Protection Impact Assessments" (DPIAs), but tailored to specifically address child-specific risks, so that developers, providers, regulators and institutional users[96] must share clear, traceable responsibilities for the long-term impacts of AI on children's well-being.

Therefore, post-deployment accountability demands a collective responsibility from multiple stakeholders.[97] Indeed, regulators must define and enforce standards for an ongoing compliance, while civil society, academic and research institutions should serve as "watchdogs" and evaluators of AI's forthcoming impact and industry actors must commit to the long-term stewardship of their technologies. On this point, instruments such as the aforementioned AAR could play a role in ensuring that AI systems consistently meet children's rights and needs. It could serve as a tool for monitoring issues identified in earlier phases and facilitating the transfer of knowledge across different phases of the design and development. This ensures alignment among all stakeholders, enabling ongoing monitoring to maintain compliance throughout the product's lifecycle.

Ultimately, accountability must be understood not merely as a legal or procedural obligation, but as a moral and social responsibility. The best interests of the child, as enshrined in Article 3 UNCRC, can become an enforceable benchmark only if a "post-deployment conscience" is embraced - one that compels designers, developers and even decision-makers to measure AI's success, by its real-world impact on children's rights and well-being.

[96] Such as schools, public agencies and other stakeholders.

[97] T. Merlin, J. Boyd and C. Donovan, 'The Role of Governments in Increasing Interconnected Post-Deployment Monitoring of AI' (2024) *arXiv preprint* arXiv:2410.04931.

ISSN 2281-5147

5. Closing the lifecycle loop of child Rights-Based AI

And so, this story - one *about* and *for* children - almost comes to an end. It is a narrative where child agency, safety and protection form the hoped-for happy ending. Yet reality proves far more complex. Even when AI systems are designed, developed and deployed in line with children's rights standards, there is no guarantee of their continued compliance in real-world use. Here is where our story begins again, going back to the development phase or even to the design phase, in a never ending, possibly safe and child rights-based loop.

To be fully applicable, the lifecycle loop of child rights-based AI suggested in this work needs to address some limitations:

(i) Existing frameworks (*e.g.*: from UNICEF[98] and IEEE 2089-2021[99]) provide important guidelines to practitioners, but they often miss out on metrics and/or practical implementation tools. These gaps can pose limitations to their applicability, resulting in too high-level recommendations of difficult understanding and/or operationalization for practitioners. At the same time, few academic works, focusing on a specific case or system, rarely offer scalability solutions "*per se*". Consequently, core research priorities are: (i) identifying, evaluating and validating metrics and operational measures specifically for AI systems intended for children, and (ii) integrating these metrics and measures with knowledge from other fields (*e.g.*: development theories). At the same time, practitioners can in the meanwhile refer to valuable already existing materials. To guide the reflection, when creating and building a new service or product for children, practitioners can indeed refer to contributions

[98] UNICEF - V. Dignum, M.Penagos, K.Pigmans and S.Vosloo (November 2021).

[99] IEEE, Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children, (2021).

ISSN 2281-5147

such as the ones highlighted above in this paper, or others like the 5Rights' "Playful by Design Toolkit"[100] or Save the Children's guide on "Child-Centered Design"[101].

(ii) Regulatory Sandboxes are expected to be created in the EU by 2026[102]. Regulatory Sandboxes can be very effective tools to bridge the gap between technological innovation and slow regulatory adaptation. This gap is particularly evident in sectors such as fintech, AI, blockchain and biotech, where technology is advancing faster than regulators can regulate it. The sector concerning the protection of minors in the use of technology presents serious regulatory gaps, making it difficult to effectively safeguard the rights of young people in the digital environment. The Italian case is an emblematic example. Since the entry into force of the new European Electronic Communications Code[103] (December 2020), a derogation that allowed ICT companies to monitor and report child sexual abuse material online has lapsed. This regulatory gap has had direct and measurable consequences: reports to the competent authorities have decreased by 46% across Europe, negatively impacting prevention and enforcement efforts against child abuse. Furthermore, the "Caivano Decree" (September 2023) [104], in an effort to strengthen child protection, delegated to AGCOM the task of defining technical tools for age verification and secure access to digital content. However, to date, no concrete implementing measures have been

[100] 5Rights Foundation, 'Playful by Design' (2021). https://playfulbydesign.5rightsfoundation.com. Accessed 11 September 2025.

[101] Save the Children Finland, 'Child-Centered Design' (2020). https://resourcecentre.savethechildren.net/document/child-centered-design. Accessed 11 September 2025.

[102]European Parliament and Council. Regulation (EU) 2024/1689 of the European parliament and of the council of 13 june 2024 laying down harmonised rules on artificial intelligence and amending regulations (ec) no 300/2008, (EU) no 167/2013, (EU) no 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (AI act) (text with eea relevance), 2024.

[103] Directive (EU) 2018/1972 establishing the European Electronic Communications Code [2018] OJ L321/36; transposed into Italian law by D. lgs., 8 november 2021, n. 207, GURI n.292, 9 December 2021.

[104] Decreto Legge 15 Settembre 2023, n°123 "Misure urgenti di contrasto al disagio giovanile, alla povertà educativa e alla criminalita' minorile, nonche' per la sicurezza dei minori in ambito digitale" https://www.gazzettaufficiale.it/eli/id/2023/11/14/23A06292/sg accessed 06 July 2025.

ISSN 2281-5147

adopted: only guidelines are in force, which are not legally binding, and actual implementation by operators remains inconsistent. In this context, innovative tools such as AI regulatory sandboxes could represent a strategic opportunity to overcome the regulatory deadlock. Sandboxes offer a regulated yet flexible environment in which to test technologies and solutions (such as age verification systems, AI-based parental control, or the automated detection of illegal content) before their full legal application. The experience of the United Kingdom, for instance, shows how regulatory experimentation can contribute to the development of dedicated legislation. The UK Information Commissioner's Office (ICO) has used sandboxes to develop the principles of the "Children's Code", a legal framework that has since established new standards for the design of digital platforms with a focus on respecting children's rights.

However, so far, there are few examples of attempts to create such environments. A recent paper[105] proposes a regulatory framework for child-friendly AI sandboxes that integrates the EU AI Act with UNICEF guidelines and other international references (UN, OECD, UNESCO). This framework is structured around a multi-stakeholder, modular, and iterative process aimed at ensuring that the development and testing of AI systems respect the rights and well-being of children. Given the international relevance of the topic, interesting new contributions are expected in the near future;

(*iii*) *Zero risk doesn't exist,* cybersecurity threats may still emerge over time. Therefore, it is essential to move beyond voluntary guidelines and soft law (meaning, codes of conduct and non-binding recommendations). To ensure the long-term protection of children's rights in digital environments, companies must be encouraged - and, where necessary, compelled - to take shared responsibility through binding legal frameworks and effective enforcement mechanisms. In the post-deployment phase, proactive regulation is crucial to clearly define the duties and liabilities of AI producers, software developers and platform operators, with enforceable measures such as substantial fines for damages and explicit rights of claim for affected parties (*post*-damage protection). This ongoing accountability should be anchored in systematic monitoring, inspired by the CRIA or comparable methodologies, and guided by

[105]V. Charisi and V. Dignum, "Operationalizing AI Regulatory Sandboxes for Children's Rights and Well-Being" in Human-Centered AI (Chapman and Hall/CRC 2024) 231.

ISSN 2281-5147

robust indicators. Relevant measures may include: (i) tracking the number and severity of cyber-incidents involving children, (ii) assessing the speed and effectiveness of responses to identified risks, (iii) evaluating the participation of children in post-deployment reviews, (iv) analysing the distribution of impacts across different groups of children in order to detect disproportionate effects, and (v) collecting data on children's own perceptions of safety and well-being when engaging with digital systems. Embedding such evidence-based indicators within regulatory frameworks ensures that accountability extends beyond the design stage, turning compliance into a continuous, transparent and participatory process that protects children's rights throughout the entire life cycle of AI systems.

Also, future efforts should aim to overcome these limitations by developing more effective strategies for engaging children directly - such as through interviews, surveys and focus groups - and by fostering a collaborative approach that integrates diverse professional and academic expertise. This strategy will better position the final AI system to meet security standards and ensure compliance with children's rights and related obligations.

ISSN 2281-5147

ISSN 2281-5147

LA TUTELA DEL MINORE NELL'ERA DELL'INTELLIGENZA ARTIFICIALE: QUESTIONI APERTE SUL METODO DI GESTIONE DEL RISCHIO

Matilde Ratti*

Abstract

La diffusione di sistemi di intelligenza artificiale evidenzia la crescente esigenza di individuare soluzioni di protezione per il minore e i suoi diritti. Sul punto, le diverse normative volte alla tutela dei minori *online*, sia nell'uso di strumenti di intelligenza artificiale sia nella fruizione dei *social network* o nel trattamento dei dati personali, presentano approcci eterogenei riconducibili a differenti metodologie regolatorie. Sono numerosi i punti di contatto tra le criticità affrontate dai provvedimenti sull'impiego di strumenti dotati di intelligenza artificiale, di protezione dei dati personali e di uso dei *social network*. Anche a livello normativo, dal modello statunitense, alla legislazione australiana alla recente normativa italiana, le principali questioni attengono al grado di effettività delle misure individuate nella gestione del rischio per i minori nell'ambiente digitale.

