

Entry

Growing Up Online: Comparative Legal Perspectives on Minors, Consent and Digital Exposure

Silvia Durán-Alonso

Topic Collection

Encyclopedia of Social Sciences

Edited by

Dr. Kum Fai Yuen, Dr. Xueqin Wang and Dr. Xue Li



Entry

Growing Up Online: Comparative Legal Perspectives on Minors, Consent and Digital Exposure

Silvia Durán-Alonso 

Faculty of Law, UCAM-Universidad Católica San Antonio de Murcia, Campus de los Jerónimos 135,
30107 Guadalupe, Murcia, Spain; sduran@ucam.edu

Definition

The increasing presence of minors on digital platforms raises complex legal questions regarding their privacy, data protection, and the limits of parental authority in supervising their online activities. This entry analyses the legal framework applicable to the use of the Internet by minors, with particular emphasis on the validity of consent for data processing, the risks of overexposure, the need for digital literacy and the particularities of minors who create content. This study incorporates a comparative perspective, examining national and international approaches—especially in Spain, the United States, and France—to highlight the existing regulatory gaps and the urgent need for legal harmonisation in protecting minors in the digital age.

Keywords: minors; digital exposure; internet law; consent; data protection; online platforms; child content creators; digital literacy



Academic Editors: Kum Fai Yuen,
Xueqin Wang and Xue Li

Received: 17 September 2025

Revised: 17 October 2025

Accepted: 27 October 2025

Published: 3 November 2025

Citation: Durán-Alonso, S. Growing Up Online: Comparative Legal Perspectives on Minors, Consent and Digital Exposure. *Encyclopedia* **2025**, *5*, 187. <https://doi.org/10.3390/encyclopedia5040187>

Copyright: © 2025 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The exponential growth of digital technologies has had a profound impact on the way in which children and adolescents interact with the world. In the contemporary era, children are increasingly exposed to a culture characterised by the pervasive use of Internet-connected devices, which is becoming available to them at an earlier age. These generations, frequently designated as ‘digital natives’ [1], are growing up in a world saturated with smartphones and tablets, which they are able to utilise with ease from a very early age [2]. Indeed, there is even evidence to suggest that children as young as two or three years old frequently use their parents’ mobile devices to watch videos or play games. Consequently, there has been an increasing tendency for individuals to establish their own profiles on social networks.

Therefore, children’s access to digital devices, and smartphones in particular, is virtually universal from adolescence onwards. A study of specific data from various countries reveals that in Spain, approximately 42% of 10-year-olds possess a smartphone, increasing to 53% at age 11 and reaching 75% at age 12 [3,4]. In France, 91% of individuals aged 12 and over possess a smartphone, and within the 12–17 age bracket, this figure rises to 96% [5,6]. However, an Organisation for Economic Co-operation and Development (OECD) report indicates that by the age of 10, only approximately 40% of French children have their own device, in contrast to the significantly higher figures observed in the Nordic countries, Poland and Latvia [7]. In the UK, 55% of 8–11 year olds already have a smartphone, rising to 97% by the age of 12 [8]. In the United States, meanwhile, access is almost universal: 92% of 13–14 year-olds and 97% of 15–17 year-olds have a smartphone [9].

Evidence shows that the process of digital socialisation among children and adolescents is occurring at an increasingly younger age. This phenomenon is driven by the concept of digital social integration, which suggests that the absence of online presence can result in social exclusion [10]. While this dynamic carries significant risks, it also offers potential benefits: online interaction can foster creativity, social engagement, and inclusion, especially for children who face barriers in offline contexts. As has been previously documented in doctrine, when accompanied by appropriate guidance and digital literacy, online participation has the capacity to contribute positively to children's development and sense of belonging [11,12]. As a result, minors are compelled to engage in digital activities, despite the potential risks such as vulnerability to harassment and even sexual exploitation. In a decentralised environment, concerns arise due to the absence of transparency and the presence of security risks, including the authentication of users and the integrity of content [13]. Legal safeguards must ensure that users' rights are protected online just as they are offline [14]. In this regard, the Council of Europe's "Digital Citizenship Education" framework provides a comprehensive approach to fostering responsible and rights-based digital participation among children and young people [15].

This situation poses not only an educational challenge but also a regulatory one. It concerns minors' privacy, their ability to give valid consent, and the risks arising from excessive online exposure. It is imperative to acknowledge that this form of early and frequently unsupervised exposure to digital platforms does indeed present a number of risks, especially when minors participate as content creators or interact with unknown users online. The absence of adequate digital education, coupled with the tendency of minors to share personal data without fully comprehending the implications, further exacerbates these risks [16].

In response to this novel and intricate reality, various state legal systems have demonstrated a lack of consistency in their approach. The capacity of minors to consent to the processing of their personal data, their right to privacy and the limits of parental authority in monitoring their online behaviour are areas of increasing legal and ethical concern. The purpose of this paper is to explore the legal implications of minors' digital exposure, with a particular focus on consent, personal data protection and the duties of parents or guardians. This analysis begins with an examination of Spanish law, the text subsequently incorporates comparative references to a variety of legal systems, including those of France and the United States of America. In so doing, it undertakes a thorough investigation of extant regulatory gaps and puts forward a series of proposals for the safeguarding of the rights of minors in an era of increasing global interconnectedness.

In methodological terms, this entry employs a comparative legal approach, with a primary focus on France, Spain, and the United States. These countries were selected as representative jurisdictions due to their differing legal traditions, which include continental European and common law, and their particular relevance in current debates on minors' rights and digital regulation.

References to other European countries (e.g., Germany or the Netherlands) are included selectively, when they provide illustrative examples or highlight alternative approaches within the broader EU framework. The objective is not to provide an exhaustive comparative survey, but rather to identify the key similarities and divergences among the leading systems that influence international standards in this field.

The analysis adopted is descriptive and normative rather than empirical, with the objective being to examine the main regulatory principles, trends, and possible avenues for harmonisation across jurisdictions. The temporal scope encompasses the most recent reforms and instruments that have been implemented as of 2024, including the General

Data Protection Regulation (GDPR), the Digital Services Act (DSA), and the U.S. Children's Online Privacy Protection Act (COPPA).

