Recent Policy Initiatives and Safeguards for Children as Online Users

DENISE AMRAM - NICOLETTA PATTI*, LIDER Lab, Dirpolis Institute, Scuola Superiore Sant'Anna, Italy

This is an extended abstract for the Designing for Children's Rights and Digital Wellbeing: An Agenda for Research and Practice Workshop at ACM International Design and Children Conference, IDCD 2024 at TU Delft, Netherlands. It includes an assessment of existing law and policy initiatives approaching the technical and organisational measures to protect children as online users.

Additional Key Words and Phrases: Children, online users, protection, safeguards

ACM Reference Format:
Denise Amram - Nicoletta Patti. 2024. Recent Policy Initiatives and Safeguards for Children as Online Users. 1, 1 (May 2024), 4 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Children are considered vulnerable subjects due to their lack of psychophysical maturity, which results in a legal incapacity. The UN Convention on the Rights of the Child [1] protects and promotes minors under the age of eighteen, establishing - as known - that States must introduce measures to pursue their best interests in any process that may concern them. In particular, Article 19 CRC establishes an obligation for signatory States to adopt all legislative, administrative, social, and educational measures to prevent any form of physical or mental violence, injury or abuse, neglect or negligent treatment, mistreatment or exploitation, including sexual abuse. The current challenge is therefore to ensure the implementation of this principle even in the digital environment, considering children's exposure to phenomena such as cyberbullying, grooming, and sexting, which fall under the hypotheses provided for in the mentioned Article 19. However, the introduction of control and monitoring systems does not appear to be an effective solution to prevent the occurrence of the mentioned risks. Furthermore, interventions must be balanced with the principle expressed in Article 16 CRC, which states the prohibition of arbitrary or unlawful interference with the privacy, family life, home, correspondence of minors.

*Both authors contributed equally to this research. Research funded under PRIN 2022 MUR Project Children as vulnerable users of iot and ai-based technologies: a multi-level interdisciplinary assessment (CURA), 2022KAEWYF and Horizon Europe Reviving, Boosting, Optimising and Transforming European film competitiveness (REBOOT) GA 101094796

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

Author's address: Denise Amram - Nicoletta Patti, denise.amram@santannapisa.it, LIDER Lab, Dirpolis Institute, Scuola Superiore Sant'Anna, Pisa , Italy.

ACM XXXX-XXXX/2024/5-ART
https://doi.org/10.1145/nnnnnnn.nnnnnnn

2 CHILDREN'S RIGHTS AND DATA PROTECTION

Recently, both the Council of Europe and the European Commission have launched strategies on children's rights [2], including specific safeguards aimed at digitization and the use of artificial intelligence, to define conditions for a safe and resilient digital environment accessible to minors through the promotion of safeguard measures by service providers, parents, healthcare professionals, and all stakeholders. The legislation on the European data strategy aims - through a plurality of initiatives - to establish rules to ensure the free and safe circulation of data flows to promote innovation and the potential of the information society in every domain. It is therefore necessary to understand how sector-related regulations are aligned with children's rights and to understand the role that the identification of risks and vulnerabilities for minors plays in the current legislative debates. The EU General Data Protection Regulation EU Reg. N. 2016/679 (hereinafter "GDPR"), indeed, plays a pioneering role for two reasons. Firstly, it constitutes an example of personal data protection by including a stakeholder-oriented approach based on risks and aimed at continuously assessing the impact of each component of data processing (i.e., means, purposes, nature of data, subjects, technology adopted). Secondly, Article 8 GDPR is refers to minors' consent to the processing of data online, opening up new interpretations of the balance between formal legal age and the actual maturity of young users. Under this provision, in fact, a child under the age of sixteen can consent to the processing of her data for information society services, and Member States can even introduce a lower age threshold [3].