The wide application of artificial intelligence systems highlights the growing need to identify solutions to protect minors and their rights. In this regard, the various regulatory initiatives aiming to protect minors in the digital environment, including both those related to the use of artificial intelligence tools, and the use of social networks, and the processing of personal data, highlight heterogeneous approaches answering to different regulatory methodologies. There are indeed several points of contact between the critical issues addressed by the provisions on the use of artificial intelligence tools, personal data protection, and the use of social networks. Even at the regulatory level, from the US model to Australian framework, and the recent Italian legislation, the main issues concern the degree of effectiveness of the measures identified in managing risks for minors in the digital environment.

* Professoressa Associata di diritto privato, Università di Bologna, matilde.ratti@unibo.it
Il presente contributo è stato sottoposto a referaggio a doppio cieco ed è finanziato su progetto *Children as Vulnerable Users of IoT and AI-based Technologies: A Multi-level Interdisciplinary Assessment* – CURA, PRIN 2022–2022KAEWYF, – Next Generation EU; CUP: J53D23005540006.

ISSN 2281-5147

Indice Contributo

Keywords

Minore – Intelligenza Artificiale – Protezione dei Dati Personali – Piattaforme Digitali – Age Verification

1. Il minore e l'accesso agli strumenti dotati di intelligenza artificiale

La crescente consapevolezza circa gli effetti dell'uso dei dispositivi che consentano l'accesso ad Internet, ai *social media* e ai sistemi dotati di intelligenza artificiale sta

ISSN 2281-5147

plasmando lo scenario politico-legale sul tema del minore che agisce *online*[1]. Alcune tematiche suscitano un particolare interesse poiché presentano evidenti rischi per il minore in quanto tale e, tra queste, vi è certamente quella connessa alla possibilità di avere rapido accesso agli strumenti dotati di intelligenza artificiale. Sul piano internazionale, il Comitato sui diritti dell'infanzia delle Nazioni Unite è intervenuto con il Commento Generale n. 25 esplicitamente estendendo l'ambito di applicazione dei diritti del fanciullo ad Internet (e alle nuove tecnologie) e ribadendo la doverosa attenzione da prestare alla fragilità ontologicamente connessa alla natura del minore[2]. Sebbene tale approccio sia penetrato in certa misura negli atti normativi dell'Unione Europea[3], confermando la rilevanza del tema nell'attuale cultura legislativa, non vi è ad oggi una disciplina europea specificamente rivolta alla protezione del minore che

[1] Tra le più recenti opere che affrontano in modo specifico il tema, cfr. D. Amram, *Non ho l'età ma… Costruire competenze abilitanti per una società dell'informazione a prova di (in)capacità del minore di età* (1° ed., Lefebvre Giuffré 2025); C. Camardi, 'Relazione di filiazione e *privacy*. Brevi note sull'autodeterminazione del minore' (2018) 5 Jus Civ 831ss.; R. Senigaglia, 'L'identità personale del minore di età nel cyberspazio tra autodeterminazione e *parental control system'* (2023) 6 NLCC, 1568ss.; G. Carapezza Figlia, '*Sharenting*: nuovi conflitti familiari e rimedi civili' (2023) 5 NGCC 1104ss.; A. La Spina, 'L'identità del minore nella realtà on-life tra protezione e autodeterminazione' (2024) 10 Famiglia e Diritto, 920ss.; I. Garaci, 'Il «superiore interesse del minore» nel quadro di uno sviluppo sostenibile dell'ambiente digitale' (2021) 4 NLCC, 800ss.; M. Giandoriggio, 'I minori d'età e i social network: l'insostenibile leggerezza del post' (2024) 3 Danno e resp. 296ss.; I. Garaci, 'La *privacy* del minore d'età nell'ambito familiare' (2023) 1 EJPLT 84ss.; L. Lenti, 'L'identità del minorenne' (2006) 1 NGCC 68ss.; E. Moscati, 'Il minore nel diritto privato, da soggetto da proteggere a persona da valorizzare (contributo allo studio "interesse del minore")' (2014) 10 Dir. fam. pers. 1141ss.

[2] Comitato sui diritti dell'infanzia, *Commento generale n. 25: Sui diritti dei minorenni in relazione all'ambiente digitale,* 2022 <I diritti dei minorenni in relazione all'ambiente digitale | UNICEF Italia> ultimo accesso 1 settembre 2025.

[3] Alcune delle enunciazioni contenute in tale Commento sono state recepite anche nei considerando del Digital Services Act (DSA). In particolare, il considerando 71 sottolinea che la protezione dei minori costituisce un obiettivo politico prioritario dell'Unione europea e definisce le condizioni in cui una piattaforma *online* può considerarsi accessibile ai minorenni, richiedendo ai prestatori l'adozione di misure appropriate e proporzionate, anche attraverso interfacce progettate secondo logiche di *privacy* e sicurezza "*by design*" e "*by default*". In stretta connessione, il considerando 81 stabilisce che le piattaforme e i motori di ricerca di dimensioni molto grandi sono tenuti a considerare, nell'analisi dei rischi sistemici, l'impatto delle proprie interfacce e dei propri servizi sui diritti del minore, con particolare attenzione ai possibili effetti pregiudizievoli sullo sviluppo fisico, mentale e morale, nonché ai meccanismi che possono sfruttare l'inesperienza o la vulnerabilità dei minorenni. Infine, il considerando 89 riafferma la necessità di modellare il *design* dei servizi digitali nel rispetto del superiore interesse del fanciullo e prevede che i meccanismi di tutela e di ricorso offerti dal regolamento siano resi effettivamente accessibili anche ai soggetti minorenni. Tali previsioni riprendono e traducono in chiave normativa europea alcune delle linee direttrici poste dal Commento Generale n. 25, che insiste sulla necessità di una protezione specifica dei minori nell'ambiente digitale, nonché sul riconoscimento del loro diritto a strumenti adeguati, trasparenti e accessibili di partecipazione e tutela.

ISSN 2281-5147

utilizzi sistemi di intelligenza artificiale. Infatti, sebbene il Regolamento europeo 2024/1689 (l'*AI Act*) vieti l'impiego di sistemi che sfruttino le vulnerabilità (anche quando siano connesse all'età)[4] e preveda obblighi di valutazione del rischio che tengano conto la natura dell'utilizzatore[5], il tema del minore non è trattato in modo specifico né è oggetto di una disciplina dedicata. Ci si propone, dunque, di valutare l'opportunità di un approccio organico alla tutela dei diritti del minore partendo da un'analisi delle più rilevanti decisioni in materia e indagando, in seguito, le potenzialità e le criticità delle primissime soluzioni giuridiche adottate nell'ordinamento italiano e in altri Stati che, in modo più o meno diretto, si sono interessati al tema[6].

2. La protezione dei dati personali volta alla tutela del minore che interagisca con strumenti di IA

Nello scenario italiano, i primi provvedimenti ad interessarsi della tutela del minore che adoperi strumenti dotati di intelligenza artificiale sono proprio quelli del Garante per la protezione dei dati personali, che ha indagato l'opportunità di implementare sistemi di verifica dell'età (o *age verification*) per l'accesso a servizi *online* allo scopo di limitare la potenziale violazione dei diritti del minore. Ci si riferisce in primo luogo al noto provvedimento del 2 febbraio 2023[7], avente ad oggetto il sistema *Replika*, una *chatbot* intelligente che genera un "amico virtuale" a supporto del benessere emotivo dell'utente, a più riprese oggetto dell'attenzione del Garante. Nel caso in commento,

[4] Cfr. AI Act, art. 5, par. 1, lett. b), Peraltro, l'art. 7 dell'*AI Act* attribuisce alla Commissione il potere di adottare atti delegati per modificare i casi d'uso dei sistemi di IA ad alto rischio se questi presentano « un rischio di danno per la salute e la sicurezza, o di impatto negativo sui diritti fondamentali» (cfr. lett. b) del par. 1) anche tenendo conto del criterio secondo il quale «esiste uno squilibrio di potere o le persone che potrebbero subire il danno o l'impatto negativo si trovano in una posizione vulnerabile rispetto al *deployer* di un sistema di IA, in particolare a causa della condizione, dell'autorità, della conoscenza, della situazione economica o sociale o dell'età» (par. 2, lett. h).

[5] Cfr. AI Act, art. 9, par. 9.

[6] EDPB, *Linee guida 8/2020 sul targeting degli utenti di social media* (2021). In dottrina, ampiamente in G. Finocchiaro, *Intelligenza Artificiale. Quali regole?,* (1ª ed., Il Mulino 2024); G. Finocchiaro, 'La proposta di Regolamento sull'Intelligenza Artificiale: il modello Europeo basato sulla gestione del rischio' (2022) 2 Dir. inform. Inf. 303ss.; G. Finocchiaro, 'Il perfezionamento del contratto on line: opportunità e criticità' (2018) 1-2 Dir. com. scambi internaz., 187ss.; G. Finocchiaro, *La protezione dei dati personali in Italia – Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101* (1ª ed., Zanichelli Editore 2019).

[7] *Provv. del 2 febbraio 2023* [2023] GPDP 9852214, Registro dei provvedimenti n. 39 del 2 febbraio 2023.