2. Digital Literacy as an Essential Element to Minimise the Risks of Children's Online Exposure

Despite the seemingly innocuous nature of online interaction, as previously discussed, children are particularly vulnerable to a number of risks due to their relative immaturity and lack of awareness regarding privacy implications. It is evident that children frequently engage in the practice of disseminating personal information, including photographs, geographical locations, and details such as their identity, residential address, and educational institution, without fully comprehending or evaluating the ramifications of such actions. For this reason, individuals are susceptible to the risk of identity theft, potential reputational damage, and even the possibility of being groomed by adults with illicit intentions [17,18].

A particularly salient issue in the context of children's online activity pertains to their lack of awareness regarding the potential dangers associated with the loss of control over uploaded content. Once a photograph, social media post or comment has been shared, it may be downloaded, forwarded or republished, reused or reworded without the consent of the original author. This loss of control is further compounded by the phenomenon of virality, which occurs when content rapidly disseminates, reaching a substantial audience. This amplifies the risks of harassment, ridicule, or exploitation [10].

A crucial yet frequently underestimated risk factor pertains to the absence of digital literacy, both among children and within their respective environments. A considerable number of children are proficient in the use of digital technologies; however, they are often oblivious to the legal and ethical ramifications of their online actions. Moreover, research has highlighted a lack of training among families, schools and teaching professionals in the area of educating children about privacy, cybersecurity and respectful communication [19,20]. This discrepancy in educational attainment has been identified on an international level. The Council of Europe has emphasised the necessity of integrating digital citizenship education into school curricula [15], with a particular focus on safeguarding children's rights and fostering responsible digital behaviour. In a similar vein, the OECD has advocated for the enhancement of children's capacity to evaluate online risks through critical thinking. OECD has underscored the imperative of digital literacy as an integral facet of the contemporary information society [21].

To better understand this gap, it is first necessary to clarify the conceptual framework of literacy in digital environments. At a conceptual level, it is important to distinguish between concepts that are related to each other and are often used interchangeably. Media literacy is traditionally defined as the ability to access, analyse and critically evaluate media content. In contrast, digital literacy encompasses a broader range of skills that enable individuals to use technology safely and responsibly, including awareness of privacy, security and data protection. Finally, legal literacy refers to understanding one's rights and obligations in digital contexts, a skill that is particularly relevant for minors, who must learn not only to navigate online environments, but also to exercise and defend their rights in them [22,23]. Empirical studies and policy evaluations demonstrate the efficacy of structured literacy programmes in enhancing children's resilience, self-regulation, and critical awareness in the online environment. Prominent examples include the Council of Europe's Handbook on Digital Citizenship Education [15] and the EU Strategy for a Better Internet for Children (BIK+) [24].

Despite these recommendations, at the European Union level, there is still no binding regulation in place that would necessitate the implementation of digital literacy policies for minors in a specific manner. The strategy has been articulated mainly through non-binding

instruments, such as the Council of Europe Recommendation on key competences for lifelong learning (2018/C 189/01), which identifies digital competence as one of the eight basic competences [25], and the Digital Education Action Plan 2021–2027, which directs public policies towards the digital empowerment of children and teachers [26]. Regulations such as the Digital Services Act (DSA, EU Regulation 2022/2065, in particular arts. 28, 39 and 45) indirectly reinforce the protection of minors online through transparency obligations and limitations on targeted advertising, which contribute to a safer digital environment, but without actually building the content of an autonomous right to digital literacy [27]. Scholars argue that digital literacy remains fragmented, largely dependent on national policies rather than a unified European framework [28]. Thus, recent empirical evidence confirms that although the European Union defines common strategic policies in the field of digital education, national implementation varies considerably, due to differences in resources, teacher training, technological infrastructure and pace of adoption [29]. As a result, there is no homogeneous European regulatory framework that guarantees minimum standards of digital literacy for children. This is despite digital literacy being identified as a fundamental component in the formulation of any comprehensive strategy for the protection of children and adolescents in online environments.

In summary, the risks arising from children's exposure to the Internet are not only the result of unsafe platform design or insufficient regulation, but also due to a lack of education and awareness about the reality of these risks. It is imperative to acknowledge that, in addition to considerations pertaining to design and regulation, content moderation and curation practices, which directly impact the visibility and accessibility of information to minors, are also becoming an increasingly significant factor in assessing the risks to which minors are exposed online. As previously indicated in doctrine, content management operates at the intersection of design, action and regulation, and therefore plays a decisive role in ensuring that online environments remain safe and pluralistic [30].

This underscores the pivotal role of technological architecture in ensuring the effective protection of minors within the digital landscape. In this regard, technology providers must assume an active role in ensuring child-sensitive design by implementing "privacy by default" settings, developing age-appropriate user modes and integrating technical safeguards that limit profiling and data sharing. The utilisation of artificial intelligence tools has the capacity to facilitate the detection of minors in uploaded photographs or video footage, thereby initiating supplementary consent or validation procedures. Age verification mechanisms, when implemented in conjunction with privacy safeguards, have the potential to impede access to content that is deemed to be harmful or of a commercial nature. As emphasised in recent EU policy guidelines and OECD [21] research on children in the digital environment, these measures embody the "design" facet of online safety, which ought to be complementary to legal measures and educational empowerment. Together, these legal, educational and technological dimensions illustrate the need for an integrated approach to child protection in digital environments.

3. Validity of Minors' Consent to Digital Interaction

3.1. Comparative National Approach: European Countries and the United States

The question of whether children are capable of providing valid consent for the processing of their personal data remains a contentious legal issue in national legal systems worldwide. In the digital context, consent is the prevailing legal foundation for accessing websites or platforms, in addition to storing and/or disseminating personal information. However, such consent is only legally valid when it is informed, specific and given by a person with the capacity to give it. This prompts the consideration of intricate issues in

the context of minors, as their evolving personality and distinctive legal status defies the conventional understanding of contractual autonomy.

