
Secção Temática/Thematic Section/Sección Temática. Artigos/Articles/Artículos
Artificial Intelligence and Privacy: The Urgent Need for
Children's Media Literacy



Inteligência Artificial e Privacidade: A Urgente Necessidade
da Literacia Mediática das Crianças

Inteligencia Artificial y Privacidad: La Urgente Necesidad de
la Alfabetización Mediática de los Niños

Katharine Sarikakis

Department of Communication, University of
Vienna, Vienna, Austria
katharine.sarikakis@univie.ac.at

Angeliki Chatziefrimidou

Department of Communication, University of
Vienna, Vienna, Austria
angechatzi@yahoo.gr

Revista Comunicando

vol. 14, no. 1, e025003 2025

Associação Portuguesa de Ciências da Comunicação, Portugal

ISSN: 2184-0636

ISSN-E: 2182-4037

Periodicity: Frecuencia continua
comunicando@sopcom.pt

Received: 30 October 2024

Accepted: 26 February 2025

Published: 02 June 2025

DOI: <https://doi.org/10.58050/comunicando.v14i1.422>

URL: <https://portal.amelica.org/ameli/journal/819/8195202006/>

Abstract: Protecting children's privacy continues to challenge policymakers and citizens alike in the media age and debates often point to the need for data protection literacy. The latter constitutes only one limited aspect of privacy, yet, it dominates actions by global platforms as they seek to monetise on personal data. The integration of artificial intelligence (AI) into the various platforms that children daily use, further complicates the effort to counter violations of privacy globally. Importantly, children's views on these matters need to be further integrated in the global debates on privacy. This study contributes to knowledge about children's experiences and perceptions of privacy while online, by examining children's media literacy through a qualitative meta-synthesis of research data from work with children in Vienna, Austria. Children's media literacy skills are presented along with children's digital privacy literacy skills and their development is traced through the different age groups. Furthermore, the study examines the intersection between privacy literacy and AI literacy. Through a systematic synthesis of qualitative findings, this study aims to develop a map that describes the essential skills needed for personal data protection at different developmental stages in AI-driven media. The findings highlight the evolution of skills across the nine-16 age range, such as critical evaluation and privacy management. Although younger children may struggle with abstract AI concepts, they are able to understand basic privacy settings. Older children may begin to grasp the implications of data used in AI but still lack the critical skills to evaluate AI-driven disinformation.

Keywords: Artificial Intelligence, Children, Digital Privacy Protection, Media Literacy, AI Literacy.

Resumo: Proteger a privacidade das crianças continua a ser um desafio tanto para os decisores políticos como para os cidadãos, na era dos meios de comunicação, sendo frequente o apelo à necessidade de literacia em proteção de dados. Esta constitui apenas um aspeto limitado da privacidade, mas domina as ações das plataformas globais que procuram rentabilizar os dados pessoais. A integração da inteligência artificial (IA) nas diversas plataformas utilizadas diariamente pelas crianças complica ainda mais os esforços para combater as violações de privacidade a nível global. Importa sublinhar que as perspetivas das próprias crianças sobre estas questões devem ser mais integradas nos debates globais sobre privacidade. Este estudo contribui para o conhecimento sobre as experiências e perceções das crianças relativamente à privacidade online, examinando a sua literacia mediática através de uma meta-síntese qualitativa de dados de investigação recolhidos junto de crianças em Viena, Áustria. As competências de literacia mediática das crianças são apresentadas juntamente com as suas competências de literacia em privacidade digital, sendo a sua evolução traçada ao longo dos diferentes grupos etários. A par disso, o estudo analisa a interseção entre a literacia em privacidade e a literacia em IA. Através de uma síntese sistemática de resultados qualitativos, este estudo pretende desenvolver um mapa que descreva as competências essenciais para a proteção de dados pessoais em diferentes fases do desenvolvimento, no contexto dos meios impulsionados por IA. As conclusões evidenciam a evolução de competências entre os nove e os 16 anos, como a avaliação crítica e a gestão da privacidade. Embora as crianças mais novas possam ter dificuldade em compreender conceitos abstratos relacionados com a IA, conseguem entender configurações básicas de privacidade. As crianças mais velhas podem começar a compreender as implicações do uso de dados pela IA, mas continuam a carecer de competências críticas para avaliar a desinformação gerada por IA.

Palavras-chave: Inteligência Artificial, Crianças, Proteção da Privacidade Digital, Literacia Mediática, Literacia da Inteligência Artificial.

Resumen: Proteger la privacidad de los niños sigue siendo un desafío tanto para los responsables políticos como para los ciudadanos en la era de los medios de comunicación, y los debates a menudo apuntan a la necesidad de una alfabetización en protección de datos. Esta representa solo un aspecto limitado de la privacidad, pero domina las acciones de las plataformas globales que buscan monetizar los datos personales. La integración de la inteligencia artificial (IA) en las diversas plataformas que los niños utilizan a diario complica aún más los esfuerzos por contrarrestar las violaciones de la privacidad a nivel mundial. Es especialmente importante que las opiniones de los propios niños sobre estos temas se integren más en los debates globales sobre la privacidad. Este estudio

contribuye al conocimiento sobre las experiencias y percepciones de los niños en relación con la privacidad en línea, examinando su alfabetización mediática a través de una meta-síntesis cualitativa de datos de investigaciones realizadas con niños en Viena, Austria. Se presentan las competencias de alfabetización mediática de los niños junto con sus habilidades en alfabetización sobre privacidad digital, y se traza su desarrollo a lo largo de los distintos grupos de edad. Además, el estudio analiza la intersección entre la alfabetización en privacidad y la alfabetización en IA. A través de una síntesis sistemática de hallazgos cualitativos, este estudio tiene como objetivo desarrollar un mapa que describa las habilidades esenciales necesarias para la protección de datos personales en las distintas etapas del desarrollo, en un entorno mediático impulsado por IA. Los resultados destacan la evolución de habilidades en el rango de edad de nueve a dieciséis años, como la evaluación crítica y la gestión de la privacidad. Aunque los niños más pequeños pueden tener dificultades para comprender conceptos abstractos relacionados con la IA, son capaces de entender configuraciones básicas de privacidad. Los niños mayores pueden empezar a captar las implicaciones del uso de datos en la IA, pero aún carecen de habilidades críticas para evaluar la desinformación impulsada por IA.

Palabras clave: Inteligencia Artificial, Niños, Protección de la Privacidad Digital, Alfabetización Mediática, Alfabetización en IA.