ISSN 2281-5147

l'Autorità aveva evidenziato la necessità che il *provider* adottasse dei meccanismi di verifica dell'età per consentire l'utilizzo della *chatbot*[8]. La società implementava dunque un meccanismo di *age gate* in tutte le pagine di registrazione, prevedeva un periodo di raffreddamento (*cooling-off period*) e predisponeva strumenti per consentire agli interessati l'esercizio effettivo dei propri diritti[9]. Due anni dopo, tali misure erano giudicate insufficienti con il provvedimento del 10 aprile 2025[10], che chiariva la prospettiva giuridica adottata dall'Autorità. Considerato che proprio secondo le ricostruzioni della Società il servizio sarebbe stato destinato a soli maggiorenni, il trattamento dei dati del minore avrebbe violato il generalissimo principio di minimizzazione previsto dal Regolamento 2016/679 (in seguito semplicemente "GDPR"). Il trattamento avrebbe inoltre violato gli obblighi di *accountability* incombenti sul *provider* (art. 24 del GDPR) e avrebbe comportato l'ingiusta esposizione del minore ad un servizio inadeguato alla sua età[11].

Un'analoga posizione era emersa anche nel 2024 in riferimento ad un altro provvedimento storico della medesima Autorità, quello avente ad oggetto il servizio di ChatGPT[12]. In questo caso, il Garante rilevava la mancanza di un sistema per

[8] La registrazione, infatti, richiedeva unicamente l'inserimento di nome, indirizzo *e-mail* e genere, senza alcuna procedura di *age verification*. Il Garante aveva inoltre rilevato la mancanza di un sistema di moderazione dei contenuti calibrato in base all'età dell'utente, con la conseguenza che i minorenni risultavano esposti a materiali non adeguati al loro grado di sviluppo. Per completezza, si segnala altresì che in mancanza di informativa sul trattamento dei dati personali l'Autorità ha segnalato l'impossibilità di comprendere le modalità del trattamento e la base giuridica dello stesso. Sul punto, il Garante ha escluso che, per i minori, la base giuridica potesse rinvenirsi nell'accettazione delle condizioni di utilizzo, stante l'incapacità legale a contrarre per la fruizione del servizio.

[9] La misura della limitazione del trattamento ordinata dall'Autorità era in seguito sospesa dal medesimo Garante. *Provvedimento del 22 giugno 2023* [2023] GPDP 10013893, Registro dei provvedimenti n. 280 del 22 giugno 2023.

[10] Cfr. *Provvedimento del 10 aprile 2025* [2025] GPDP 10130115, Registro dei provvedimenti n. 232 del 10 aprile.

[11] Cfr. *ivi*: «Nello specifico, la mancata adozione da parte della Società di misure idonee a salvaguardare l'accesso e l'utilizzo del servizio Replika aveva comportato non solo che Luka trattasse, sistematicamente, dati personali ulteriori rispetto a quelli realmente necessari per conseguire la finalità del trattamento (vale a dire offrire il servizio ad utenti maggiorenni), ma anche che tale trattamento riguardasse dati relativi a soggetti vulnerabili (minorenni, potenzialmente di età anche inferiore ai 13 anni) che, a causa di tale carenza ed attesa la tecnologia innovativa sottesa al servizio e la natura altamente sensibile delle conversazioni fornite dal chatbot, sono stati esposti ad un rischio particolarmente elevato».

[12] *Provvedimento del 2 novembre 2024* [2024] GPDP 10085455, Registro dei provvedimenti n. 659 del 2 novembre 2024. La decisione si inserisce a chiusura della vicenda che aveva coinvolto la Società OpenAI in relazione ai trattamenti di dati personali condotti tramite la sua IA *ChatGPT*. Con primo provvedimento del 30 marzo 2023, doc. web n. 9870832, il Garante aveva comminato la sanzione di limitazione del trattamento dei dati personali degli interessati stabiliti in Italia sulla base di una serie di violazioni intercorse. Spiccavano, in particolare, un *data breach* avvenuto nel marzo 2023, consistente nella visualizzazione da parte degli utenti del servizio di dati personali appartenenti ad altri utilizzatori; l'assenza di informativa adeguata sul sito *web* e la mancanza di meccanismi per garantire i diritti di opposizione e cancellazione degli interessati; l'assenza di base giuridica del trattamento per l'addestramento degli algoritmi sottesi al funzionamento della piattaforma. La sanzione

ISSN 2281-5147

verificare la provenienza del consenso dall'esercente la responsabilità genitoriale[13], consenso richiesto dal *provider* proprio per utilizzare il servizio[14]. Da un lato, l'obbligo di verifica dell'età era posto in capo al titolare del trattamento, ovverosia il *provider*: questi avrebbe dovuto verificare l'età dell'utente con la necessaria diligenza. Dall'altro, l'Autorità ammetteva che il contratto stipulato tra l'infraquattordicenne (con il permesso del genitore) e il *provider* per l'uso del servizio *ChatGPT* potesse costituire un'idonea base giuridica per trattare i dati personali del minore ai sensi del GDPR. Inoltre, pur considerando le diverse caratteristiche del servizio rispetto a quello esaminato nel provvedimento in precedenza richiamato, il Garante anche in questo caso evidenziava il rischio di esposizione del minore a contenuti inappropriati[15] ed individuava quale soluzione sostanziale l'imposizione di un vincolo di accesso a ChatGPT tramite la precostituzione di un idoneo meccanismo di *age verification*.

3. La protezione dei dati e la tutela del minore nell'accesso ai *social network*: profili di analogia

Nel medesimo periodo in cui il Garante italiano affrontava le questioni sul minore che acceda a strumenti dotati di intelligenza artificiale, negli Stati Uniti d'America era

comminata era stata poi sospesa con *Provvedimento dell'11 aprile 2023*, 874702, a seguito dell'adozione di misure organizzative e tecniche da parte della società volte ad adeguare il trattamento dei dati personali alle previsioni normative.

[13] Ancora a titolo di completezza, interessante la replica della Società, avallata dal Garante, che, con riferimento alla mancata adozione di misure idonee per verificare il consenso prestato dai minori, nega l'applicazione dell'art. 8 GDPR in quanto la base giuridica del trattamento non sarebbe rinvenibile tanto nel consenso degli interessati, quanto nell'esecuzione di un contratto ai sensi dell'art. 6 lett. b) GDPR.

[14] La decisione, a ben vedere, si pone in contraria direzione rispetto a quanto l'Autorità stessa aveva in precedenza stabilito nel citato Provvedimento del 2 febbraio 2023 in relazione al servizio Replika. In quell'occasione, il Garante aveva escluso *a priori* che la base giuridica potesse rinvenirsi nell'esecuzione di adempimenti nell'ambito di un contratto concluso con l'utente, stante l'incapacità del minore a contrarre nell'ordinamento.

[15] Con riguardo alle modalità di verifica dell'età, la società aveva vagliato alcune misure correttive, quali l'inserimento dei dati di una carta di credito, l'introduzione di appositi meccanismi di IA in grado di misurare l'età, la scansione della carta di identità prima dell'accesso al servizio. OpenAI aveva infine deciso di affidare l'attività ad una società esterna (Yoti), la quale avrebbe restituito ad OpenAI solo l'esito positivo o negativo della verifica previo autoscatto dell'utente e scansione di un documento di identità. Tale sistema è stato tuttavia giudicato insufficiente dall'Autorità. In aggiunta, per ciò che qui interessa ai fini della delineazione di un sistema di responsabilità in merito all'accesso al servizio da parte di minore, si evidenzia che la sanzione è stata comminata al titolare per aver mantenuto esposti i minori al rischio di contenuti inappropriati per un determinato periodo di tempo. Non è peraltro accolta la posizione di OpenAI che imputa alla mancanza di *standard* uniformi sulle misure più idonee per la tutela dei minori, ritenendo il Garante che la responsabilità di individuare le soluzioni idonee alla tutela del minore caso per caso ricada sul titolare del trattamento.

ISSN 2281-5147

adottato il Provvedimento della *Federal Trade Commission* del 2 agosto 2024[16] sull'adeguatezza del trattamento di dati personali di minori svolto dalla Bytedance, proprietaria di TikTok, alle disposizioni del *Children's Online Privacy Protection Act* (COPPA, 15 U.S.C. 6501) e del *Children's Online Privacy Protection Rules* (16 C.F.R. Part 312). Seppur adottato nei confronti di un *social network*, il provvedimento appare incentrato su un tema assai vicino a quello in esame, avendo ad oggetto il trattamento automatizzato dei dati personali degli utenti minorenni (anche con finalità di *marketing*). Nel *social* era consentito che minori di 13 anni creassero *account* personali. In particolare, al momento dell'apertura del profilo erano raccolti nomi, indirizzi *e-mail*, numeri di telefono e immagini, dati successivamente ritenuti eccedenti rispetto a quanto consentito dalla normativa applicabile. Secondo quanto evidenziato dalla *Federal Trade Commission*, infatti, la Sezione 312.4(c) delle COPPA *Rules* prevedeva che il *provider* potesse raccogliere solo alcuni dati del minore prima di ottenere il consenso da parte dell'esercente la responsabilità genitoriale e, comunque, solo al fine di consentire il funzionamento del servizio. Inoltre, come nei casi oltreoceano, era rilevato che il sistema di verifica dell'età dell'utente fosse facilmente aggirabile tramite, ad esempio, una falsa dichiarazione di età o accedendo al *social* attraverso piattaforme terze (come Google o Instagram) che non prevedevano, a loro volta, rigidi sistemi di verifica dell'età[17]. Il procedimento, ancora pendente presso la *Federal Trade Commission* e dall'esito è incerto, pone il problema – se non ancora dal punto di vista legislativo, quantomeno in via di valutazione di opportunità sociale – della possibilità per il minore di agire liberamente in rete sui *social network* e lascia emergere la stretta connessione esistente tra le preoccupazioni avanzate dall'Autorità per la protezione dei dati personali italiana nei confronti dei prestatori di sistemi di IA e la *Federal Trade Commission* in relazione ai prestatori di *social network*. Il fulcro di entrambe le questioni sta proprio nell'applicazione del principio di minimizzazione del trattamento dei dati e nell'appropriatezza degli strumenti normativi e tecnici previsti nell'ipotesi in cui il minore possa accedere ad ambienti virtuali ove, a seconda del caso specifico, potrebbero anche essere utilizzati sistemi di intelligenza artificiale.