In the context of Spain, the regulatory framework governing the legal capacity of minors is enshrined in both civil and data protection legislation. It is evident that the minimum age for consenting to the processing of personal data, and consequently for registering on a social network, is set at 14 years of age (Royal Decree 1720/2007, Regulation implementing the Law on the Protection of Personal Data, art. 13) [31]. It is important to note that prior to the specified age, minors are legally incapable of providing valid consent for the processing of their personal data. Such processing must be authorised by their parents or legal guardians. This threshold is consistent with the broader principles of civil law, as articulated in Article 1263 of the Spanish Civil Code. This article acknowledges the absence of contractual capacity in unemancipated minors, unless dictated by specific legal provisions. Additionally, art. 162 of the same legal code stipulates the requirement for parental representation in legal transactions involving minors. However, the latter exempts from this requirement ‘acts relating to personality rights that the child, in accordance with his or her maturity, may exercise on his or her own’ [32].

Doctrinally, in fact, a certain contradiction has been pointed out between the latter precept and art. 13 of the Royal Decree, on the understanding that, although age limits offer legal certainty, they do not always correspond to the real understanding by the minor of the risks involved [19,20]. However, despite this limitation, many younger children actively participate in social networks, often bypassing age restrictions, thanks to inadequate control mechanisms. Although some platforms offer privacy options to restrict access to content, children may not activate them or may mistakenly believe that they are unnecessary due to their small number of followers.

A similar situation can be observed in France, where Law No 2018-493 (which amended the previous Data Protection Act to bring it into line with the EU General Data Protection Regulation), set the minimum age of digital consent at 15 years, a higher threshold than in other EU Member States [33]. This option responds to a legislative approach that is traditionally more protective of minors, but which has generated certain tensions in practice, given that age verification mechanisms on platforms are, in general, easily circumvented, which weakens the effectiveness of the regulation and shifts the burden of control onto families. Thus, most teenagers create profiles before reaching that age, using fictitious identities or lax verification systems, so that compliance with age limits on platforms is poor, leaving the burden of supervision in the hands of parents and the child him/herself.

In this context, the French Data Protection Authority (National Commission for Data Protection and Liberties, CNIL) has repeatedly warned that the technical measures implemented by providers are insufficient to ensure compliance with legal age limits. CNIL has recommended more robust age-verification systems and digital education campaigns targeting both minors and parents [34,35]. More recently, the focus of French regulatory action has been on the specification of technical and operational requirements: on 11 October 2024, French Authority for the Regulation of Audiovisual and Digital Media (ARCOM) published technical guidelines on age verification with the objective of protecting individuals under the age of 18 from online pornography and related content [36]. These guidelines set out models and privacy protection safeguards for age assurance that authorities expect platforms to implement. Collectively, these sectoral and technical instruments, in conjunction with national legislation, serve as the foundational framework for enhancing the enforcement of age-related protections within France.

Continuing with European examples, in Germany, where the minimum age of consent was set at 16 years, research shows a similar phenomenon: a large proportion of teenagers

access social networks before the legal age, especially through shared devices or accounts co-managed with adults. This creates a gap between the norm and social practice, which erodes the effectiveness of the protection provided by the General Data Protection Regulation [37].

In the United States, the threshold is even lower: the Children's Online Privacy Protection Act (COPPA), in force since 2000, prohibits children under 13 from opening accounts without parental consent: online services directed at children under 13 must obtain verifiable parental consent before collecting, using or disclosing personal data. This regulation requires companies to implement effective age and consent verification mechanisms, as well as accessible and child-friendly privacy policies [38]. Enforcement and supervision of compliance with this regulation is the responsibility of the Federal Trade Commission (FTC), and significant penalties are foreseen: the FTC can impose fines of more than \$40,000 per violation, in addition to requiring external audits and compliance plans. In fact, high media impact rulings have already been handed down, such as the \$170 million penalty against Google/YouTube in 2019, the \$5.7 million fine against TikTok that same year, or the settlement with Epic Games (Fortnite) in 2022, which included a \$275 million penalty and the obligation to modify its child data collection practices. Despite these measures, this model has been criticised doctrinally for focusing on data collection and ex post facto action by the administrative authority, without addressing other risks related to digital exposure or ensuring structural protection beyond sanctioning. Moreover, practice shows that a large proportion of children create profiles on social networks before that age, with the tacit tolerance of the platforms. Studies by the Pew Research Center indicate that more than half of US children aged 11–12 already have an account on at least one social network, despite the fact that this violates the norm [39].

In contrast, the United Kingdom has adopted a more preventative and systemic approach with the recent Online Safety Act [40]. This establishment of legislation signifies that online platforms are now subject to a heightened duty of care, and that the Office of Communications (Ofcom) is granted extensive supervisory powers. The Act therefore necessitates that digital service providers assess and mitigate potential risks to minors, implement robust mechanisms for age verification, and ensure that systems are designed to be suitable for underage users. This model reflects a shift towards promoting continuous risk management and responsibility in design [41].

Overall, comparative experience confirms that legal age thresholds are rarely strictly adhered to, due to the ease of falsifying birth dates, the absence of effective verification mechanisms and social pressure to participate in digital environments from a very young age.

A comparative overview reveals that, despite the shared concern to protect minors, national frameworks differ in their approach: Spain and France emphasise the legal incapacity of the minor to consent and the protective representation of parents –although in France, while no specific law mandates technological safeguards for online age verification, public guidance recommends more robust measures to ensure compliance with legal age limits–, while the US model focuses on the obligation for providers to implement measures to ensure such consent, without addressing structural or design-related issues. The United Kingdom, by contrast, has adopted a more preventive and systemic approach through the Online Safety Act 2023, introducing a statutory duty of care for digital platforms and shifting the emphasis towards continuous risk assessment and design accountability. This diversity has been identified as a hindrance to the effective protection of cross-border digital environments, underscoring the necessity for international convergence in this regard. The extant literature suggests that neither model is fully satisfactory and that shared responsibility between parents, platforms and public authorities would be necessary to effectively protect children online [37].

3.2. European Union Standards and the Shift Toward Child-Centred Regulation

At the supranational level, the General Data Protection Regulation (GDPR), approved in 2016 and applicable since May 2018, which replaced Directive 95/46/EC, is of direct and mandatory application in all Member States [42]. Beyond establishing a uniform framework for data protection, the GDPR is particularly relevant to the online exposure of minors, as it strengthens the principles of consent, transparency and the right to erasure—key guarantees when children’s personal data are processed by digital platforms.