1. Introduction

Digital devices and social media pervade everyday life, making it increasingly difficult for individuals to maintain their privacy. Data is collected from a plethora of devices at a speed outpacing that of privacy laws aimed at protecting individual privacy rights (Kerry, 2018, p. 1). Adults are assumed to be more familiar with online privacy (European Union Agency for Fundamental Rights, 2020). But what about the underage internet users? The extensive internet usage by children has been highlighted in a range of studies; for instance, UNICEF's study found that 33% of children and youth aged 0-25 years old globally have access to the internet at home (UNICEF, 2020, p. 5) The degree of usage varies by country and continent. Nevertheless, as children spend more time online, it also calls for an increase in privacy protection.

Protecting children's privacy involves three main difficulties (Livingstone, Stoilova, & Nandagiri, 2019a, p. 6). First, children are often the first to experiment with new digital devices, services and contents, encountering risks before most adults become aware of them or understand how to minimise them. Second, children cannot realise that the digital environment poses present and future dangers to their well-being. Third, digital environments do not adequately consider children's specific needs and rights. These challenges increase as artificial intelligence (AI) systems are embedded in a variety of applications and toys (UNICEF, 2021). Personalised media content can enhance children's media use in entertainment, information and learning domains (Ramachandran et al., 2017); protect children's digital experiences by filtering harmful online content (Kumaresamoorthy & Firdhous, 2018); or may improve accessibility for children with special needs (Baykal et al., 2020). Despite advantages of AI, considerable risks regarding misinformation and children's ability to evaluate social media content arise. Hartwig et al. (2024) examined the skills of 39 teenagers aged 13 to 16 and their ability to perceive and spot misinformation on the platform TikTok. They found that although children were able to recognise manipulated videos and wrong information, they tend to accept automated systems without skepticism, underlying the need for transparency.

Furthermore, there are important concerns about AI systems in the digital privacy domain. Richards (2021) examined TikTok in terms of data collection, such as contact lists, IP addresses, location data and biometric information, raising concerns regarding issues of monitoring from the TikTok's parent company, ByteDance. Using algorithms that predict users' preferences and selling the prediction to

companies “the consumers are turned into the product” (Richards, 2021, p.3). Zulkifli (2022) shared the same concerns as a result of TikTok’s extensive data collection practices, third-party sharing and tracking services.

For the purpose of this study AI is understood as:

- Systems that continuously collect users’ data by tracking online activities through online spaces such as platforms, websites and applications (Richards, 2021; Zulkifli, 2022).
- AI-driven recommendation systems that are algorithms, which personalise online content on social media platforms or advertisements, based on the previous users’ choices (Richards, 2021).
- Generative AI that produces audiovisual content that is not original and authentic (Cooke et al., 2024).

This study aims to define and interconnect media literacy, digital privacy literacy and AI privacy literacy competencies children demonstrate and to map the ways in which children’s privacy literacy competencies develop as children get older. We explore understandings of media literacy for children in the following part, by conceptualising it in terms of digital media and digital privacy forms of literacy and AI privacy literacy to showcase that these literacies are interconnected and build on each other. Following, the study presents the method of meta-synthesis and goes on to define and combine children’s literacies as these literacies develop through the years.

2. Media Literacy for Children

2.1. Digital Media Literacy

For children to perceive AI issues related to their privacy, they must first develop basic media literacy. Media literacy encompasses more than just reading and writing (Frau-Meigs, 2016, p. 20) and goes beyond superficial interface skills, such as operating a computer, using a keyboard and searching online. While these skills are important, they are limited to a functional form of literacy (Buckingham, 2015). Hugger (2008) distinguishes between media competence, which includes criticism, knowledge, use and design and media education, which adds a pedagogical aspect. Buckingham’s (2015) media literacy framework encompasses representation, language, production and audience: “representation” involves evaluating content based on creator intent, “language” relates to

understanding digital media composition, “production” covers understanding communicator, audience and purpose and “audience” focuses on self-perception as a user. These frameworks demonstrate the fluidity of the concept of media literacy as technologies and social uses evolve, but also the level of complementarity with each other.

Moreover, media literacy changes across age demographics, presenting different challenges to different age groups (Rasi et al., 2019). For children and adolescents, the approach of media literacy is described as “collaborative, creative, playful (...) as well as analytic, reflective, inquiry- and project-based learning practices” (Rasi et al., 2019, p. 3). In line with these ideas, the European Commission developed a Digital Competencies Framework (DigComp) aiming to cover competencies of digital literacy: information and data literacy, communication and collaboration, digital content creation, digital security and problem-solving as well as the sub-competencies therein (Carretero et al., 2017, p. 21).

2.2. Digital Privacy Literacy

Acquiring critical media literacy, is argued, empowers children with skills (and hence the individual responsibility) to protect their personal data. Privacy literacy is understood as knowledge about privacy issues. Damberger (2013) emphasises that children need personal insight to navigate media responsibly, arguing that solely following rules will not foster self-responsible, self-determined media engagement. The protection of privacy on the internet requires responsible use of media: “media and internet literacy are an antecedent for individuals to be able to understand, protect and defend their privacy” (Culver & Grizzle, 2017, p. 25). To achieve this, children require an understanding of protective measures, the maturity to recognise risks and the knowledge to apply them appropriately. Therefore, a combination of self-determination and a sense of social responsibility (Gapski, 2001) is necessary. If the above concerns the conditions of strengthening individuals’ skills through media literacy, Sas et al. (2023) explored the effectiveness of existing age-appropriate privacy design strategies and evaluated how well nine free-to-play (F2P) mobile games adhere to these strategies. Evaluation criteria included the clarity of privacy policies, the use of child-friendly language and formats and the inclusion of parental consent mechanisms, underlining the need for privacy education (Sas et al., 2023).

Expanding on this need for effective privacy education, Livingstone, Bulger et al. (2022) provided a socio-cultural perspective in this discourse as they examined children’s digital privacy across different cultures, focusing on education and regulation. They

conducted qualitative research, with 690 children in the UK, USA, Austria, Belgium and East Asia. Findings show that children mainly understand privacy in interpersonal contexts but struggle with institutional and commercial data uses, especially related to platforms. The study found that children from privileged regions showed varying levels of awareness of data protection, while lower-income regions focused on basic digital literacy skills, underlining the need for both adequate regulation and media education.