[16] Federal Trade Commission, *Provvedimento Bytedance ltd, Us v.* (2024), <https://www.ftc.gov/legal-library/browse/cases-proceedings/bytedance-ltd-us-v> ultimo accesso 17 settembre 2025

[17] È stata inoltre rilevata la mancanza di un'informativa adeguata che spiegasse quali dati personali dei minori trattasse e per quale finalità, violando le Sezioni 312.3(a) e 312.4(d) delle COPPA Rules e non è stato richiesto il consenso da parte dei genitori, violando così le Sezioni 312.3(b) e 312.5(a)(1) COPPA Rules

ISSN 2281-5147

Dell'assenza di misure per la tutela dei minori nei *social network* si sono interessati anche altre autorità per la protezione dei dati personali. In particolare, nell'agosto 2022, l'Autorità irlandese aveva adottato un progetto preliminare di decisione[18] nei confronti di TikTok Technology Limited riguardante l'assenza di strumenti in grado di proteggere il minore sulla piattaforma. Il progetto di decisione si concentrava sulla possibile violazione di alcune delle norme in materia di protezione dei dati personali previste dal GDPR[19]. In particolare, l'Autorità irlandese rilevava la mancanza di un sistema di *parental control*, l'assenza di informazioni circa la diffusione dei contenuti pubblicati dai minori e la carenza di protezione dei profili da questi creati, impostati di *default* come *account* "pubblici" e tramite un sistema di verifica dell'età consistente nella semplice dichiarazione espressa dall'utente al momento dell'iscrizione. A seguito delle osservazioni poste da TikTok sul progetto di provvedimento, l'Autorità irlandese condivideva il progetto anche con l'Autorità tedesca e con quella italiana, le quali presentavano alcune obiezioni[20]. L'Autorità irlandese deferiva dunque la controversia all'EDPB, che interveniva con decisione vincolante[21]. Era così stabilito che la società avesse violato alcune delle norme del GDPR richiamate, ma non l'art. 25 del GDPR in materia di *privacy by design* e *by default*, disposizione solitamente invocata in funzione dell'accertamento di un trattamento di dati eccessivo. Cionondimeno, era osservato il mancato rispetto del principio di correttezza nell'omettere di comunicare al minore le potenzialità di diffusione dei dati personali che questi avrebbe caricato sulla piattaforma[22]. Il Garante irlandese escludeva, a cascata, la violazione dell'art. 25 GDPR, ma ordinava a TikTok di provvedere all'inserimento di una notifica a comparsa durante la registrazione e la pubblicazione di video, riconoscendo il rischio

[18] Data Protection Commission, *In the matter of TikTok Technology Limited: Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act 2018 and Articles 60 and 65 of the General Data Protection Regulation,* (IN-21-9-1 2023) <final_decision_tiktok_in-21-9-1_-_redacted_8_september_2023.pdf> ultimo accesso 18 settembre 2025.

[19] In particolare, si trattava degli artt. 5, 12, 13, 24, 25 GDPR.

[20] Anche queste avevano infatti segnalato la violazione delle stesse norme del GDPR da parte di TikTok.

[21] EDPB, *Decisione vincolante 2/2023 relativa alla controversia presentata dall'autorità di controllo irlandese riguardante TikTok Technology Limited (articolo 65 del RGPD)* (2023) <edpb_bindingdecision_202302_ie_sa_ttl_children_it_0.pdf> ultimo accesso 17 febbraio 2025.

[22] Preme osservare che l'EDPB nega la violazione dell'art. 25 non in punto di diritto, ma in quanto ritiene che le informazioni presentate dall'Autorità irlandese circa l'assenza di ulteriori misure adottate dal prestatore per la verifica dell'età sono insufficienti a stabilire se le soluzioni adottate da TikTok siano inadatte a tutelare i minori. Cfr. EDPB, *Decisione vincolante 2/2023,* (n 21) 58.

ISSN 2281-5147

per il minore che utilizzasse la paittaforma[23]. La misura di tutela prescelta era dunque volta alla maggiore sensibilizzazione del minorenne e del genitore nei confronti dei potenziali rischi di utilizzo del *social network*, pur non risultando violato il principio di *privacy by design* e *by default*[24].

A ben vedere una simile posizione, di delicato equilibrio, è emersa proprio nel provvedimento ChatGPT sopra richiamato, nel quale l'Autorità italiana, pur ordinando la predisposizione di misure tecniche per la tutela del minore, aveva negato l'applicabilità dell'art. 8 GDPR, sostenendo che il consenso a cui tale norma si riferisce non costituisse la legittima base giuridica per il trattamento dei dati personali svolto, con la conseguenza che la sua ipotetica violazione sarebbe risultata in concreto irrilevante.

L'esame dei provvedimenti pone in primo luogo in luce le evidenti incertezze connesse ad un processo, attualmente in atto, di definizione del quadro normativo applicabile. Tutti i provvedimenti citati riconoscono il rischio di ingiusta esposizione del minore e la necessità di adottare idonee misure tecnologiche, di processo o di trasparenza, atte a limitare tale rischio. Nello scenario europeo, non è tuttavia chiarita la norma o il principio di diritto violato. In effetti, il riferimento all'art. 8 GDPR in materia di consenso prestato dall'esercente la responsabilità genitoriale in caso di minore che utilizzi servizi *online* presenta il limite dell'applicabilità materiale della previsione, letteralmente confinata ai casi nei quali la base giuridica da porre a fondamento del trattamento sia proprio il consenso. Tale norma non sarebbe dunque applicabile qualora la base del trattamento dei dati (come precisato dal Garante nel caso ChatGPT) fosse da individuarsi nella conclusione di un contratto tra l'utente del servizio (ancorché tramite il consenso espresso dai soggetti esercenti la responsabilità genitoriale) ed il prestatore titolare del trattamento. Evidenziare un trattamento che non rispetti il *principio di privacy by design* o *privacy by default* (con conseguente violazione dell'art. 25 GDPR) potrebbe costituire una soluzione giuridicamente più appropriata in astratto, considerata la natura ontologicamente elastica dei principi di diritto citati, ma l'EDPB non pare ad oggi confermare la soluzione prospettata dal Garante irlandese. Ciò nondimeno, in tutti i provvedimenti richiamati, è evidente il ricorso alle

[23] Il Garante irlandese, con provvedimento 1° settembre 2023, irroga quindi la sanzione di euro 345 milioni ritenendo violati gli artt. 5, 12, 13 e 24 GDPR. Cfr. Data Protection Commission, *In the matter of TikTok Technology Limited* (n 18).
[24] Cfr. EDPB, *Decisione vincolante 2/2023* (n 21) 67.

ISSN 2281-5147

previsioni in materia di protezione dei dati personali allo scopo di affrontare il tema della tutela del minore. Si osserva, inoltre, che tale tendenza è trasversale ai casi di impiego dei sistemi intelligenti e dei *social media*.

La seconda osservazione che si può svolgere discende proprio da quest'ultima circostanza, nel senso che l'illecito trattamento dei dati, le modalità di accesso al servizio e i derivanti rischi di utilizzo per il minore appaiono intersecare scenari e strumenti assai differenziati. In altre parole, non si tratta solo di impiego di strumenti intelligenti, né unicamente di illecito trattamento dei dati personali o di improprio utilizzo dei *social network*. Spesso, le problematiche in ordine alla tutela del soggetto altamente vulnerabile possono sussistere a prescindere dalla tipologia di servizio prestato e riguardano le modalità di trattamento dei dati personali degli utenti, così come il rischio di esporli a contenuti o servizi inadeguati alla loro età[25]. Analogamente, e in modo logicamente conseguente, la misura alla quale più sovente i Garanti volgono la loro attenzione pare quella connessa alla limitazione di accesso alla rete, alla piattaforma, al *social network* o allo strumento di IA.

4. Le regole in materia *age verification* quali strumenti trasversali di tutela

Le norme in materia di limitazione dell'accesso in ragione dell'età appaiono dunque uno strumento trasversale nell'intento di garantire tutela al minore. Il punto di contatto evidenziato spinge a valutare positivamente l'opportunità di estendere il presente ambito di indagine. Ciò pare utile per più ragioni. In primo luogo, le norme sui *social network* e minori sono state adottate in un'epoca precedente (seppur non distante) a quella attuale, nella quale ci si interroga anche sul più recente tema dell'intelligenza artificiale. L'antecedenza storica, seppur minima, è certamente di interesse poiché consente di esaminare le tendenze legislative e gli orientamenti decisionali che si sono formati in relazione ai *social network*, sì da verificarne l'utilità e l'efficacia rispetto all'eventuale normazione in materia di intelligenza artificiale. In secondo luogo, l'estensione dell'ambito di indagine pare utile in ragione di alcune osservazione di carattere operativo, in quanto da un lato i *provider* potrebbero trovarsi ad impiegare strumenti dotati di intelligenza artificiale proprio nella fornitura dei loro servizi. Dall'altro, la stretta connessione tra le tematiche è altresì data dalla circostanza

[25] Ibid.