Article 8 GDPR enables Member States to stipulate the minimum age, ranging from 13 to 16 years, at which a minor can provide valid consent for the processing of their personal data by information society services. GDPR underscores the imperative for special protection for children, particularly in contexts pertaining to marketing, personality or user profiling, and the utilisation of personal data for commercial purposes in relation to services directed towards minors. However, it also safeguards the minor’s right to provide consent, explicitly stating that ‘the consent of the holder of parental authority or guardianship should not be required in the context of preventive or counselling services offered directly to children’ (Recital 38). As stated in Recital 58, which deals with the duty of transparency, it is imperative to recognise the particular needs of children and ensure that any information pertaining to them is communicated in a manner that is comprehensible to them. This entails the utilisation of clear and simple language, thereby facilitating the understanding of the information presented. It is imperative that children possess complete clarity and certainty regarding the consent they are providing, as well as the potential risks associated with the processing of their data and images [43].

This child-centred orientation, as articulated by Macenaite [37], signifies a paradigm shift from the prevailing universal data protection framework to a model that acknowledges an evolution in the capacity of children to provide their own consent, along with the inherent vulnerabilities that characterise them.

4. Minors as Creators of Content: Legal Challenges and Policy Responses

4.1. How Different Legal Systems Address the Issue

Another problem with the participation of minors in digital platforms is that it is not limited to the mere recreational use of social networks. Indeed, in recent years the phenomenon of minor content creators, also known as ‘kidfluencers’, has become established. These children and adolescents generate videos, publications, or live broadcasts, which are often monetised, thus becoming active participants in the digital economy. This shift in their economic activities has the potential to generate significant revenues. This activity gives rise to a number of complex legal issues, including the question of whether it can be considered a form of child labour. Furthermore, the degree of responsibility that should fall to parents and platforms must be determined. In addition to this, the management of the income of these minors must be clarified, as must the ways in which the right to privacy, personal development and the best interests of the minor can be guaranteed.

In France, Law No. 2020-1266, which pertains to the commercial exploitation of the image of minors under the age of 16 on online platforms, signified a pivotal moment in the specific regulation of child influencers [44]. This legislative development emerged as a consequence of the repeated expressions of concern by the Observatory on Parenting and Digital Education concerning the potential dangers associated with the professionalisation of these young YouTubers [45]. The objective of this legislation is to protect French minors from being exploited commercially, thereby ensuring the well-being of young influencers. It establishes constraints on their schedules, obliging them to reconcile recording times with their academic commitments, and it also establishes regulatory measures concerning the

right to be forgotten. Specifically, social networks and platforms are obligated to remove any content if a minor requests it, even without the need for parental authorization [46].

Moreover, the objective is to prevent the exploitation of underage content creators (including situations in which parents or legal guardians themselves encourage or manage their children's online activity for financial gain), by affording them the same protection as is given to underage actors and models at the employment level. In light of this, the French labour code was reformed, establishing that individuals who create videos featuring minors under 16 years of age, including their parents, with the objective of generating economic profit through a digital platform, are obligated to obtain prior authorisation from the relevant administrative authority. Failure to do so may result in sanctions being imposed. Conversely, should the dissemination of content on the network result in income in excess of those established for this purpose by the Council of State, parents are obliged to declare such activities of their minor children, in addition to depositing the amounts established in the Deposits and Consignments Fund, where they will be administered until the minor reaches the legal age [47]. Similarly, advertisers of a product who use a video in which a minor under 16 years of age appears are obliged to check whether the economic benefit derived from the commercialisation of this video is destined to the person responsible for its broadcast or to the blocked account of the minor. Failure to comply with this obligation may result in financial penalties. In a similar vein, digital platforms such as YouTube are obliged to ensure that minors are informed in a comprehensible manner about their rights and the potential psychological and legal ramifications that may arise from the dissemination of their imagery. This regulatory framework has been regarded as a pioneering model for safeguarding children's assets and reputations in the digital domain [48].

In more recent times, the French government promulgated Law No. 2023-451 (9 June 2023) with a view to regulating commercial influence and addressing the abuses of influencers on social media [49]. The law stipulates the requirement for transparent labelling of sponsored content, thereby establishing a framework of contractual rules between influencers, agencies, and advertisers. Despite the fact that the legislation does not specifically focus on the protection of minors, it complements existing measures under the 2020 framework, which regulates the professional activity of minors. This includes mandatory parental consent and the management of income in blocked accounts for influencers under the age of 16. In accordance with the provisions of the 2023 legislation, the authorities have been vested with the power to impose sanctions for any practices that are deemed to be deceptive or exploitative, with the potential for this to extend to consumers, including minors who have been exposed to influencer marketing.

In Spain, there is an evident regulatory evolution on the matter, which appears to include specific protection for minors in the near future. Consequently, the specific activity of content creators has been incorporated into the audiovisual framework through Law 13/2022, the General Law on Audiovisual Communication, and Royal Decree 444/2024, which regulates the so-called 'users of special relevance' in video-sharing services. This legislation imposes certain obligations, such as registration in the State Register of Audiovisual Providers, respect for age classification, compliance with codes of conduct on the protection of minors, parental control systems, or transparency in advertising [50,51]. However, the current regime continues to address influencers in general, with no specific provisions for minors engaged in this activity. It is acknowledged that minor influencers who generate income would be subject to the aforementioned obligations.

It is evident that certain reform proposals pertaining to the engagement of underage performers do advocate for the equalisation of child influencers with child performers in public performances. This would facilitate the extension of a labour and patrimonial

protection regime to the aforementioned group. A Draft Organic Law for the Protection of Minors in Digital Environments has been proposed, encompassing a digital labour protection regime and enhanced supervisory measures for platforms, thereby foreshadowing a more comprehensive regulatory framework [52]. Moreover, a proposal for a Royal Decree has been submitted for the purpose of modernising the Royal Decree 1435/1985, which currently regulates labour relations in the artistic sector (comprising the domains of art, audiovisual, music, and so forth). This Royal Decree has not been updated for a period of 40 years. This reform, associated with the Artist's Statute, introduces a novel regulation on the work of minors in social networks, assimilating this activity to the performing arts (rules that had previously been applied by analogy, with the obvious difficulties that this entails). The objective is to ensure the safeguarding of labour and personal rights of minors who create content [53]. The main new features that this reform would introduce, following the French regulation, are:

- Only minors will be allowed to carry out artistic activities as employees, under the responsibility of a company, eliminating informal self-employment;
- Strict time limits: it is forbidden to carry out these activities during school hours;
- Introduction of the figure of the privacy coordinator, aimed at protecting minors in sensitive or intimate contexts during recordings;
- Requirement of administrative authorisation, and obligation to protect their income [54].