While educating children about privacy is challenging due to the complexity of the privacy concepts and their limited media literacy skills, Choi (2023) adds to these findings by addressing privacy literacy in social media. Using surveys with Facebook users, students in the USA, the study argued that privacy literacy goes beyond mere knowledge, including the understanding of technology and co-ownership of information as children's privacy perception evolves with age (Choi, 2023). Building on the developmental perspective, Livingstone, Stoilova, Yu et al. (2018) presented the types and levels of privacy children develop through the years. First, children aged five to seven, had developed an understanding of ownership but still have a low awareness of danger and are still learning the rules. Second, children aged eight to 11 developed a basic understanding of privacy risks related to sharing data and parental monitoring and rules. Finally, in the last age group from 12 to 17 years old, children perceive online space as personal expression and are aware of risks with a focus on interpersonal privacy, including "data traces" and "device tracking".

Kumar et al. (2023) turned their attention to the structural factors challenging the efficacy of such attempts. Through an analysis of 90 publications with focus on digital technologies designed for children aged five to 12 found that children's autonomy is compromised by technological systems that collect, process and disseminate children's data. Their study highlights the lack of theoretical frameworks to guide privacy decisions. They propose using theoretical frameworks that involve children in design in navigating privacy challenges. The increasing complexity of AI-based systems is further accelerating the privacy issues in children's lives, which we discuss below.

2.3. AI Literacy

Research interest in recent years has shifted to the role of AI in children's digital experiences. Wang et al. (2022) conducted a systematic literature review of 188 articles, discussing AI systems that are specifically designed for children for purposes such as education, healthcare and safety. Regarding ethical considerations, AI systems adapt to children's developmental stages, but there are concerns

regarding socially disadvantaged backgrounds and personalised solutions (Wang et al., 2022).

An additional aspect is children's understanding of AI. Okkonen and Kotilainen (2019) investigated how AI applications adapt to children's behaviours, raising questions about privacy and awareness. They conducted interviews with 16 pairs of minors, aged 10-17 and their parents, in Finland and in South Africa. Their key findings included low awareness of AI among minors, as they trust AI, raising concerns amongst parents (Okkonen & Kotilainen, 2019). Similarly, Mertala et al. (2022) examined children's understanding of AI among 195 Finnish students in grades 5 and 6. Their findings described children's AI knowledge as superficial, as they were unaware of the privacy risks associated with data collection. The study highlighted the importance of education to support children to "demystify AI", addressing topics such as personalised services, marketing, deepfakes and generative media.

Moreover, Bendeche et al. (2021) explored digital privacy literacy through the AI in "My Life" workshops, conducting a study among 500 children aged 15 to 16 in Dublin. Their study aimed to improve AI understanding and empower disadvantaged teenagers concerning issues such as ethics, privacy and security, despite children's low awareness of how much personal data they produce and how AI systems collect and use it (Bendeche et al., 2021). Similarly, Ali et al. (2021) conducted an online workshop with interactive activities and games to introduce 38 middle school students aged 10 to 15 in the USA to AI and topics such as misinformation and deepfakes. The study found that participants had low awareness of AI systems and faced difficulty identifying AI-generated content. After the workshop activities, children's skills improved. Finally, the study calls for an expanded media literacy curriculum that includes critical AI literacy.

The literature review underlines the importance of privacy literacy that empowers children with respect to their age and developmental capabilities as well as to develop skills dealing with privacy and AI risks. Key elements to address these demanding issues are regulatory frameworks to protect children's online privacy and privacy education. Despite the existing research, it is still unclear what digital privacy literacy competencies and AI privacy literacy competencies are developed by different age groups and how this evolves as children get older and how these are intersecting across the field of privacy, digital platforms and AI.

This study's overall aim is to create a map to link media skills, privacy literacy and AI literacy across the different age groups, highlighting what skills are crucial for children at each stage of development. Building on the above, we asked:

In which ways do children's media literacy, digital privacy literacy and AI literacy competencies intersect and develop through the age groups of nine, 12 and 14 to 16?

3. Methodology

Based on that foundational research, this current study aims to conduct a meta-synthesis to define the media literacy, digital privacy literacy and AI privacy literacy competencies and interconnects them and to present how they evolve as children get older. This current study is a meta-synthesis of a single initial research, under the topic of online privacy protection strategies of children. The research was conducted in Vienna, Austria, between the years 2018 and 2019 and involved a total of 18 focus groups with a sample of 116 children focused on three different age groups nine, 12 and 14-16. Vienna is characterised by the high quality of life and diversity among the population with high migration rates (City of Vienna, n.d.) which is depicted in the sample as the schools were chosen from districts of low, middle and high income and educational background. Additionally, the methodology of the initial research draws upon the LSE Global Kids Online methodology (Livingstone, Stoilova, & Nandagiri, 2019b; Livingstone, Stoilova, Yu et al., 2018) and follows ethical procedures ensuring approval from University Ethics Committee, schools directorates and parental i.e. guardians' consent. Specifically, all the required ethical processes were conducted to secure the approval of the Ethics Committee. Written informed parental consents were collected. In addition to parental consent, children's explicit oral consent was sought before proceeding. The researchers explained the research aims and processes in child friendly language, informing children that their participation is voluntary and can be withdrawn any time of the research without facing any negative consequences. Finally, the entire process was carried out on the basis of the General Data Protection Regulation and the participants' data were fully anonymised.

The method of the present study is a qualitative meta-synthesis which systematically synthesises qualitative findings from the existing research to form an understanding of AI privacy literacy. The method of meta-synthesis consists of the following steps drawing upon Chrastina's (2018) model, which were applied to the initial research:

1. Deciding the phenomenon of interest: The aim of the synthesis is to contribute to the scientific discourse and "design conceptual models of the phenomenon" (Chrastina, 2018, p. 115). This study aims to map the intersection of media, digital

privacy and AI literacy through three different age groups of children.

2. Deciding what is relevant: This study is a meta-synthesis conducted based on the initial research, which described privacy understanding and online privacy protection strategies of children.

3. First coding of concepts: The data were carefully read in order to highlight the information related to media and digital privacy literacies.

4. Finalising the coding: In this study, after deriving the first themes, the researchers identified associations between them.

5. Synthesising: This step involves the gathering of the themes and combining them meaningfully in order to map the themes' synthesis.

4. Findings

The findings are organised into key categories identified through the content analysis. First, media literacy and digital privacy literacy insights for each age group will be outlined. Afterwards, AI literacy relevant to each age group is introduced, based on the participants' media and privacy literacy levels.

Skills are presented below (Table 1) as they evolve across age categories whereby older children possess skills acquired earlier as well as the ones developed or experience-based skills.