ISSN 2281-5147

che tali strumenti potrebbero comunque essere resi disponibili tramite l'identificazione svolta proprio dai *social network*.

Con riferimento a tali fornitori, nello scenario europeo è utile richiamare il *Digital Services Act*[26] e, in particolare, l'art. 28[27]. La norma stabilisce l'obbligo in capo ai fornitori di piattaforme *online* di adottare misure adeguate e proporzionate a garantire un elevato livello di tutela dei minori[28]. Tra i progetti avviati dalla Commissione europea volti all'attuazione di questa previsione[29] rientra il recente *Statement* 1/2025 dell'EDPB a tutela dei minori nell'ambiente digitale, che pure caldeggia l'adozione di sistemi di *age assurance* allo scopo di realizzare un bilanciamento tra gli obblighi derivanti dal diritto dell'Unione europea e il rispetto del GDPR[30]. In particolare, l'atto è indirizzato ai fornitori di servizi *online* (piattaforme, siti, applicazioni, operatori

[26] Regolamento (UE) 2022/2065 del Parlamento Europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali) [2022] OJ L277/1.

[27] Sul punto, la Commissione Europea ha reso disponibile un modello tecnico di verifica dell'età volto a proteggere i minori *online*. Si veda <Commission releases enhanced second version of the age-verification blueprint | Shaping Europe's digital future> ultimo accesso 18 settembre 2025.

[28] La norma dà inoltre la possibilità alla Commissione di adottare orientamenti in merito. Reg. (UE) 2022/2065, art. 28, par. 1 e 4: «I fornitori di piattaforme *online* accessibili ai minori adottano misure adeguate e proporzionate per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori sul loro servizio. […] La Commissione, previa consultazione del comitato, può emanare orientamenti per assistere i fornitori di piattaforme *online* nell'applicazione del paragrafo 1».

[29] Giova inoltre evidenziare che i progetti avviati dalla Commissione inerenti all'individuazione di meccanismi di verifica dell'età ai sensi dell'art. 28 DSA si intrecciano anche con l'esigenza dell'Unione di sviluppare soluzioni di Portafoglio europeo di Identità Digitale (PEID). La Commissione, infatti, intende vagliare la possibilità che un domani gli attributi relativi "all'età anagrafica" possano essere condivisi dall'utente europeo anche tramite il PEID, nel caso in cui i prestatori di servizi siano tenuti a verificare l'età. Da <Commission releases enhanced second version of the age-verification blueprint | Shaping Europe's digital future>: «The age verification blueprint lays the groundwork for broader deployment of age-appropriate services in the future. It is also referred to as the 'mini-wallet', as it is built on the same technical specifications as the forthcoming European Digital Identity Wallets, ensuring long-term compatibility and providing a stepping stone toward the rollout of the European Digital Identity Wallets before the end of 2026».

[30] EDPB, *Dichiarazione 1/2025 sulla garanzia dell'età* (2025) <*edpb_statement_20250211ageassurance_it.pdf*>. Il Garante europeo ha stabilito che i sistemi di *age assurance* debbano essere conformi ai principi sanciti dal GDPR, in particolare necessità, proporzionalità, minimizzazione dei dati, correttezza e trasparenza. L'implementazione deve fondarsi su un'idonea base giuridica di cui all'articolo 6 GDPR (ed eventualmente, ove rilevante, su una delle eccezioni di cui all'articolo 9, paragrafo 2), ed essere preceduta, nei casi di trattamenti ad alto rischio, dalla redazione di una valutazione d'impatto *ex* articolo 35 GDPR. È fatto divieto che l'*age assurance* si traduca in attività ulteriori rispetto alla finalità propria di verifica dell'età, quali identificazione, localizzazione o profilazione degli utenti, in violazione dei principi di limitazione della finalità e di minimizzazione del trattamento. I dati trattati devono essere limitati agli attributi strettamente necessari a dimostrare il superamento o meno di una determinata soglia anagrafica, anche attraverso soluzioni di tokenizzazione o tecniche crittografiche. Infine, i titolari e i responsabili del trattamento sono tenuti ad adottare un quadro di *governance* che assicuri la piena *accountability* ai sensi dell'articolo 5, paragrafo 2, GDPR, garantendo tracciabilità delle decisioni, la possibilità di svolgere *audit* dei processi e la possibilità di controllo da parte delle autorità competenti.

ISSN 2281-5147

digitali) che devono limitare l'accesso dei minori o offrire contenuti e servizi adeguati alla loro età. Questi, unitamente ai fornitori dei servizi di verifica dell'età (*Identity Provider*) dovrebbero limitare l'accesso a contenuti vietati o non appropriati, adottare misure specifiche contro le differenti casistiche di rischio (a titolo esemplificativo abusi, *grooming*, violenza, pornografia, etc.) e attivare sistemi di *parental control* e segnalazione.

A livello internazionale, la maggior parte delle regolamentazioni a tutela dei minori *online* suddividendo la responsabilità e l'onere della tutela del minore tra l'apparato latamente statuale, le famiglie (sovente tramite meccanismi di richiesta del consenso al genitore) e le imprese (tramite meccanismi di autoregolamentazione e previsione di obblighi di diversa natura)[31]. Nella gran parte degli scenari, il minore può, tramite meccanismi più o meno stringenti, navigare *online*, ma la sua capacità naturale o giuridica è limitata da meccanismi di acquisizione del consenso dell'esercente la responsabilità genitoriale.

In Inghilterra, è stato adottato l'*Online Safety Act* nel 2023[32], il quale prevede una serie di adempimenti precauzionali in capo ai fornitori dei servizi *online* per la valutazione dei rischi sulla base di una logica progressiva decrescente, secondo la quale più intense misure sono necessarie al diminuire dell'età del minore. I servizi interessati sono quelli che pongono in contatto gli utenti tra loro (i cd. *user-to-user services*) e i servizi di ricerca (i cd. *Search services*). Entrambi devono adottare misure proporzionate per mitigare i rischi per i bambini e proteggere le diverse fasce d'età da contenuti dannosi[33]. Sul punto, le modalità di attuazione di tali *duty of care* sono esplicitate nel Children's Code

[31] Anche la Legge sulla Protezione dei Minori della Repubblica Popolare Cinese (中华人民共和国未成年人保护法) del 17 ottobre 2020 demanda ai genitori la regolamentazione dell'utilizzo della rete e l'accesso dei minori a Internet, attribuendo tuttavia un rilevante ruolo nella formazione dei minori anche allo Stato e alle scuole. La normativa, in vigore dal 1° giugno 2021, sottolinea fortemente il ruolo dell'alfabetizzazione digitale dei minori e impone in capo allo Stato e alle famiglie il compito di prevenire il fenomeno di indipendenza da Internet. Una disciplina specifica è inoltre prevista per i fornitori di servizi *online* di gioco, i quali sono tenuti ad adottare misure per limitare l'accesso dei minori. A titolo esemplificativo, la legge prevede l'istituzione di un sistema di autenticazione elettronica dell'identità e la classificazione dei giochi offerti sulla base degli standard nazionali. I fornitori sono inoltre tenuti a fornire suggerimenti adatti all'età dell'utente e ad adottare misure tecniche per non consentire ai minori di accedere a giochi o funzioni di gioco inappropriate. Ulteriore misura prevista consiste nel vietare la fornitura ai minori di giochi *online* in capo ai fornitori dalle 22:00 alle 8:00 del giorno successivo.

[32] *Online Safety Act* 2023 del 26 ottobre 2023.

[33] Rileva in particolare il *Chapter 2* «Providers of user-to-user services: duties of care», la cui *Section* 12 dispone verso i fornitori l'obbligo di implementare politiche chiare nei termini di servizio per garantire la sicurezza dei bambini.

ISSN 2281-5147

ad opera dell'Autorità garante inglese (*Information Commissioner's Office* – più brevemente "ICO")[34]. Per limitare l'accesso ai contenuti vietati, gli operatori possono avvalersi di specifici meccanismi di verifica dell'età previsti dall'Autorità, che vanno dall'autodichiarazione all'impiego di documenti di identificazione[35]. Il Children's Code distingue poi cinque fasi di sviluppo (ad es. fase di pre-alfabetizzazione, adolescenziale etc.) in relazione ai quali gli operatori sono tenuti ad adottare diversi approcci precauzionali[36]. Sono previste regole sulla trasparenza e di limitazione delle tecniche manipolatorie. In particolare, vengono posti limiti al cosiddetto *nudge,* l'uso di tecniche per guidare o incoraggiare bambini a fornire dati personali non strettamente necessari come, ad esempio l'impiego di colori specifici per favorire associazioni mentali. È necessario adottare misure che rendano evidenti eventuali operazioni di raccolta o registrazione dei dati personali, tramite luci o segnali visivi[37].