However, it is evident that the protection of minors as consumers of content has progressed at a faster rate than the protection of minors as creators of content.

In other European countries, partial progress has been made. In the context of Belgium (Flanders), the Content Creator Protocol imposes obligations of transparency, the labelling of advertising, and limitations on the dissemination of violent or offensive content by underage influencers [55]. Despite its lack of legal status, it represents a significant instance of regulated self-governance.

The United States' regime for protecting children in entertainment has long been based on the Coogan model [56], which was originally designed to protect the earnings and working conditions of child actors. However, recent scholarship has emphasised that this framework does not fully address the novel risks faced by internet child stars. It is the contention of scholars that the monetisation structures and platform-mediated labour of contemporary child creators reveal significant legal lacunae [57]. In response to this perceived lack of regulatory oversight, several U.S. states have introduced targeted legislation aimed at extending the provisions of the actor-style protections to minors who appear in monetised online content. It is noteworthy that the state of California passed Senate Bill 764 (SB 764) in 2024, which stipulates that a portion of the income derived from content that features minors must be retained in trust accounts for the benefit of the minor [58]. The bill also establishes additional procedural safeguards, including record-keeping obligations, disclosure requirements, and enhanced rights to seek the suppression or removal of specific content. SB 764 can thus be regarded as an effort to adapt the Coogan logic to platformed content creation, illustrating how U.S. state-level innovation is beginning to fill regulatory lacunae even as the federal framework remains sectoral and fragmented. Similar legislation has been adopted in other states, including Illinois, Louisiana and New Mexico, encompassing restrictions on participation, time limits and prohibitions on parent-only contracts [59], reflecting a growing recognition of the need for legal safeguards to protect child content creators from economic exploitation [60]. These reforms are indicative of a concerted effort to prevent a 'new form of child labour exploitation' in the digital environment [61].

The rise in child content creators shows how platforms seek to attract audiences, creating new challenges for traditional child protection frameworks. The French regulation

is a pioneering example in recognising minor influencers as particularly vulnerable subjects. It introduces valuable economic and reputational safeguards, which are perfectly exportable to other legal systems, given that the social reality regulated is similar in all countries. The Spanish model, on the other hand, although displaying indications of evolution towards the French model, remains firmly rooted in a paradigm that perceives the minor as a consumer, without having fully transferred the logic of labour and economic protection. In the United States, the recovery of the tradition initiated by the Coogan Law of 1939 through recent laws in California, Illinois or Louisiana reflects an effort to shield minors' income and limit their digital labour exposure. The comparison demonstrates regulatory fragmentation, which engenders gaps in protection. This reinforces the need to move towards a uniform status of the minor content creator at the international or, at the very least, the European level.

4.2. European and International Approach

At European level, there is currently no uniform regulation specifically targeting child influencers. However, several instruments have an indirect impact in this area. The GDPR [42] establishes enhanced safeguards for minors, particularly with regard to consent and personalised advertising (Art. 8 and Recital 38). The DSA [27] reinforces these guarantees by imposing obligations on platforms to protect minors, such as setting accounts to private by default and prohibiting manipulative design techniques. Although it does not expressly address the activity of minors as content creators, it does introduce a logic of proactive responsibility on the part of platforms in relation to the risks of exploitation and exposure. The Audiovisual Media Services Directive [62] is also applicable insofar as it considers influencers to be providers of audiovisual communication services. This implies an obligation to comply with rules on surreptitious advertising, protection of minors and editorial responsibility.

At the international level, the prevailing legal doctrine has underscored the imperative to interpret these practices in the context of the Convention on the Rights of the Child (1989). The aforementioned convention acknowledges the right of minors to be safeguarded from economic exploitation (Art. 32) and to maintain their identity and image (Art. 8) [63]. It has been posited by certain authors that child influencers should be regarded as a particularly vulnerable demographic, whose online exposure necessitates a protective framework that is analogous to that historically recognised for child performers in live shows [64,65].

5. Conclusions: Policy Challenges and Future Directions

The legal protection of minors online has evolved considerably over the last decade. Nevertheless, a number of political and legislative challenges remain unresolved, thereby impeding the efficacy of the prevailing framework. These include legal fragmentation, problems with effective law enforcement, a lack of digital education and the limited participation of minors themselves in regulatory processes.

Legal fragmentation remains a significant challenge. In the European Union, as has been demonstrated, Member States have adopted divergent age thresholds for valid digital consent, ranging from 13 to 16 years. Despite the intention behind this flexibility being to respect national autonomy, the outcome has been a patchwork of rules that engender uncertainty for platforms that typically operate on an international level, given the internet's borderless nature. This has consequently led to a reduction in the efficacy of child protection measures. In a similar vein, although the DSA [27], applicable from February 2024, introduces uniform obligations for platforms, its implementation is influenced by the roles and actions of national digital services coordinators. As Mattioli has demonstrated [66], variations in enforcement practices are the consequence of differences in resources, pri-

orities and interpretations across Member States. These variations are a reflection of the challenges of achieving a fully harmonised application of the DSA.

A second major challenge pertains to the discrepancy between regulatory frameworks and actual practices. It has been demonstrated by a considerable number of studies that online platforms persist in the collection of data from minors, either deliberately or inadvertently, as a consequence of design flaws. This phenomenon occurs despite the implementation of age restrictions and mechanisms for parental consent. The utilisation of ambiguous patterns, addictive interfaces and deceptive privacy options frequently results in the absence of adequate informed consent, even in instances where it is formally obtained. As has been documented [27], the reliance on mechanisms for obtaining individual consent is increasingly being called into question in environments designed to exploit attention and data.

A further persistent weakness is evidenced by the absence of regulatory development in the training of minors in digital skills. It is evident that, despite their legal obligations, parents frequently experience a paucity of the requisite knowledge, training and support to competently supervise and guide their offspring in their digital activities. Furthermore, educational institutions frequently lack the necessary resources to incorporate legal and ethical knowledge of digital life into their curricula. In the absence of structural investment in digital literacy for all stakeholders (minors, parents, educators, public authorities), the already limited legal provisions will continue to be underutilised or misinterpreted.