3 LEGAL POLICIES IN EU AND BEYOND

In the digital dimension, children's vulnerability appears mitigated due to the daily use of information society services as well as fueled by exposure to impactful risks to the child's well-being in terms of seriousness and probability of occurrence, as well as evidence of critical issues not yet entirely foreseeable or measurable. In this regard, we may provide the example of the future consequences of a child's identity theft: it is not certain that the effects will be produced immediately or be perceptible to the child or its family, and it is unclear to what extent there might be implications in the future [4]. In this context, protecting the fundamental rights of minors in the digital dimension is far from being easily to address: for some policy-making initiatives, it seems possible only through a defensive attitude aimed at limiting and/or prohibiting the use of technology to avoid the occurrence of risk; for other ones, it is about identifying who should be burdened with assessing the impact of risks case by

[2]For details on the strategy launched by the European Commission, EU Strategy on the Rights of the Child and the European Child Guarantee and for the one launched by the Council of Europe, Strategy for the Rights of the Child (2022-2027), https://www.coe.int/en/web/children/strategy-for-the-rights-of-the-child
[3]D. Amram, Children (in the digital environment), in G. Comandé (ed.), Elgar Encyclopedia of Law and Data Science, 2022, 64 s.
[4]For a more in-depth see the contributions included in the volume C. Crea, A. De Franceschi (eds.), Digital Vulnerability in European Private Law, being published in Nomos, 2024

case and, consequently, who should introduce mitigation measures and mechanisms. In terms of legal policy, it is interesting to analyze different legislative initiatives also outside the EU, in order to better understand emerging solutions and approaches to a global issue.

3.1 Examining International Perspectives

Starting with initiatives taken outside the European context, a relevant case is that of Florida. Here, in line with the 'defensive' approach, a bill is under consideration that would prohibit access to social networks by minors under the age of seventeen, with some corrections aimed at making adults responsible for minor users [5]. This initiative is in line with what has already been approved in Utah [6], which prohibits opening accounts for subjects under the age of eighteen residing in the State, except with the consent of the parent/guardian, providing for a fourteen-day account verification period, also requiring digital service providers to introduce appropriate methods of verification and identification of the profile users, not limited to the presentation of the ID card, as it is considered easily circumvented by minors themselves. The legislation also prohibits the use of social media at night and sets a maximum number of hours online; however, parents/guardians have the possibility to modify the settings, thus extending the autonomy of the minor, where specific conditions are recurring. The technical-organizational measures suitable to protect minors represented in the mentioned legislative initiatives appear aimed at confirming a proactive role of parents to ensure that they are aware of the registration of underage children on certain platforms, the duration of online presence, limiting the managerial autonomy of activities in the digital dimension in the absence of adults' validation. This perspective assumes particular relevance in terms of parental responsibility, setting standards of care that could, however, be called into question in the specific case. Possible conflicts between parents may arise, for instance, in case of restrictions the reduction/elimination of predefined blocks, or of the scope of decisions taken by the parent in the event of exposure to a risk, which then actually occurs in the digital sphere, and the consequent need to ascertain liabilities even of the service provider. Similarly, conflicts may arise between the adolescent and the inhibiting position of the parent and, in these cases, the judge will be required to interpret which solution pursues the best interests of the child in the specific matter.

3.2 The EU Approach

Conversely, in Europe, with the exception of sporadic features implemented on specific applications, which allow the parent to intervene in platform settings, there is no obligation to control content or monitor access to online platforms once an account has been created by the parent (or with their consent). The approach of the European legislator seems more inclined to trust in cultural change : the allocation of roles and responsibilities to providers of digital services in the context of impact assessments regarding the fundamental rights of children constitutes the key to establishing conditions for a safe and reliable digital environment, as it emerges from the recent EU Regulation No. 2022/2065 on the Digital Services Act (hereinafter DSA) . Therefore, an attentive by design approach that includes the well-being and safety of adolescents in the operation of digital and AI-based technologies characterizes the EU paradigm of responsibilities in Europe. Services intermediaries must take into account the vulnerabilities of underage users, proceeding, for example, to first assess their impact, then implementing suitable measures to mitigate the negative consequences, under articles 34-35 DSA, or to explain in a comprehensible manner for minors the conditions and restrictions that apply to the use of the service itself pursuant to article 12 DSA, or to proceed with the identification and implementation of measures to protect minors online, pursuant to article 44 DSA. Article 28 DSA, in particular, states that online platforms that are accessible to minors must adopt appropriate and proportionate measures to ensure a high level of protection of privacy and security, inhibiting - for example - profiling-based advertising interfaces. The scope of application of the legislation on digital services concerns, in fact, the definition of conditions for the development of a safe, predictable, and reliable online environment regarding the dissemination of illegal, discriminatory, or otherwise non-inclusive content, introducing transparency obligations also regarding profiling activities for advertising purposes. The architecture of the DSA is therefore linked to the protection of the individual as a consumer user of digital services. This is complementary to the more general protection of privacy regulated by the GDPR. The evolution of sensitivity between the two regulations reflects also the statistical data that reserves a significant online presence for minors aged between 11 and 16 [7].