Anche negli Stati Uniti sono previste numerose indicazioni in merito alla trasparenza. L'impianto normativo in materia si compone di due diversi atti, il *Children's Online Privacy Protection Act* del 1998, 15 U.S.C. 6501–6505 (in seguito semplicemente "COPPA Act") e il part 312— *Children's Online Privacy Protection Rule* (in seguito solo "*COPPA Rule*"). La normativa COPPA prevede una serie di obblighi per prestatori di servizi *online*, che possono essere distinti in obblighi di trasparenza e di diligenza. Ad esempio, quanto alla trasparenza, i *provider* sono tenuti a fornire un avviso riguardo alle informazioni raccolte sul minore, alle modalità con cui si domanda al genitore il

[34] Information commissioner's officer, *Children's code* (2020) <Age appropriate design: a code of practice for online services | ICO> consultato il 17 settembre 2025.

[35] Il *Children's code, Section 3,* fa riferimento a diversi metodi di verifica dell'età. Sono annoverati: l'autodichiarazione, sulla base della quale gli utenti dichiarano autonomamente la loro età senza fornire alcuna prova ulteriore; l'uso di sistemi di IA, che in base all'analisi delle interazioni dell'utente è in grado di stimare l'età; il ricorso a servizi di verifica di terze parti, le quali si impegnano a non raccogliere dati sensibili; la conferma da parte del titolare adulto avente un *account* presso lo stesso servizio; l'uso di misure tecniche che scoraggino dichiarazioni false, come il blocco automatico di *account* ripetutamente non confermati; l'uso di documenti di identificazione, che consentano di confermare l'età. L'ICO ha cura, tuttavia, di precisare che tale ultimo metodo appare sproporzionato rispetto all'esigenza di tutelare i minori, in quanto produrrebbero impatti eccessivi sulla *privacy* dell'utente.

[36] Le differenti fasce si suddividono in: 0 – 5 anni, periodo della pre-alfabetizzazione e sviluppo iniziale; 6 – 9 anni, periodo dell'apprendimento scolastico di base; 10 – 12 anni, anni di transizione; 13 – 15 anni, adolescenza iniziale; infine, 16 - 17 anni, periodo dell'avvicinamento all'età adulta. La tabella che consente di individuare le capacità cognitive dei minori per ogni fascia d'età è disponibile *online*: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/annex-b-age-and-developmental-stages/>

[37] Ad esempio, una luce che si accende quando il dispositivo sta registrando.

ISSN 2281-5147

consenso al loro impiego, il loro utilizzo e le pratiche di divulgazione[38]. I genitori devono avere la possibilità di accedere ai dati raccolti sui figli[39]. Ancora, è fatto divieto di condizionare la partecipazione a giochi o attività alla fornitura di informazioni personali non necessarie[40]. Il COPPA prevede poi la possibilità di aderire a programmi *Safe Harbour* disciplinati dal § 312.11, uno strumento di autoregolamentazione volontaria per i *provider*, proposti da gruppi industriali o soggetti privati e approvati dalla *Federal Trade Commission* (FTC) qualora garantiscano protezioni equivalenti o superiori a quelle stabilite dalla normativa[41]. Nello scenario statunitense, si precisa, il divieto di accedere[42] ai siti internet per i minori di 13 anni è strutturato come una mera possibilità per il *provider*.

Nell'opposta direzione si muove invece l'*Online Safety Act* australiano del 2021[43] che, alla Sezione 63 D, definisce come *age restricted social media platform,* ossia come

[38] Children's Online Privacy Protection Rule 16 CFR Part 312 §312.4(b): «*Direct notice to the parent.* An operator must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives direct notice of the operator's practices with regard to the collection, use, or disclosure of personal information from children, including notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented».

[39] Children's Online Privacy Protection Rule 16 CFR Part 312, § 312.6(a(1)): «Upon request of a parent whose child has provided personal information to a website or online service, the operator of that website or online service is required to provide to that parent the following: A description of the specific types or categories of personal information collected from children by the operator, such as name, address, telephone number, email address, hobbies, and extracurricular activities».

[40] Children's Online Privacy Protection Rule 16 CFR Part 312, §312.7: «An operator is prohibited from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity».

[41] Alcuni dei progetti attualmente in corso sono reperibili al seguente link <https://www.ftc.gov/enforcement/coppa-safe-harbor-program> ultimo accesso: 14 marzo 2025.

[42] L'indicazione è reperibile tra le FAQ del COPPA: «Can I block children under 13 from my general audience website or online service? Yes. COPPA does not *require* you to permit children under age 13 to participate in your general audience website or online service, and you may block children from participating if you so choose. By contrast, you may not block children from participating in a website or online service that is directed to children as defined by the Rule, even if the website or online service is also directed to users age 13 or older».

[43] Online Safety Act 2021, come modificato da Act No. 127, 2024. L'Online Safety Act 2021 (OSA) intende assicurare che Internet rimanga uno spazio sicuro intervenendo secondo due linee di azione: la prima consiste nell'attribuire ampi poteri di controllo all'Autorità garante australiana (*eSafety Commissioner*), la quale assume un ruolo attivo nei rapporti tra i prestatori di servizi *online* e gli utenti; la seconda consiste nell'individuare le cd. "Expectations" nei confronti dei prestatori di servizi per garantire un ambiente digitale sicuro (*Part 4 – Basic online safety expectations*), senza tuttavia entrare nello specifico delle modalità con le quali tali "Expectations" possono essere raggiunte. Con riferimento alla prima linea di azione, ai sensi del *Part 3 – Complaints, objections and investigations, Division 1- Introduction, No. 29* ss., i minori possono rivolgersi direttamente al *Commissioner* lamentando episodi di cyberbullismo o segnalando contenuti a loro vietati. Il *Commissioner* può, a sua volta, ai sensi del *Part 5, No 65* e *No. 109,* emettere un avviso di rimozione al fornitore di *social media* qualora l'oggetto dei contenuti sia stato accertato essere in violazione dell'OSA; inoltre, ai sensi del *No. 49* e *No. 56,* può richiedere ai prestatori un "*periodic reporting notice*" sullo stato di conformità alle cd. "Expectations". Sono infine previsti

ISSN 2281-5147

piattaforme *online* vietate ai minori di 16 anni[44], quei servizi elettronici[45] che consentono l'interazione tra due o più utenti o che consentono di caricare materiali *online*[46]. Il divieto in esame è di natura sostanziale. In altre parole, a differenza di

ulteriori poteri per il controllo della compliance e monitoraggio (*Part 10 -Enforcement)*. Con riferimento alla seconda linea d'azione, il legislatore australiano prevede gli obiettivi che i prestatori devono raggiungere per garantire un ambiente digitale sicuro (*Part 4, Division 2 – Basic online safety expectations, No. 46 Core Expectations*), delegando ai codici di condotta la definizione delle modalità tecniche ed organizzative per raggiungerli. La *Part 9 – Online content scheme* definisce comunque uno schema minimo che tali codici di condotta devono seguire, specificando i contenuti vietati ai minori di diciotto anni (*No. 106 – 107*) e fornendo esempi di "argomenti" da disciplinare nei codici. A titolo esemplificativo, la *Subdivision B—General principles relating to industry codes and industry standards, No. 138 "Examples of matters that may be dealt with by industry codes and industry standards"* prevede che i codici di condotta debbano individuare le procedure atte sia ad assicurare che gli account *online* non possano essere creati dai minori senza il consenso dei genitori sia a fornire ai genitori informazioni circa i modi e gli strumenti con cui possono monitorare o controllare l'attività dei propri figli sui loro servizi. Anche nella redazione di tali codici di condotta si prevede un diretto coinvolgimento del *Commissioner*, che può aggiornare gli indirizzi degli standard tecnici ed organizzativi da adottare, gli ambiti nei quali i codici devono intervenire, ed organizzare delle consultazioni pubbliche al fine di agevolare la stesura dei codici di condotta (*Part 9, Division 7, Subdivision C – E*). L'approccio che traspare è di mantenere la sfera d'azione pubblica separata dalla sfera d'azione privata. In altre parole, il legislatore australiano dell'OSA 2021 non intende obbligare in concreto il prestatore a determinati "comportamenti" nella prestazione del suo servizio, limitandosi piuttosto a fissare i risultati che i prestatori di servizi devono raggiungere attraverso proprie scelte d'azione.

[44] Giova precisare che la *Part4A - Social media minimum age*, adottata il 2 dicembre 2024 con l'*Act No. 127, 2024* e in vigore a partire dal 10 dicembre 2025, è l'unica parte del testo normativo australiano che impone direttamente l'obbligo a determinati prestatori di vietare l'accesso ai loro servizi ai minori di 16 anni. In tale contesto normativo si inseriscono inoltre le eSafety Commissioner, *Basic Online Safety Expectations* (2024) in <Federal Register of Legislation - Online Safety (Basic Online Safety Expectations) Determination 2022> ultimo accesso 14 febbraio 2025. "*The Expectations"* integrano l'OSA attraverso l'individuazione più specifica di misure standard minime che i fornitori di servizi devono assicurare per il raggiungimento dei risultati previsti dalla *Part 4* OSA.

[45] La normativa si concentra sui *social network*, ma al contempo prevede norme specifiche qualora siano impiegati sistemi di IA. Nella *Division 2 – Basic Online safety expectations, Section 8A "Additional expectations—provider will take reasonable steps regarding generative artificial intelligence capabilities* vi è espresso rimando all'adozione di misure in grado di consentire solo un utilizzo sicuro di IA generativa per tutti. Tuttavia, mentre a Settembre 2024, il *Commissioner* australiano ha formalmente richiesto a YouTube, Facebook, Instagram, TikTok, Snap, Reddit, Discord e Twitch di indicare quali meccanismi di *age assurance* avessero adottato, nessuna richiesta in tal senso è stata avanzata nei confronti di fornitori di sistemi di IA. In eSafetyCommissioner, *eSafety calls on social media giants to reveal just how many Aussie kids are signing up* (2024) <eSafety calls on social media giants to reveal just how many Aussie kids are signing up | eSafety Commissioner> consultato il 14 febbraio 2025.