International organisations such as the Council of Europe and the OECD have advocated for a more comprehensive approach, emphasising the necessity to develop digital citizenship training, platform responsibility and the incorporation of children's voices in policy design. As stated in Article 12 of the Convention on the Rights of the Child [63], children are already recognised as having the right to express their views on all matters that affect them. However, this right is often overlooked when regulatory frameworks are being established that have a bearing on children. It is evident that young users are seldom consulted, and even less often are digital services designed with their needs and vulnerabilities in mind.

Recent innovations, however, offer some cause for hope. EU guidelines on online child protection recommend mechanisms such as anonymous age verification, default privacy settings and educational interfaces, all of which point to a preventive rather than reactive model.

Looking ahead, a more coherent and effective regulatory approach could include:

- Harmonising age thresholds and consent conditions in different Member States' regulations;
- Strengthening independent supervisory bodies with units specifically dedicated to child protection;
- Establishing clear legal obligations for platforms to offer privacy protection options, consent provision, or recommendation systems, among others, tailored to children;
- Investing in public education policies that integrate the legal, ethical, and civic dimensions of digital life;
- Promoting the integration of technological safeguards—such as privacy-by-default settings, reliable age-verification tools, and transparent content recommendation systems—as complementary mechanisms to legal and educational measures;
- Enabling children to participate meaningfully in decisions that affect their digital experience, as rights holders and active citizens.

When considered collectively, these measures would establish a comprehensive framework that integrates legal coherence, technological responsibility, and digital literacy. A balanced interaction between regulation, platform design and education has the potential

to foster safer and more empowering digital environments for minors. The challenge for the coming years lies in ensuring that legal rules and technological architecture evolve in parallel, mutually reinforcing one another to uphold children's rights in the digital age.

In conclusion, protecting minors online remains a crucial issue today. As children become increasingly involved with digital platforms from a very early age, the law must adapt not only to the risks of misuse and data exposure, but also more fundamental issues of autonomy, education and equity. Although progress has been made, significant gaps still remain and demand urgent attention.

A preventative approach, predicated on legal, educational and technological reforms, is imperative to ensure that children can navigate the online environment safely, with dignity and protection, and with respect for their autonomy as they reach the legal age. Ensuring the optimal outcomes for children in digital environments necessitates a multifaceted approach that encompasses the protection of minors from potential harm, in conjunction with the cultivation of their competencies to become responsible, informed, resilient, and engaged digital citizens.

Ultimately, ensuring that children's rights are upheld online necessitates a concerted, global effort that encompasses legal harmonisation, ethical design and digital education.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The author declares no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

BOE	Boletín Oficial del Estado (Spain)
CNIL	Commission Nationale de l'Informatique et des Libertés (National Commission for Data Protection and Liberties)
COPPA	Children's Online Privacy Protection Act
DSA	Digital Services Act
GDPR	General Data Protection Regulation
OECD	Organisation for Economic Co-operation and Development

References

1. Prensky, M. Digital natives, digital immigrants. *Horizon* **2001**, *9*, 1–6. [CrossRef]
2. Organista Sandoval, J.; McAnally Salas, L.; Lavigne, G. El teléfono inteligente (smartphone) como herramienta pedagógica. *Apertura* **2013**, *5*, 6–19. Available online: https://www.redalyc.org/pdf/688/68830443002.pdf?utm_source=chatgpt.com (accessed on 13 September 2025).
3. Marketing Charts. At What Age do Kids Start Getting Smartphones? Available online: <https://www.marketingcharts.com/demographics-and-audiences/teens-and-younger-225502> (accessed on 13 September 2025).
4. Wilson, J.; Kellman, L. Should Young Kids Have Smartphones? These Parents in Europe Linked Arms and Said No. Medicalxpress. Available online: <https://medicalxpress.com/news/2024-06-young-kids-smartphones-parents-europe.html> (accessed on 13 September 2025).
5. Arcep. Digital Market Barometer: Digital Device Ownership and Usage in France. Available online: <https://en.arcep.fr/news/press-releases/view/n/digital-device-ownership-and-usage-190325.html> (accessed on 13 September 2025).
6. Statista. Smartphone Penetration in France by Age Group. 2023. Available online: <https://www.statista.com/statistics/408427/smartphone-penetration-in-france-by-age-group/> (accessed on 13 September 2025).
7. OECD. *How's Life for Children in the Digital Age?* OECD: Paris, France, 2025. [CrossRef]