Table 1

Comprehensive summary of media literacy and privacy literacy skills of the age groups nine, 12 and 14-16 years old alongside representative examples.

Nine-year-olds (early childhood)	12-year-olds (pre-adolescence)	14-16-year-olds (adolescence)
<i>Media Literacy</i>		
<p>Children understand the different types of media Example: children mentioned the use of different devices: smartphones, tablets and social media platforms: YouTube, WhatsApp, Instagram. Different purposes of online content and contacts Example: children mentioned they use media for: texting, uploading photos, playing online games.</p>	<p>Critical understanding of media content Example: children mentioned searching for information on google, playing online games and chatting with other players; they could evaluate if a message is from a reliable source; they blocked rude people. Managing online interactions Example: children mentioned they carefully choose their online contacts and block contacts in case of non-respectful communication.</p>	<p>Critical evaluation of digital content and corresponding actions Example: Children mentioned encountering fake accounts among their followers which they did not like, hence, they switched to private accounts to reduce such contacts and uphold their safety and privacy.</p>
<p>Permanent online data Example: children mentioned that the internet does not forget and knows everything about them.</p>	<p>Internet tracking Example: children mentioned that once data is on the internet they remain forever online.</p>	<p>Ability to perceive power structures of social media Example: children mentioned scandals of Facebook selling confidential information and that social media companies collect users' data.</p>
<p>Creating media Example: children mentioned taking photos, making videos and sharing on social media.</p>	<p>Creating media content Example: children mentioned having many accounts on different platforms; they frequently post different contents such as comments to stories, they share location, songs, photos, pictures, they upload videos they make with friends.</p>	<p>Developed abilities related to producing and distributing media content Example: children mentioned they are independent to download and use all applications; they switch to different platforms based on their needs; they are aware of different options in each platform e.g. on Instagram they do comments, reels, posts, they have many followers.</p>

<p>Dealing with online risks Example: children mentioned they were connected in social media only with people they personally knew and they deleted messages they did not understand.</p>	<p>Ethical aspect of online contacts Example: children mentioned they ask for their friends' approval to upload photos with them. Strategies against risks Example: children mentioned they used fake names and fake ages; children made settings with parents or even alone; children distinguished between private and public accounts.</p>	<p>Risk prevention Example: children mentioned they disable GPS to avoid sharing their location for privacy reasons.</p>
<p>Rules and parental mediation Example: children requested help from their parents when they received messages they could not understand and followed rules.</p>	<p>Gradual self-regulation of media consumption Example: children mentioned that they decide when and how long to use social media, what media to download and parents provide approval. Limited parental mediation Example: they mentioned their parents discussing privacy topics.</p>	<p>Self-regulation of media use Example: children proactively protect themselves and mention they switch to private accounts to control the contacts who access the information they post. Rejection of parental mediation Example: children mentioned they do not want to be connected with their parents on social media.</p>
<p><i>Digital Privacy Literacy</i></p>		
<p>Basic privacy perception Example: children mentioned their conversations, their name, age and password.</p>	<p>More developed understanding of personal information Example: children referred to permission about private information and mentioned they use fake names and age.</p>	<p>Advanced understanding of personal data Example: children mentioned that privacy is related to their own decision: it is under their control to share personal information.</p>
<p>Basic protection of digital privacy as users Example: children mentioned not wanting to share their name or their age on the internet. Online digital risks Example: children mentioned that thieves can come to their house.</p>	<p>Weak strategies to manage privacy protection, start trying to make settings Example: children mentioned they try to read terms and conditions, they used the words private and public accounts. They can identify scams and misinformation, and avoid it Example: children mentioned they would not respond to messages of people they do not know.</p>	<p>Ability to manage privacy settings Example: children mentioned they regulate privacy settings from public to private, giving or denying access to their contacts. They perceive the importance of consent when sharing online and partly the consequences of online sharing Example: children mentioned some children always ask for friends' permission before posting on social media about them.</p>

<p>First comprehension of digital footprints Example: children mentioned that the internet knows everything about them.</p>	<p>Awareness of digital footprint Example: children mentioned data cannot be deleted from the internet, even if they delete it from their accounts.</p>	<p>Ability to minimise digital footprint Example: children mentioned future repercussions, such as employee profile checks by companies; they have to be careful as what they post stays permanently on the internet.</p>
<p>Terms and Conditions (T&C) only with parental support Example: children mentioned that just close the messages or ask their parents to deal with this.</p>	<p>They are aware of existence of privacy policies but find it difficult to follow up Example: children mentioned they do not ask for parental permission to download applications, they said they inform their parents afterward.</p>	<p>Limited ability to comprehend privacy policies at their general points Example: children mentioned that they have to accept the T&C whether they agree or not, whether they understand or not, because it is necessary to use the application.</p>
<p>Parental mediation is strong and plays important role Example: children download applications with parental approval.</p>	<p>Limited parental mediation Example: children mentioned that their parents discuss with them about privacy topics but also children mentioned they do not want parental monitoring.</p>	<p>Independence and self-regulation on privacy issues Example: children mentioned that even though they love their parents, they deny having them in their online contacts.</p>

4.1. Media Literacy: Types, Purposes and Critical Evaluation

Children understand the different types of media starting with small steps at the age of nine and expanding in preadolescence and adolescence. Children learn with the support of their parents about media devices, their purposes and their functions. Starting with a few contacts restricted to family members and close friends, many children are regular social media users, such as YouTube, WhatsApp or Instagram, also found by Smahel et al. (2020). However, their activities are still under parental supervision. Children are active users as they send messages, have profile pictures, send emojis and play online games. At the same time, this age group starts experimenting with media production, taking photos or producing videos and even publishing them on social media. As children's skills in this age group are basic, parents play a key role in enabling media use while also ensuring children's protection. Nevertheless, appropriate formal education lacks to support children's media skills and the responsibility lies on parents.

By the age of 12, children have more confidence to explore the tools and opportunities platforms provide. Children perceive that different platforms serve other purposes. Parents' role is supportive, aiming to balance between active and monitoring practices, also found in Kalmus et al. (2022), but children seek to self-regulate their

media consumption and rely on parental help when confronted with issues exceeding their skills. Children's media skills allow them to produce more quantitative and diversified media content and at the same time their understanding of digital footprints grows. They are aware that the data they upload cannot be erased from the internet even if they delete it from their account, also found in Buchanan et al. (2017). Moreover, the 12-year-olds also have more online contacts, not just close family and friends. They have developed skills to manage connections; they decide to accept or deny online contacts; they remove existing contacts; they can distinguish fake accounts. The quality of skills in this age group is more advanced than younger children, enabling them to be more active on social media and thus exposed to more risks. However, structural factors represent the most important barriers to the efficacy of literacy.