[46] Specificamente, le piattaforme che vi rientrano sono: «(a) an electronic service that satisfies the following conditions: (i) the sole purpose, or a significant purpose, of the service is to enable online social interaction between 2 or more end users; (ii) the service allows end users to link to, or interact with, some or all of the other end users; (iii) the service allows end users to post material on the service; (iv) such other conditions (if any) as are set out in the legislative rules; OR (b) an electronic service specified in the legislative rules but does not include a service mentioned in subsection. For the purposes of subparagraph (1)(a)(i), online social interaction includes online interaction that enables end-users to share material for social purposes». È inoltre previsto che il *provider* di tali piattaforme non possa raccogliere strumenti identificativi emessi dallo Stato australiano né utilizzare servizi di accreditamento previsti dal Digital IA Act del 2024. Cfr. OSA, s(63DB): «A provider of an age restricted social media platform must not: (a) collect government issued identification material; or (b) use an accredited service (within the meaning of the Digital ID Act 2024); for the purpose of complying with section 63D, or for purposes that include the purpose of complying with section 63D». In altre parole, la piattaforma non può avvalersi né delle carte di identità rilasciate nell'ambito del Commonwealth, né

ISSN 2281-5147

quanto prevede l'art. 8 del GDPR o, seppur in maniera graduata, la normativa britannica, il legislatore australiano non si limita ad imporre il rispetto di regole in materia di accesso, capacità giuridica o moderazione dei contenuti, bensì vieta in modo radicale l'impiego di tali piattaforme ai minori di 16 anni. La responsabilità non è in questo caso allocata in capo al genitore, ma vi è una chiara scelta di politica legislativa che riconosce a priori la rischiosità dell'impiego dei *social media*.

5. La recente legge italiana sull'impiego degli strumenti di IA

Nello scenario italiano, il tema della tutela del minore è stato recentemente oggetto di specifica normazione. A differenza di quanto è avvenuto in Australia con riferimento alla limitazione dell'uso dei *social network*, ove il legislatore ha scelto di imporre un limite di natura sostanziale con riferimento allo specifico servizio, la legge del 23 settembre 2025, n. 132 (Legge sull'IA) ha adottato un approccio più mediato, che appare ispirato dall'art. 8 del GDPR. L'art. 4 della Legge sull'IA, astenendosi da valutazioni circa la rischiosità del mezzo, prevede infatti che «l'accesso alle tecnologie di intelligenza artificiale dei minori di anni quattordici richied[a] il consenso di chi esercita la responsabilità genitoriale»[47]. Tale formulazione sembra poter includere l'accesso ai sistemi di IA tramite ogni tipo di piattaforma o fornitore, privilegiando la

utilizzare servizi di identità digitale. La Sezione 63DB, *Use of certain identification material and services*, prevede infatti che per «government issued identification material» sia da intendersi «identification documents issued by the Commonwealth, a State or a Territory, or by an authority or agency of the Commonwealth, a State or a Territory (including copies of such documents); and (b) a digital ID (within the meaning of the Digital ID Act 2024) issued by the Commonwealth, a State or a Territory, or by an authority or agency of the Commonwealth, a State or a Territory». È inoltre previsto dalla *Section 63DA* che il Ministero per le Comunicazioni possa individuare con propri provvedimenti quali informazioni le *social media platform* non devono raccogliere per assolvere all'obbligo.

[47] Cfr. L. 132/2025, art. 4 c. 4: «L'accesso alle tecnologie di intelligenza artificiale da parte dei minori di anni quattordici nonché il conseguente trattamento dei dati personali richiedono il consenso di chi esercita la responsabilità genitoriale, nel rispetto di quanto previsto dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e dal codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196. Il minore di anni diciotto, che abbia compiuto quattordici anni, può esprimere il proprio consenso per il trattamento dei dati personali connessi all'utilizzo di sistemi di intelligenza artificiale, purché le informazioni e le comunicazioni di cui al comma 3 siano facilmente accessibili e comprensibili». Sempre nello scenario europeo, lo Stato del Vaticano ha adottato con Decreto n. DCCII le *Linee guida in materia di intelligenza artificiale* (2024) <*Linee guida in materia di intelligenza artificiale del Governatorato dello Stato della Città del Vaticano*> ultimo accesso: 17 settembre 2025. Pur non entrando nell'ambito della tutela dei minori, le linee guida intendono promuovere uno sviluppo ed uno utilizzo di sistemi di IA in ottica antropocentrica, con ciò adeguandosi alla direzione intrapresa dal legislatore europeo. Sebbene con formulazione differente, sono infatti presenti sia gli stessi divieti disposti dall'art. 5 AI Act sia l'obbligo di rispettare i principi di trattamento dei dati personali nell'ambito dello sviluppo ed utilizzo del sistema di IA.

ISSN 2281-5147

natura particolare del minore e la sua fragilità. La scelta circa l'idoneità del servizio o del prodotto dotato di IA è dunque rimessa in primo luogo al *provider* che lo renda disponibile sul mercato. Qualora il servizio non fosse dichiaratamente ritenuto adeguato al minore infraquattordicenne, sarebbe poi il genitore o l'esercente la responsabilità a poter rendere il consenso al suo utilizzo. Da ultimo si osserva che, come è avvenuto per l'art. 8 GDPR nei provvedimenti sopra richiamati, l'onere di consentire l'applicazione in concreto della disposizione ricadrà (in una misura che occorrerà determinare) sul *provider* che (in modo autonomo o tramite un *Identity Provider*) predisporrà il sistema di riconoscimento del genitore o, in ottica di minimizzazione, di *age verification* del minore, prima, e dell'esercente la responsabilità genitoriale poi.

Quanto all'effettività della previsione, il ruolo degli *Identity Provider* è evidentemente cruciale e, nello scenario italiano, è già stato declinato con riferimento ad uno specifico settore nella delibera dell'AGCOM 96/25/CONS [48] di attuazione dell'art. 13-*bis* del Decreto Caivano[49]. Si tratta della norma che impone ai fornitori di piattaforme che diffondono in Italia «immagini e video a carattere pornografico» di verificare la maggiore età degli utenti, allo scopo di «evitare l'accesso a contenuti pornografici da parte di minori degli anni diciotto». La delibera dell'AGCOM ha un contenuto del tutto specifico e settorialmente indirizzato, in quanto contiene obblighi diretti ai soggetti che diffondono in Italia contenuti pornografici. Tuttavia, in relazione alla corrente analisi, pare utile evidenziare le osservazioni formulate dall'Autorità in merito alle soluzioni tecniche per la limitazione dell'accesso ai servizi citati, in quanto appaiono potenzialmente rilevanti ogniqualvolta ci si accinga ad imporre un sistema di *age limitation* in relazione ad un servizio, sia questo quello del *social network* o quello

[48] AGCOM, *Delibera 96/25/CONS: adozione delle modalità tecniche e di processo per l'accertamento della maggiore età degli utenti in attuazione della legge del 13 novembre 2023, n. 159* (2025) <delibera 96-25-CONS.pdf> ultimo accesso 17 settembre 2025: «In via di premessa, è importante sottolineare che la Commissione ha condiviso l'obiettivo perseguito da Agcom attraverso il progetto notificato inteso a proteggere i minori *online*, in particolare dai contenuti a carattere pornografico, che possono nuocere alla loro salute e al loro sviluppo fisico, mentale e morale. Si tratta, infatti, di obiettivi allineati a quelli del quadro giuridico europeo per i servizi online, in particolare il regolamento (UE) 2022/2065 (di seguito il «regolamento sui servizi digitali o DSA) e la direttiva 2000/31/CE (direttiva sul commercio elettronico)».

[49] D.l. 15 settembre 2023, n. 123, art. 13-*bis*: «I gestori di siti web e i fornitori delle piattaforme di condivisione video, che diffondono in Italia immagini e video a carattere pornografico, sono tenuti a verificare la maggiore età degli utenti, al fine di evitare l'accesso a contenuti pornografici da parte di minori degli anni diciotto. […] L'Autorità per le garanzie nelle comunicazioni stabilisce, […] con proprio provvedimento, sentito il Garante per la protezione dei dati personali, le modalità tecniche e di processo che i soggetti di cui al comma 2 sono tenuti ad adottare per l'accertamento della maggiore età degli utenti».

ISSN 2281-5147

connesso all'impiego di un sistema dotato di intelligenza artificiale. Pur non imponendo univoche soluzioni tecnologiche, l'AGCOM ha rilevato rischi trasversali connessi alla previsione di *age gate,* raccomandando che a procedere alla verifica dell'età siano soggetti terzi rispetto al gestore del servizio e scoraggiando i prestatori dall'avvalersi di meccanismi interni per la verifica dell'età[50]. Si tratta del sistema del "doppio anonimato", secondo il quale da un lato i dati personali dell'utente devono essere tutelati nei confronti della piattaforma che offre il servizio e, dall'altro, i siti visitati non possono essere conosciuti dall'*Identity Provider*. Da ultimo, non può non evidenziarsi come nella delibera emerga altresì la valutazione dell'Autorità sull'efficacia della soluzione tecnica proposta: nessuno dei sistemi di *age verification* è considerato completamente sicuro rispetto a meccanismi elusivi da parte degli utenti[51].