8. Ofcom. Children and Parents: Media Use and Attitudes Report. Available online: <https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/media-literacy-research/children/childrens-media-use-and-attitudes-report-2025/childrens-media-literacy-report-2025.pdf?v=396621> (accessed on 13 September 2025).
9. Statista. Percentage of Teenagers in the United States Who Have Access to a Smartphone at Home as of October 2023, by Age Group. Available online: <https://www.statista.com/statistics/476050/usage-of-smartphone-teens-age/#:text=According%20to%20a%202023%20survey,stated%20owning%20a%20smartphone%20device> (accessed on 13 September 2025).
10. Martínez-Rodrigo, E.; Martínez-Cabeza Jiménez, J. Proyección de los menores en las redes sociales. In *Desafíos de la Protección de Menores en la Sociedad Digital. Internet, Redes Sociales y Comunicación*; Tirant lo Blanch: Valencia, Spain, 2018; pp. 487–512.
11. Livingstone, S.; Blum-Ross, A. *Parenting for a Digital Future: How Hopes and Fears About Technology Shape Children's Lives*; Oxford Academic: New York, NY, USA, 2020. [CrossRef]
12. Livingstone, S.; Mascheroni, G.; Staksrud, E. European research on children's internet use: Assessing the past and anticipating the future. *New Media Soc.* **2018**, *20*, 1103–1122. [CrossRef]
13. Aranda Serna, F.J. Los retos jurídicos del metaverso: Aproximación a los riesgos y desafíos que plantea para la identidad digital [Legal challenges of the metaverse: An approach to the conflicts and problems posed for digital identity]. *Eur. Public Soc. Innov. Rev.* **2024**, *9*, 1–19. [CrossRef]
14. Dizaji, A.; Dizaji, A. Metaverse and its legal challenges. *Synesis* **2023**, *15*, 138–151.
15. Council of Europe. *Digital Citizenship Education Handbook*; Council of Europe Publishing: Strasbourg, France, 2019. Available online: <https://rm.coe.int/16809382f9> (accessed on 15 October 2025).
16. Gil Antón, A.M. El menor y la tutela de su entorno virtual. *Rev. Derecho UNED* **2015**, *16*, 275–319. [CrossRef]
17. Barrio Fernández, A. Los adolescentes y el uso de los teléfonos móviles y de videojuegos. *Int. J. Dev. Educ. Psychol.* **2014**, *3*, 563–570. [CrossRef]
18. Gómez Cabranes, L. Las emociones del internauta. In *Emociones y Estilos de Vida: Radiografía de Nuestro Tiempo*; Editorial Biblioteca Nueva: Madrid, Spain, 2013; pp. 211–243.
19. Faggiani, V. Derechos del menor e internet: Una aproximación desde el derecho constitucional europeo. In *Desafíos de la Protección de Menores en la Sociedad Digital: Internet, Redes Sociales y Comunicación*; Tirant lo Blanch: Valencia, Spain, 2018; pp. 21–54.
20. Gil Antón, A.M. Redes sociales y privacidad del menor: Un debate abierto. *Rev. Aranzadi Derecho Nuevas Tecnol.* **2014**, *36*, 143–180.
21. OECD. *Children in the Digital Environment: Revised Typology of Risks*; OECD Digital Economy Papers; OECD: Paris, France, 2021; p. 302. [CrossRef]
22. UNESCO. *Media and Information Literacy Curriculum for Educators and Learners*, 2nd ed.; UNESCO: Paris, France, 2021. Available online: <https://unesdoc.unesco.org/ark:/48223/pf0000377065> (accessed on 16 October 2025).
23. Livingstone, S.; Stoilova, M.; Nandagiri, R. *Children's Data and Privacy Online: Growing Up in a Digital Age*; London School of Economics and Political Science (LSE): London, UK, 2023. Available online: https://plattform-privatheit.de/p-prv-wAssets/wp-content/uploads/Livingstone_Childrens-data-and-privacy-online.pdf (accessed on 16 October 2025).
24. European Commission. *A Better Internet for Kids (BIK+) Strategy*; European Commission: Brussels, Belgium, 2022. Available online: <https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids> (accessed on 16 October 2025).
25. Council Recommendation of 22 May 2018 on key competences for lifelong learning (2018/C 189/01). *Off. J. Eur. Union C* **2018**, *189*, 1–13. Available online: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32018H0604\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32018H0604(01)) (accessed on 14 September 2025).
26. European Commission. *Digital Education Action Plan 2021–2027: Resetting Education and Training for the Digital Age*; Publications Office of the European Union: Luxembourg, 2020. Available online: <https://op.europa.eu/en/publication-detail/-/publication/33b83a7a-ddf9-11ed-a05c-01aa75ed71a1/language-en> (accessed on 14 September 2025).
27. Regulation (EU) 2022/2065 of the European Parliament of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services ACT) Amending Directive 22000/31/EC. *Off. J. Eur. Union L* **2022**, *277*, 1–102. Available online: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng> (accessed on 14 September 2025).
28. Gabriel, F.; Marrone, R.; Van Seville, Y.; Kovanovic, V.; de Laat, M. Digital education strategies around the world: Practices and policies. *Ir. Educ. Stud.* **2022**, *41*, 85–106. [CrossRef]
29. Gkoutis, G.; Thode, M.; Paliokas, I. A European Examination of Digital Education Strategies: Broader Insights into Policy Adoption and Economic Impact. *Digit. Soc.* **2025**, *4*, 53. [CrossRef]
30. Gosztonyi, G. Content Management or Censorship? In *Censorship from Plato to Social Media*; Law, Governance and Technology Series; Springer: Cham, Switzerland, 2023; Volume 61, pp. 15–34. [CrossRef]
31. Royal Decree 1720/2007 of 21 December 2007 Approving the Regulation Implementing Organic Law 15/1999 on the Protection of Personal Data. Boletín Oficial del Estado (BOE-A-2008-979). Available online: <https://www.boe.es/buscar/act.php?id=BOE-A-2008-979> (accessed on 14 September 2025).