In adolescence children aged 14 to 16 showcase advanced skills in using social media platforms, they own many accounts on different platforms. They want to be independent and self-regulated, even though parental support in the form of discussions and settings is still apparent, also found in Kalmus et al. (2022). For teenagers to maintain their privacy against their parents, they reject parental support and block them from social media. Adolescents have developed skills to use multimedia tools to create videos and podcasts that communicate their ideas and needs. They are confident users of a variety of tools and devices. They have numerous online contacts and are conscious of social media account management; such as, they choose to allow contacts, have public profiles or aim for private profiles. Teenagers are able to distinguish online sources and question their reliability to an extent. Children also understand that their data is harvested by platforms and have a "theoretical" understanding that platforms could potentially manipulate their data against them in the future. As the role of parents is being perceived as an invasion, or with insufficient knowledge, children of this age group rely on using their existing literacy skills in a self-empowering way to navigate media, which underlines the pressing need for regulation and education to support them.

4.2. Building Privacy Awareness and Control

Children aged nine have already developed an understanding, albeit very limited, regarding their online and offline privacy, such as personal information, their name, address and information about their family. They tend to protect their personal information and feel insecure sharing it online. At the same time, many children share their names and pictures of themselves without being aware of the online risks. Children learn about rules and have developed some

primary protection strategies to deal with things they do not understand, mostly by deleting the app or the message or asking for support from parents or older siblings. Parents' role is important regarding downloading and subscriptions on social media and other platforms, aligning with the Ofcom (2017) study. Children are not aware of digital footprints and the fact that their online activities and information are collected by companies and are permanent online and they connect privacy risks with burglary. Still, they have an abstract all-encompassing view that the internet "knows" everything about them.

At the age of 12, children perceive privacy in more sophisticated ways: they refer to online privacy as the information that refers to their identity and they perceive the right to decide whether to share or hide private information. Children tend to avoid sharing private data on the internet, using fake names and the same applies to their age and profile photo, also found in Stoilova et al. (2020). They are aware of online privacy risks, which agrees with the findings of Kumar, Naik et al. (2017), that online platforms track and collect their data, accessing information, such as their home address, location and contacts. However, they do not showcase awareness of further complexities of data harvesting, such as companies selling their information to third parties and monetisation from their data. Children are able to identify suspicious messages and avoid clicking or downloading from unknown sources that could be harmful. Children face unequal systemic challenges that cannot be overcome because the moment they exercise their right to access media, they are also fighting to protect their right to privacy. Even if they have a private account, platforms continue to collect data on their activities and this can only be regulated through strong regulatory measures against platforms and by promoting literacy and awareness among children from a young age.

In adolescence, children between 14 and 16 have developed a solid understanding of the forms of personal data including location, photos and biometric data, which exceed their name and birthdate, which aligns with Livingstone, Stoilova, and Nandagiri (2019a). They comprehend that data is collected by companies and platforms and there is targeted advertising and tracking. Additionally, they are aware of the risks of sharing intimate content and that their digital footprint could potentially impact their future, demonstrating long-term thoughts, on the basis that online information is permanent. At the same time, they acknowledge that engaging with online platforms requires giving up aspects of their privacy. While media and digital privacy literacy are valuable tools, relying solely on these skills at the current pace will leave future citizens at a disadvantage. We argue that a fundamental regulatory change is needed to protect minors' privacy.

4.3. Navigating Online Risks and Regulations

Dealing with online risks, nine-year-old children have developed some basic strategies to cope, largely based on parental guidance. Nevertheless, the conditions under which they enter social media are unknown to them and beyond their developmental level. Their self-protection is restricted to closing or accepting pop-up messages - mostly in order to continue their online activity. They keep a small number of online connections and use fake information about themselves. Their technological skills are also limited and they rely on parents for information and management of settings.

In pre-adolescence, children have already developed awareness of basic rules and regulations. Children try to read and comprehend terms and conditions of platforms but the language is demanding, therefore they still pursue parental support. At the same time children start developing skills regarding privacy settings. Even though they are aware of private and public online accounts, they generally make the settings with parental support or just accept the automated settings offered by platforms, also found in Cricchio et al. (2021). Children are mostly unaware of current privacy policies. They avoid seeking parental permission to download and sign up on social media platforms and inform their parents afterwards.

Older children, aged 14 to 16, understand key points of the policies related to privacy matters. However, as the language of the terms and conditions is still demanding, they tend to accept the terms and conditions. Regarding privacy protection, teens have developed some skills to handle privacy settings and manage who has access to the information they post and even control their followers. They can switch from public to private accounts and unfollow or block online contacts, which agrees with Kumar, O'Connell et al. (2023). Additionally, they are aware of location-sharing settings and know how to turn off location services on apps and devices when not necessary, recognising that their data is often used by companies to track behaviour and adapt ads accordingly. In this age group, parental mediation is not welcome since adolescents perceive parental control as an invasion of their privacy, also found in the study of Savic et al. (2016).

In both areas of media and data protection literacy, developments reflect a gradual shift from external dependence to internal reliance and, accompanied by a gradual increase in critical assessment, self-regulation and an understanding of long-term impacts. The development of these skills evolves with the cognitive and other developmental stages of children. At the same time, it is important to note that technological architecture, particularly around privacy,

which includes both the management of settings and functions and the conditions under which the platform's environment allows its usage, remain beyond the reach and control of young users. Despite the advanced level of digital privacy literacy of this age group, teenagers are being disempowered by structural factors that turn children's need for connection and socialisation into a product (Richards, 2021). This is fuelled by the complexification of AI-driven systems being integrated in children's lives. However, AI privacy literacy has never been more essential than it is now.

4.4. AI Privacy Literacy

Against the above mapping of media and digital privacy literacies, in this section, we attempt to map the ways in which AI-related functions correspond at each age level.

At the age of nine, reflecting the results of Okkonen and Kotilainen (2019), children are able to start perceiving the concept of privacy and they develop an interest in protecting their online privacy. However, the concept of AI is very complex and they can comprehend and discuss it based on terms connected to their everyday experiences, such as "smart technologies" voice assistants and smart toys. At the age of nine children can understand AI as helpful tools and the fact that the platform remembers children's choices and preferences and suggests similar ones. Regarding online privacy protection, children can learn that smart systems collect information to support them, but it is important to ask for parental permission before giving apps or devices personal information, including their own voices. Children should be aware of what kind of information should be protected and not shared with smart technologies. Finally, children can learn basic privacy settings such as muting a microphone.