3.3 The UK Approach towards Digital Literacy

In this context, in the realm of digital governance, one such notable initiative is the "Age-Appropriate Design Code," also referred to as the Children's Code, enacted in the United Kingdom in 2020 . Spearheaded by the Information Commissioner's Office (ICO), this code is principally directed at information service providers overseeing data for online platforms such as apps, games, and social media, which are deemed 'likely' to be applied by minors. The fundamental objective of this code is to ensure that these digital interfaces are meticulously crafted, taking into account the different age groups and specific developmental needs of children [8]. Platforms targeting these demographics are mandated to incorporate proactive measures, aligning with the delineated standards within the code. These measures encompass comprehensive mapping of personal data sourced from children in the UK, discerning the age demographics of platform visitors and users, disabling geolocation services, not using nudge techniques and implementing stringent privacy protocols as the default setting. Furthermore, service providers are required to prioritize the best interests of children during product development and ensure that privacy policies are articulated in a lucid and understandable manner for their comprehension. Concurrently, alongside

[5] An act relating to social media use for minors; creating s. 501.1736, F.S. https://custom.statenet.com/public/resources.cgi?id=ID:bill:FL2024000H1ciq=urn:user:PA679253Applicat...d=2635336eb5ea69fb2ddc58b26c7a72ecmode = current_text

[6] https://le.utah.gov/ 2023/bills/static/SB0152.html

[7] S. Livingstone, One in three: Internet Governance and Children's Rights, 2016, UNICEF report

[8] M. Comite, Prevent Phishy Business: Comparing California's and the United Kingdom's Age-Appropriate Design Code to Protect Youth from Cybersecurity Threats in U Miami Int'l Comp L Rev, 31, 2023, 175-200; E. Lampmann-Shaver, Privacy's next Act, in Washington Journal of Law, Technology Arts, vol. 19, 1, 2024, 97-129

the onus placed on service providers, there exists a pressing need for institutional initiatives aimed at fostering digital literacy, not only among the youth but also, critically, among adults. ICO has taken proactive strides in this direction by promoting awareness campaigns targeting a diverse spectrum of professionals, extending even beyond those directly involved in managing children's data, such as executives and managers with key responsibilities in organisations, their advisors, those working or volunteering in local organisations, like youth groups, arts groups or sports teams, including the social sector, civil servants, etc [9]. In this way, ICO promotes a 'child-friendly' digital culture in all spheres and not only with regard to services closer to children. From this point of view, therefore, the challenge of societal responsibility for cultural change to pay attention to the vulnerabilities of children - as potential users - constitutes a virtuous practice that implements inclusive strategies for present and future society.

4 LARGE PLATFORMS RECENT INITIATIVES

Operationalizing these principles at a pragmatic level, observable trends emerge on platforms predominantly frequented by adolescents [10]. When young individuals engage with such platforms, they frequently agree to the terms of service, privacy policies, and data protection measures. This is primarily due to their lack of digital literacy, demonstrated by their limited grasp of the privacy risks linked with social media[11]. It is therefore imperative for platforms to adopt measures to protect minors who use or produce content online, while it becomes increasingly crucial to promote digital literacy among both minors and adults. To illustrate the application of these principles (the management of children's data, measures taken to protect their interests and rights, platform design and models, and parental support) we have chosen to examine two case studies: TikTok, which ranks among the platforms preferred by children (see section 4.1), and WhatsApp, which has recently made changes to its terms of service (see section 4.2).