32. Código Civil (Civil Code). Consolidated Text. BOE-A-1889-4763. 1889. Available online: <https://www.boe.es/buscar/act.php?id=BOE-A-1889-4763> (accessed on 14 September 2025).
33. Loi n° 2018-493 du 20 Juin 2018 Relative à la Protection des Données Personnelles. *J. Off. République Française* **2018**. Available online: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037085952> (accessed on 14 September 2025).
34. CNIL. *La CNIL Publie 8 Recommandations Pour Renforcer la Protection des Mineurs en Ligne*; CNIL: Paris, France, 2021. Available online: <https://www.cnil.fr/fr/la-cnil-publie-8-recommandations-pour-renforcer-la-protection-des-mineurs-en-ligne> (accessed on 14 September 2025).
35. CNIL. *Recommendation 7: Check the Age of the Child and Parental Consent While Respecting the Child's Privacy*; CNIL: Paris, France, 2021. Available online: <https://www.cnil.fr/en/recommendation-7-check-age-child-and-parental-consent-while-respecting-childs-privacy> (accessed on 16 October 2025).
36. ARCOM. *Technical Guidelines on Age Verification for the Protection of Persons Under 18 Online*; ARCOM: Fort Smith, AR, USA, 2024. Available online: <https://www.arcom.fr/en/find-out-more/legal-area/legal-resources/technical-guidelines-age-verification-protection-persons-under-18-online-pornography> (accessed on 16 October 2025).
37. Macenaite, M. From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. *New Media Soc.* **2017**, *19*, 765–779. [CrossRef]
38. Children's Online Privacy Protection Act of 1998. Available online: <https://www.congress.gov/bill/105th-congress/senate-bill/2326/text> (accessed on 14 September 2025).
39. Livingstone, S.; Byrne, J. Parenting in the Digital Age. The Challenges of Parental Responsibility in Comparative Perspective. In *Digital Parenting. The Challenges for Families in the Digital Age*; Mascheroni, G., Ponte, C., Jorge, A., Eds.; Nordicom: Göteborg, Sweden, 2018; pp. 19–30. Available online: <https://norden.diva-portal.org/smash/get/diva2:1535895/FULLTEXT01.pdf> (accessed on 14 September 2025).
40. UK Government. *Online Safety Act 2023: Explainer*; UK Government: London, UK, 2024. Available online: <https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer> (accessed on 16 October 2025).
41. Nash, V.; Felton, L. Treating the Symptoms or the Disease? Analysing the UK Online Safety Act's Approach to Digital Regulation. *Policy Internet* **2024**, *16*, 818–832. [CrossRef]
42. 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 (General Data Protection Regulation, GDPR). *Off. J. Eur. Union L* **2016**, *119*, 1–88. Available online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679> (accessed on 14 September 2025).
43. Cebrián Beltrán, S. Sharenting: Nuevo reto para el derecho a la imagen y a la protección de datos del menor. *Lex Soc. Rev. Derechos Soc.* **2023**, *13*, 8227. [CrossRef]
44. Loi n° 2020-1266 du 19 Octobre 2020 Visant à Encadrer L'exploitation Commerciale de L'image D'enfants de Moins de Seize ans sur les Plateformes en Ligne. Available online: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042439054> (accessed on 14 September 2025).
45. Le Monde. Available online: https://www.lemonde.fr/pixels/article/2018/05/23/les-chaines-youtube-familiales-epinglees-pour-travail-illicite-par-une-association_5303447_4408996.html (accessed on 14 September 2025).
46. Cremades, P. Futuro profesional de los menores y ejercicio de la patria potestad. *Rev. Boliv. Derecho* **2021**, *32*, 252–277.
47. Wong, R. Social Media and Social Reform: Why States Should Consider Protecting the Rising Kidfluencers. *SMU Dedman Sch. Law* **2024**, *77*. [CrossRef]
48. Thuegaz, A. Encadrement Juridique de L'exploitation Commerciale de L'image des Enfants Influenceurs sur les Plateformes en Ligne. Village de la Justice. 2025. Available online: <https://www.village-justice.com/articles/exploitation-commerciale-image-des-enfants-influenceurs-encadrement-juridique,53452.html> (accessed on 14 September 2025).
49. 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. *J. Off. République Française* **2023**. Available online: <https://www.legifrance.gouv.fr/eli/loi/2023/6/9/ECOX2308125L/jo/texte> (accessed on 16 October 2025).
50. Law 13/2022, the General Law on Audiovisual Communication. Boletín Oficial del Estado (BOE-A-2022-11311). Available online: <https://www.boe.es/buscar/act.php?id=BOE-A-2022-11311> (accessed on 14 September 2025).
51. Royal Decree 444/2024 of 7 May 2024 Regulating the Procedure for Verifying the AGE of users on Information Society Services that Offer Pornographic Content. Boletín Oficial del Estado (BOE-A-2024-8716). Available online: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2024-8716 (accessed on 14 September 2025).
52. Ministerio de la Presidencia, Justicia y Relaciones con las Cortes. El Congreso da luz Verde a la Tramitación de la ley Orgánica Para la Protección de los Menores en Entornos Digitales. Available online: <https://www.mpr.gob.es/prencom/notas/Paginas/2025/100925-tramitacion-lo-proteccion-menores-entornos.aspx> (accessed on 14 September 2025).

53. Europa Press. El Gobierno Presenta el Real Decreto que Regula el Trabajo de Menores en Redes Sociales y Limita la IA Generativa. Available online: <https://www.europapress.es/cultura/exposiciones-00131/noticia-gobierno-presenta-real-decreto-regula-trabajo-menores-rss-limita-selva-ia-generativa-20250728133830.html> (accessed on 14 September 2025).
54. Diariolaley. El Gobierno Presenta el Real Decreto que Regula el Trabajo de Menores en rrrs y Limita la “selva” de la IA Generativa. Available online: <https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAMtMSbH1czUwMDAyMjQ1MDNXK0stKs7Mz7M1MjAyNTA3sgAJZKZVuuQnh1QWpNqmJeYUpwIAzB5AfDUAAAA=WKE> (accessed on 14 September 2025).
55. Better Internet for Kids. Available online: <https://better-internet-for-kids.europa.eu/en/rules-guidelines/content-creator-protocol-ccp> (accessed on 15 September 2025).
56. Shor, T. The Coogan Law. Available online: https://www.writing.ucsb.edu/sites/secure.lsit.ucsb.edu.writ.d7/files/sitefiles/publications/2010_Sho.pdf (accessed on 15 September 2025).
57. Clouse, K. Cash Kid: The Need for Increased Financial Protections of Internet Child Stars on YouTube. *William Mary Law Rev.* **2023**, *65*, 195.
58. California Senate Bill No. 764, 2023–2024 Reg. Sess. Signed into Law. 2024. Available online: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB764&utm (accessed on 15 September 2025).
59. SAG-AFTRA Coogan Law. Available online: <https://www.sagaftra.org/membership-benefits/young-performers/coogan-law> (accessed on 15 September 2025).
60. Miller, A.J. Ensuring Ethical Practices Within the Influencer Playground: Extending Coogan’s Law to Digital Content Creators. *Calif. West. Law Rev.* **2025**, *61*, 123–145.
61. Clark, D.R.; Jno-Charles, A.B. Child Labor in Social Media: Kidfluencers, Ethics of Care, and Exploitation. *J. Bus. Ethics* **2025**, *201*, 35–62. [CrossRef]
62. Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive, AVMSD). *Off. J. Eur. Union L* **2010**, *95*, 1–24. Available online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32010L0013> (accessed on 15 September 2025).
63. United Nations General Assembly. *Convention on the Rights of the Child*; United Nations General Assembly: New York, NY, USA, 1989.
64. Levesque, R.J.R. *Adolescents, Media, and the Law: What Developmental Science Reveals and Free Speech Requires*; Oxford University Press: New York, NY, USA, 2007. [CrossRef]
65. Steinberg, S. The Art of Sharing: Children’s Rights in the Influencer Era. *Fla. Entertain. Sports Law Rev.* **2023**, *3*, 4.
66. Mattioli, P. Navigating the Complexities of the DSA’s Enforcement: The Role of National Coordinators. *Utrecht Law Rev.* **2025**, *17*, 19–35. [CrossRef]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.