At the age of 12, children are transitioning to a deeper understanding of personal data and are able to handle more complex discussions about how systems work and the consequences of certain digital behaviours. They also begin to use social media platforms more frequently, making this a critical age for learning how algorithms work. Children are able to learn about tracking systems of platforms based on their preferences in order to suggest similar content. Another issue for this age group is data collection in apps and games, which use AI to tailor experiences to the user but at the same time they collect data. Children at this age are able to perceive that every interaction on the internet leaves a digital footprint and AI uses those footprints to customise their online experience. Moreover, children can be introduced to AI-targeted advertising. When they search for a product, they may see advertisements for similar products as the AI

tracks their internet searches. The focus should be placed on how children can manage their privacy settings to control who has access to their data such as posts, location information and preferences. Finally, this age group can be introduced to data privacy laws and how they protect young users' privacy. The results echo the studies of Mertala et al. (2022) and Ali et al. (2021).

At the age of 14 to 16, aligning with in line with the studies of Bendeche et al. (2021) and Hartwig et al. (2024), children have developed strong privacy literacy skills and eventually they use a variety of AI-driven technologies such as social media, gaming and search engines. At this age group, children are able to perceive the way AI intersects with broader ethical issues, especially regarding privacy. Children can engage with the complexities of facial recognition technology, used in different instances of everyday life from unlocking phones to public surveillance, and the privacy consequences. Another topic of discussion are the ethical concerns and how AI systems handle large-scale data analysis, such as providing targeted content and advertisements. Teens are able to understand that the more data AI collects about themselves, the more accurately it can predict their preferences, raising concerns about autonomy and privacy protection.

The development of media and digital privacy literacy through the three age groups and what skills children are able to learn regarding AI privacy literacy are presented in Table 2.

Table 2

Level of media and digital privacy literacy through the three age groups and what skills children are able to learn regarding AI privacy literacy.

	<i>Level of media literacy</i>	<i>Level of digital privacy literacy</i>	<i>What can children learn on the era of AI privacy literacy</i>
<i>Nine-year-olds (early childhood)</i>	Basic usage of devices, some knowledge of social media platforms	Limited understanding of online privacy, without understanding long-term consequences of sharing information	Able to develop minimal, if any, understanding of algorithms or data collection by AI systems
<i>12-year-olds (pre-adolescence)</i>	Active engagement and use of social platforms, media creation, they own devices, have many different accounts and many contacts not only family members	Growing awareness of privacy and settings, but may have difficulties to manage them without any parental support	Able to learn basic traits of AI-driven content recommendations but limited knowledge of how data is collected and used
<i>14-16-year-olds (adolescence)</i>	Competent with social media, content creation and complex navigation	High understanding of privacy settings, management of online data and autonomy	Able to raise awareness of how AI affects their online choices and a more critical perspective on data privacy

5. Conclusions

In response to the need for media literacy from studies focused on digital privacy and especially embedded AI systems, this study aimed to map children’s competencies and highlight persisting obstacles to a meaningful function of literacy in their everyday lives. We regarded media literacy and such skills as the basis and starting point of interaction with platforms and their contents, hence connecting basic “traditional” skills around usage of media and origins of messages to the complexity of social media across technological features of engagement and interaction; content creation, sharing and consumption; conditions of usage affecting privacy protection; and finally self-empowerment and control across these domains. The embeddedness of AI in social media raises significant concerns about protection of children’s privacy rights: on the one hand, the field of AI is rapidly developing largely without clear parameters of possible consequences for users. Global and EU policies aim to regulate around the principles of development of AI, with rather weak

understandings and provisions of potential future consequences. In other words, this is an unexplored territory for policymakers and for users, who find themselves unknowingly interacting with AI and at a disadvantage vis a vis forms and degrees of control. With these concerns in mind, we mapped skills relevant across two domains of privacy (media and digital aspects) and aimed to project those on the emerging demands deriving from expanding AI.

This study underscores the importance to introduce media literacy at a young age to children to develop stronger data protection skills that enable children to navigate digital environments in more empowered ways (Buchanan et al., 2017; Kumar, Naik et al., 2017; Livingstone, Stoilova, Yu et al., 2018; Stoilova et al., 2020). Yet, this basic understanding must be juxtaposed to the uneven, indeed enorm imbalance, power of young users and platforms. Despite strong EU based regulations, the very technical design of platforms shapes the degrees to which even savvy users can protect their privacy. Often, the ultimate solution for adequate protection lies in the total denial of use of social media platforms, a choice which is not only disadvantageous for young people, but also highly unpopular. Between total “off” platforms choices and literacy informed choices online, there is a large gap which pushes action to possible extremes.

Amidst severe existing obstacles to the meaningful protection of privacy online, another layer of complexity characterised by lack of transparency derives from the introduction of AI to the mundane and more serious functions of the digital world. Based on media and data protection skills, the study presented an overview of the AI competencies that children, pre-adolescents and adolescents would require, in order to partly meet some of the challenges of their data protection. Drawing upon the call of Kumar, O’Connell et al. (2023) for more theoretical frameworks that are based on children’s involvement, for their empowerment in navigating privacy challenges. The study highlights the need for age-appropriate AI education that introduces children to the AI concepts (Ali et al., 2021; Bendeche et al., 2021; Mertala et al., 2022). Effective privacy and AI literacy education should be age-appropriate and evolve alongside children’s development. There is a call for media literacy which equally entails digital privacy literacy and AI as part of the compulsory curriculum as children interact with it in their daily lives. We argue that a comprehensive literacy framework can provide children with comprehensive skills for managing digital risks meeting the necessity of understanding AI concepts, as a requirement for children to be more capable to deal with their implications and learn how to safeguard their personal data.

However, ultimately, as literacy needs evolve, the concept itself requires a constant reassessment, particularly when it comes to

translating it to policy and practical action. In the AI era, especially the early stages we are experiencing currently, literacy might need to mean, at a minimum, basic understandings of coding and design of AI as a core component of education from nurseries to end of school. Moreover, surrounding the issue of privacy are challenges that cannot be tackled by attention merely on the individual responsibility of children, as educational, market, technological and human rights and public policy aspects merge powerfully providing us with the urgent need to overhaul basic literacy understandings and practices that have served with some degree of success young generations. The implications of disempowered citizens are unfathomed for the purposes of democratic participation and realisation and it is our conclusion through the above exercise and exploration.

