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.

Table of Contents

Keywords

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

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.

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.

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.

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.

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.

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.

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

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-

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.

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.

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.

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/.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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*".

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.

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.

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/.

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.

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.

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.*

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 conduct 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.

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.

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

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.

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.

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.

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*".

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

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.

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.

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).

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.

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.

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.

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.

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.

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*).

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

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.

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.

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.

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.

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

the complexity at hand and to transform it into an opportunity for shared growth and care.