4.1 TikTok: A Case Study on Child Safety Initiatives

The mounting concern over the significant national security risks associated with TikTok, as emphasized by recent discussions, particularly centers on the data collection practices of the Chinese company ByteDance and its profound influence on user behavior. These practices have raised substantial concerns, especially in the United States, which is becoming increasingly wary of China's ascent as a geopolitical rival wielding extensive control over the technology sector [12]. However, the issues extend beyond national security, encompassing broader regulatory challenges related to social media use, of which TikTok constitutes a pertinent case study given its pervasive adoption among young people. These challenges include their negative impact on mental health, the spread of misinformation, and the erosion of privacy, particularly concerning vulnerable demographic groups such as children. Platforms like TikTok have come under scrutiny for fostering harmful behaviors among underage users, including grooming, sexting, and harassment [13]. In response to these pressing concerns, TikTok has undertaken measures aimed at safeguarding underage users. These include implementing stringent privacy settings and robust content moderation policies. For instance, TikTok now defaults the accounts of children under 16 to private, restricts access to certain features for underage users, and prohibits direct messaging for users under 16. Additionally, TikTok has instituted comprehensive policies such as restricting video visibility to approved followers, banning advertising directly targeting minors below the digital age of consent, and preventing the downloading of videos created by minors under 16 by generic users. Despite these proactive efforts, lingering doubts persist regarding the efficacy of these measures and the platform's capacity to effectively shield young users from potential harm. In this context, the European Union emerges as a vanguard in social media regulation, spearheaded by landmark legislations such as the GDPR and the DSA. These regulatory frameworks furnish exhaustive provisions for data protection and content moderation, fortifying the privacy and security apparatus for EU citizens, including minors. Notably, the GDPR establishes exacting privacy standards and imposes stringent penalties for non-compliance, while the DSA delineates clear-cut responsibilities for online platforms in content moderation. Conversely, the United States grapples with a dearth of robust federal privacy frameworks, exacerbating apprehensions surrounding social media regulation and oversight, especially concerning the protection of minors. Absent clear regulatory directives, heightened vulnerabilities persist, as evidenced by ongoing debates surrounding data access and algorithmic targeting practices[14] . Unlike the EU, where steadfast regulatory measures are firmly entrenched, the United States confronts formidable hurdles in ensuring commensurate protection for users, notably minors, within the rapidly evolving social media milieu.

4.2 4.2. WhatsApp's Minimum Age Reduction: Implications for Data Privacy and Security

The recent decision by messaging platform WhatsApp [15] to lower the minimum age threshold have raised pertinent concerns regarding data privacy and security [16]. Specifically, Meta has opted to lower the minimum age of access from 16 to 13 years in European Union countries and the United Kingdom. The stated objective is to "align the age requirement globally" , following the standards established in countries such as the United States, without considering the cultural and regulatory differences present in various regions. This decision raises several concerns regarding the safety and privacy implications for young online users, as well as the compatibility with the provisions related to the national implementations of the

[9]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/

[10]E. Lampmann-Shaver, "Privacy's next Act," cit., 103 s

[11]V. Polito, G. Valença, M. Wanick Sarinho, F. Lins, R. Pereira dos Santos, On the Compliance of Platforms with Children's Privacy and Protection Requirements-AnAnalysisofTikTok, in Software Business, N. Carroll, A. Nguyen-Duc, X. Wang, V. Stray (Eds.), 2022, pp.85-86

[12]S. Patnaik, R.E. Litan, Tiktok Shows Why Social Media Companies Need More Regulation, Brookings Institution, 2023, p. 1

[13]Ibidem

[14]S. Patnaik, R.E. Litan, Tiktok Shows Why Social Media Companies Need More Regulation, cit., pp. 4 e 10

[15]https://www.whatsapp.com/legal/terms-of-service-eea.

[16]https://www.whatsapp.com/legal/privacy-policy-eea

principle stated in article 8 GDPR on the age to provide valid consent for information society services. While the adjustment of the minimum age reflects the widespread presence of adolescents under 16 years on the platform, thereby formalizing their access, it also highlights legitimate concerns regarding their exposure to risks such as inappropriate content, cyberbullying, and potential forms of exploitation. Despite the implementation of end-to-end encryption, WhatsApp continues to encounter significant challenges concerning the security of its younger users. The reduction of the minimum age could exacerbate these risks, necessitating increased parental involvement and the adoption of preventive measures to mitigate potential harm.

5 REMARKS FOR THE SHARED DISCUSSION

From the foregoing, it is evident that the digital dimension presents an alternative scenario to the physical realm, wherein minors can construct their identities, thereby encountering common and distinct risks - to be mitigated by design and by default - to avoid deleterious consequences. Simultaneously, however, for an effective promotion of minors' rights in the digital realm, it is imperative to establish paradigms of responsibility capable of apportioning roles and responsibilities in a multi-level framework: from institutions, to schools, to parents, the entire civil society must endeavor to ensure that the digital environment frequented is a child-friendly one. Policy responses may not adhere to identical parameters and may yield varied effects on the reference society, but they all share the same premise concerning the necessity and urgency of intervening to construct a digital environment that is safe and respectful of the fundamental rights of children looking at the daily routine activities and uses.