Authorship and Contribution

Katharine Sarikakis: Conceptualisation, Supervision, Investigation, Methodology, Project administration, Resources, Writing – review & editing, Visualisation

Angeliki Chatziefrimidou: Data curation, Formal analysis, Investigation, Writing – original draft, Visualisation

Biographical Notes

Katharine Sarikakis (PhD Glasgow Caledonian University) is a professor of Communication Science at the University of Vienna/ Department of Communication. She has held positions as Santabder Chair of Excellence at Universidad Carlos III de Madrid, visiting senior fellow at London School of Economics and Political Science, affiliate fellow at University of Witwatersrand among others. She has consulted with international organisations such as the Council of Europe and Organization for Security and Co-operation in Europe and has received the Jean Monnet Chair and the Jean Monnet Centre of Excellence awards for research and policy on European integration in the fields of democracy and communication. Her research interests include media governance, media organisation and media industries.

Angeliki Chatziefrimidou, who holds a Master of Arts from the University of Vienna, is a predoctoral researcher in the Department of Communication at the University of Vienna. Her research interests include children and youth as media users, children's rights and online safety.

References

- Ali, S., DiPaola, D., Lee, I., Sindato, V., Kim, G., Blumofe, R., & Breazeal, C. (2021). Children as creators, thinkers and citizens in an AI-driven future. *Computers and Education: Artificial Intelligence*, 2, Article 100040. <https://doi.org/10.1016/j.caeai.2021.100040>
- Baykal, G. E., Van Mechelen, M., & Eriksson, E. (2020). Collaborative technologies for children with special needs: A systematic literature review. In *Proceedings of the 2020 CHI conference on human factors in computing systems* (pp. 1–13). Association for Computer Machinery. <https://doi.org/10.1145/3313831.3376291>
- Bendeche, M., Tal, I., Wall, P.J., Grehan, L., Clarke, E., Odriscoll, A., Der Haegen, L.V., Leong, B., Kearns, A. & Brennan, R. (2021). AI in my life: AI, ethics & privacy workshops for 15-16-year-olds. In O. Senevirtane, V. Singh, A. Freire, & J.-D. Luo (Eds.), *Companion Publication of the 13th ACM Web Science Conference 2021* (pp. 34–39). Association for Computing Machinery. <https://doi.org/10.1145/3462741.3466664>
- Buchanan, R., Southgate, E., Smith, S. P., Murray, T., & Noble, B. (2017). Post no photos, leave no trace: Children’s digital footprint management strategies. *E-learning and digital Media*, 14(5), 275–290. <https://doi.org/10.1177/2042753017751711>
- Buckingham, D. (2015). Defining digital literacy — What do young people need to know about digital media? *Nordic Journal of Digital Literacy*, 10, 21–35. <https://doi.org/10.18261/ISSN1891-943X-2015-Jubileumsnummer-03>
- Carretero, S., Vuorikari, R., & Punie, Y. (2017). *DigComp 2.1: The digital competence framework for citizens with eight proficiency levels and examples of use*. European Union. <https://doi.org/10.2760/38842>
- Choi, S. (2023). Privacy literacy on social media: Its predictors and outcomes. *International Journal of Human–Computer Interaction*, 39(1), 217–232. <https://doi.org/10.1080/10447318.2022.2041892>
- Chrastina, J. (2018). Meta-synthesis of qualitative studies: Background, methodology and applications. In *Proceedings of the 2nd International Conference on Social Sciences and Humanities (NORDSCI)* (pp. 113–124). NORDSCI.
- City of Vienna. (n.d.). *Vienna in a global context*. Retrieved March 5, 2024, from <https://www.wien.gv.at/english/politics/international/comparison/>

- Cooke, D., Edwards, A., Barkoff, S., & Kelly, K. (2024). *As good as a coin toss human detection of ai-generated images, videos, audio, and audiovisual stimuli*. ArXiv:2403.16760. <https://doi.org/10.48550/arXiv.2403.16760>
- Cricchio, M. G. L., Palladino, B. E., Eleftheriou, A., Nocentini, A., & Menesini, E. (2021). Parental mediation strategies and their role on youths' online privacy disclosure and protection. *European Psychologist*. Advance online publication. <https://doi.org/10.1027/1016-9040/a000450>
- Culver, S. H., & Grizzle, A. (2017). *Survey on privacy in media and information literacy with youth perspectives*. UNESCO Publishing. <https://unesdoc.unesco.org/ark:/48223/pf0000258993.locale=en>
- Damberger, T. (2013). „Halbmedienkompetenz?“ – Überlegungen zur kritischen Dimension von Medienkompetenz. *Medienimpulse*, 51(1), 1–17. <https://doi.org/10.21243/mi-01-13-02>
- European Union Agency for Fundamental Rights. (2020). *Fundamental rights report 2020*. Publications Office of the European Union. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-fundamental-rights-report-2020_en.pdf
- Frau-Meigs, D. (2016). *Media education*. UNESCO. <https://doi.org/10.54676/UYKM6672>
- Gapski, H. (2001). *Medienkompetenz. Eine Bestandsaufnahme und Vorüberlegungen zu einem systemtheoretischen Rahmenkonzept*. Westdeutscher Verlag. <https://doi.org/10.1007/978-3-322-87335-4>
- Hartwig, K., Biselli, T., Schneider, F., & Reuter, C. (2024). From adolescents' eyes: Assessing an indicator-based intervention to combat misinformation on TikTok. In F. F. Mueller, P. Kyburz, J. R. Williamson, C. Sas, M. L. Wilson, P. Toups, & I. Shklovski (Eds.), *Proceedings of the CHI Conference on Human Factors in Computing Systems* (pp. 1–20). Association for Computing Machinery. <https://doi.org/10.1145/3613904.3642264>
- Hugger, K. U. (2008). Medienkompetenz. In U. Sander, F. von Gross, & K. U. Hugger (Eds.), *Handbuch Medienpädagogik* (pp. 93–99). VS Verlag für Sozialwissenschaften.
- Kalmus, V., Sukk, M., & Soo, K. (2022). Towards more active parenting: Trends in parental mediation of children's internet use in European countries. *Children & Society*, 36(5), 1026–1042. <https://doi.org/10.1111/chso.12553>