[50] L'Autorità non esclude, poi, che tale verifica potrà essere soddisfatta, a partire dal 2026, anche con il PEID. Infatti, i nuovi *digital wallet* potranno essere in grado di condividere anche solo l'attributo dell'età anagrafica con i prestatori di servizi, senza per ciò stesso rivelare l'identità dell'utente. Cfr. Allegato B) alla delibera n. 96/25/CONS cit., 14: «Nella maggior parte dei casi, i cittadini non possono scambiare digitalmente a livello transfrontaliero, in modo sicuro e con un livello elevato di protezione dei dati, informazioni relative alla loro identità quali indirizzi, età e qualifiche professionali, patenti di guida e altri permessi e dati di pagamento. Pertanto, l'*EUDI wallet* consentirebbe di superare tali limiti offrendo la possibilità di scambiare attributi minimi dell'identità necessari ad accedere determinati servizi online per cui è richiesta l'autenticazione, come ad esempio la prova dell'età. Inoltre, il nuovo Regolamento eIDAS prevede che, qualora le piattaforme online di dimensioni molto grandi, come definite dal DSA, impongano agli utenti di autenticarsi per accedere ai servizi online, queste dovranno accettare anche l'uso dei portafogli europei di identità digitale, rigorosamente su richiesta volontaria dell'utente, anche per quanto riguarda gli attributi minimi necessari per lo specifico servizio online per il quale è richiesta l'autenticazione, come la prova dell'età». L'allegato riporta anche il rapporto del regolatore inglese OFCOM, che si è espresso in relazione all'*Online Safety Act*. L'autorità inglese ha ritenuto che la verifica dell'età tramite PEID sia altamente efficace. L'AGCOM non ritiene, invece, che lo SPID possa considerarsi una soluzione ottimale, almeno fino a quando i relativi prestatori avranno accesso alle informazioni circa i siti visitati dagli utenti che richiedono l'identificazione. Cfr. Allegato A), Delibera 96/25/CONS, cit., 4-5: «[…] tale sistema di autenticazione SPID consente all'*Identity Provider* di conoscere il particolare sito/piattaforma visitato dall'utente e non è da escludere che tale informazione venga memorizzata all'interno dei sistemi dell'Identity Provider. […] Si evidenzia, pertanto, la possibilità, con un sistema pubblico, di poter disporre in breve tempo di un insieme di Identity Provider certificati e di una rete di connessioni e accordi (basati su obblighi normativi esistenti), in grado di fornire, all'utente e per il tramite di questo alla piattaforma, la cosiddetta prova dell'età. Quanto detto vale sia per la modalità di verifica dell'età collegate a sistemi di verifica dell'età non basati su applicativi installati nel terminale utente sia per quelli basati su applicativi installati nel terminale utente (cosiddetti *digital wallet*), fermo restando la necessità di preservare la libertà di scelta dell'utente in merito all'utilizzo di uno o dell'altro sistema, anche considerando la potenziale invasività dell'installazione di determinate app sul proprio dispositivo personale. L'Autorità, pertanto, solo laddove soddisfatti i requisiti di cui alla sezione seguente sul doppio anonimato (protezione dei dati personali nei confronti del sito/piattaforma e non conoscenza del sito visitato/piattaforma da parte dell'Identity Provider), ritiene che sistemi pubblici siano utilizzabili».

[51] Allegato A), Delibera 96/25/CONS, cit., 10: «Per quanto riguarda i dispositivi attualmente offerti sul mercato, diversi regolatori evidenziano che attualmente tutte le soluzioni proposte possono essere in qualche modo aggirate. Ad esempio, l'utilizzo di una VPN, che nasce per garantire sicurezza nell'utilizzo di Internet agli utenti,

ISSN 2281-5147

6. Considerazioni conclusive: verso un approccio trasversale alla tutela del minore *online*?

Le soluzioni normative esaminate in materia di tutela del minore *online*, sia che questo utilizzi sistemi di intelligenza artificiale, *social network* o che semplicemente coincida con il soggetto interessato del trattamento dei dati personali, possono essere raggruppate per metodologie. Mentre Stati Uniti e Regno Unito hanno adottato approcci basati rispettivamente sulla co-regolamentazione e sulla valutazione del rischio, senza prevedere specifici divieti, l'Australia ha introdotto un divieto sostanziale in merito all'uso dei *social network* ai minori di sedici anni. L'Italia e l'Europa sembrano aver adottato una posizione intermedia. L'art. 28 del DSA impone un obbligo sui prestatori di servizi *online* di garantire «un elevato livello di tutela» per il minore. Con riferimento all'accesso agli strumenti dotati di intelligenza artificiale, nel solo scenario italiano, è da ultimo stato attribuito al soggetto esercente la responsabilità genitoriale il compito di acconsentire a che il minore vi sia esposto, mentre è allocata sul *provider* la responsabilità di implementare un sistema di verifica[52] della provenienza del consenso dal soggetto legittimato ad esprimerlo o di verifica dell'età del minore *tout court*. Appare corretto l'approccio del legislatore europeo (e italiano) nell'astenersi dall'individuare un metodo specifico per lo svolgimento dell'*age verification*, dimostrando di intendere che di una rincorsa tra metodi di verifica e sviluppo tecnologico potrebbe trattarsi in concreto.

In ognuno dei casi qui richiamati, però, l'efficacia in concreto delle norme che si pongono l'obiettivo di limitare l'accesso agli strumenti dotati di intelligenza artificiale, ai *social network* o al trattamento dei dati personali *online*, è subordinata alla possibilità tecnica di aggirare il divieto. Come anticipato, l'AGCOM conferma che tutte le soluzioni tecniche per garantire la sicurezza dei processi di *age verification* esaminate nella Delibera 26/95/CONS. si prestano, ad oggi, a meccanismi elusivi mediante l'uso di VPN da parte degli utenti. A ben vedere, la medesima conseguenza è trasversale a

può allo stesso tempo consentire a un minore di eludere un sistema di verifica dell'età. Il soggetto tenuto, ai sensi della legge, a realizzare il sistema di controllo dell'età per l'accesso ai contenuti, non deve promuovere o fare comunque riferimento a qualsiasi meccanismo di elusione dei sistemi di age *assurance*».

[52] Già oggi obbligatoriamente basato sul sistema del doppio anonimato per quanto concerne il ristretto ambito di applicazione della Delibera 96/25/CONS.

ISSN 2281-5147

tutti i sistemi normativi esaminati, sia nel caso in cui non sia previsto alcun limite di utilizzo per i minori (quando questo venga ad esempio imposto dal *provider*), sia nel caso in cui vi sia l'imposizione di un divieto assoluto di utilizzo (come nel caso australiano), sia nel caso in cui la scelta circa la possibilità di accedere al servizio venga affidata al consenso del genitore (come prevedono la legge italiana ed il GDPR). In ognuna delle situazioni richiamate, il minore che voglia aggirare il divieto si scontrerà con le misure di sicurezza adottate dal fornitore del servizio e, a seconda dell'ordinamento, dall'*Identity Provider*.

Ne consegue la necessità di approcciare la questione della tutela del minore non solo dal punto di vista legislativo e prescrittivo, ma anche a livello culturale, includendo nel dialogo non solo i legislatori ma gli stessi *provider*. Ad accrescere il livello generale di consapevolezza dei consociati circa i rischi connesso all'utilizzo dell'IA *online*, accentuati dall'intrinseca fragilità del minore, possono contribuire alcuni strumenti, già evidenziati nei provvedimenti esaminati, quali le tecniche anti *nudge*, i processi di co-regolamentazione con gli stessi fornitori e, pur con i limiti già emersi negli studi in materia di protezione dei dati personali, i sistemi di notifica informativa (si pensi al provvedimento Tik Tok). Tuttavia, una riflessione di carattere culturale sui rischi per i minori che utilizzino strumenti di IA, non può prescindere dal considerare, al contempo, i rischi impliciti e connessi all'accesso e all'impiego di questi strumenti *online*. Dati i numerosi livelli di sovrapposizione che possono esistere tra le attività svolte dai minori sui *social media*, quando accedono a strumenti dotati di intelligenza artificiale e quando divengono interessati del trattamento dei dati personali, oltre a regole puntuali nei differenti settori di interesse sembra utile prendere in considerazione una visione più ampia, quella del minore, soggetto vulnerabile, che agisce *online*. L'esame dei rimedi emersi nei differenti ordinamenti sia a livello normativo (emergono gradualmente limiti di età e divieti d'accesso) sia provvedimentale (i rischi rilevati nell'esame di casistiche apparentemente dissimili appaiono i medesimi) ha infatti posto in luce come, in tutti gli scenari esaminati, il rischio evidenziato e la relativa misura correttiva siano direttamente collegati al momento in cui il minore accede al servizio che, in molti casi, coincide con la possibilità per questi di accedere *online*. A prescindere dal settore, deve dunque emergere la consapevolezza che la vulnerabilità del minore è descritta in relazione a rischi condivisi (in modo più o meno acuto a seconda della specifica tipologia dello

ISSN 2281-5147

strumento o dei servizi utilizzati) quando questi accede alla rete, luogo di amplificazione dei diritti, ma anche delle vulnerabilità.

ISSN 2281-5147