- Kerry, C. F. (2018, July 12). *Why protecting privacy is a losing game today — And how to change the game*. The Brookings Institution. <https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game>
- Kumar, P., Naik, S. M., Devkar, U. R., Chetty, M., Clegg, T. L., & Vitak, J. (2017). 'No telling passcodes out because they're private': Understanding children's mental models of privacy and security online. In C. Lampe, J. Nichols, K. Karahalios, G. Fitzpatrick, U. Lee, A. Monroy-Hernandez, W. Stuerzlinger (Eds.), *Proceedings of the ACM on Human-Computer Interaction, 1(CSCW)* (pp. 1–21). Association for Computing Machinery. <https://doi.org/10.1145/3134699>
- Kumar, P. C., O'Connell, F., Li, L., Byrne, V. L., Chetty, M., Clegg, T. L., & Vitak, J. (2023). Understanding research related to designing for children's privacy and security: A document analysis. In *Proceedings of the 22nd Annual ACM Interaction Design and Children Conference* (pp. 335–354). Association for Computing Machinery. <https://doi.org/10.1145/3585088.3589375>
- Kumaresamoorthy, N., & Firdhous, M. F. M. (2018). An approach of filtering the content of posts in social media. In A. Rocha, & T. Guarda (Eds.), *2018 3rd International Conference on Information Technology Research (ICITR)* (pp. 1–6). IEEE.
- Livingstone, S., Bulger, M., Burton, P., Day, E., Lievens, E., Milkaite, I., De Leyn, T., Martens, M., Roque, R., Sarikakis, K., Stoilova, M., De Wolf, R. (2022). Children's privacy and digital literacy across cultures: Implications for education and regulation. In L. Pangrazio & J. Sefton-Green (Eds.), *Learning to live with datafication* (pp. 184-200). Routledge.
- Livingstone, S., Stoilova, M., & Nandagiri, R. (2019a). *Children's data and privacy online: Growing up in a digital age: An evidence review*. London School of Economics and Political Science. https://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf
- Livingstone, S., Stoilova, M., & Nandagiri, R. (2019b). *Talking to children about data and privacy online: Research methodology*. London School of Economics and Political Science. <https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Talking-to-children-about-data-and-privacy-online-methodology-final.pdf>

- Livingstone, S., Stoilova, M., Yu, S., Byrne, J., & Kardefelt-Winther, D. (2018). *Using mixed methods to research children's online opportunities and risks in a global context: The approach of Global Kids Online*. LSE Research Online. https://eprints.lse.ac.uk/84711/7/Livingstone__using-mixed-methods-to-research.pdf
- Mertala, P., Fagerlund, J., & Calderon, O. (2022). Finnish 5th and 6th grade students' pre-instructional conceptions of artificial intelligence (AI) and their implications for AI literacy education. *Computers and Education: Artificial Intelligence*, 3, Article 100095. <https://doi.org/10.1016/j.caeai.2022.100095>
- Ofcom. (2017). *Children and parents: Media use and attitudes report*. <https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/media-literacy-research/children/childrens-media-literacy-2017/children-parents-media-use-attitudes-2017.pdf?v=322847>
- Okkonen, J., & Kotilainen, S. (2019). Minors and artificial intelligence: Implications to media literacy. In Á. Rocha, C. Ferrás, & M. Pas (Eds.), *Information technology and systems: Proceedings of ICITS 2019* (pp. 881-890). Springer. https://doi.org/10.1007/978-3-030-11890-7_82
- Ramachandran, A., Huang, C.-M., & Scassellati, B. (2017). Give me a break! Personalized timing strategies to promote learning in robot-child tutoring. In B. Mutlu, M. Tscheligi, A. Weiss, & J. E. Young (Eds.), *Proceedings of the 2017 ACM/IEEE International Conference on Human-Robot Interaction* (pp. 146-155). Association for Computing Machinery. <https://doi.org/10.1145/2909824.3020209>
- Rasi, P., Vuojärvi, H., & Ruokamo, H. (2019). Media literacy education for all ages. *Journal of Media Literacy Education*, 11(2), 1-19. <https://doi.org/10.23860/JMLE-2019-11-2-1>
- Richards, A. (2021). TikTok: The darkside of surveillance. *Critical Reflections: A Student Journal on Contemporary Sociological Issues*, (9). <https://ojs.leedsbeckett.ac.uk/index.php/SOC/article/view/4614>
- Sas, M., Denoo, M., & Mühlberg, J. T. (2023). Informing children about privacy: A review and assessment of age-appropriate information designs in kids-oriented F2P video games. In J. Nichols (Ed.), *Proceedings of the ACM on Human-Computer Interaction*, 7(CHI PLAY) (pp. 425-463). Association for Computing Machinery. <https://doi.org/10.1145/3611036>

- Savic, M., McCosker, A., & Geldens, P. (2016). Cooperative mentorship: Negotiating social media use within the family. *M/C Journal*, 19(2). <https://doi.org/10.5204/mcj.1078>
- Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., and Hasebrink, U. (2020). *EU Kids Online 2020: Survey results from 19 countries*. EU Kids Online. <https://doi.org/10.21953/lse.47fdeqj01of0>
- Stoilova, M., Livingstone, S., & Nandagiri, R. (2020). Digital by default: Children's capacity to understand and manage online data and privacy. *Media and Communication*, 8(4), 197–207. <https://doi.org/10.17645/mac.v8i4.3407>
- UNICEF. (2020). *How many children and young people have internet access at home? Estimating digital connectivity during the COVID-19 pandemic*. UNICEF. <https://data.unicef.org/resources/children-and-young-people-internet-access-at-home-during-covid19/>
- UNICEF. (2021). *Policy guidance on AI for children: Recommendations for building AI policies and systems that uphold child rights (Version 2.0)*. UNICEF Office of Research - Innocenti. <https://www.unicef.org/innocenti/reports/policy-guidance-ai-children>
- Wang, G., Zhao, J., Van Kleek, M., & Shadbolt, N. (2022). Informing age-appropriate ai: Examining principles and practices of ai for children. In S. Barbosa, C. Lampe, C. Appert D. A. Shamma, S. Drucker, J. Williamson, & K. Yatani (Eds.), *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (pp. 1–29). Association for Computing Machinery. <https://doi.org/10.1145/3491102.3502057>
- Zulkifli, A. (2022). TikTok in 2022: Revisiting data and privacy. *Computer*, 55(6), 77–80. <https://doi.org/10.1109/mc.2022.316422>

AmeliCA

Available in:

<https://portal.amelica.org/amelica/amelica/journal/819/8195202006/8195202006.pdf>

How to cite

Complete issue

More information about this article

Journal's webpage in portal.amelica.org

AmeliCA

Open Science for Common Good

Katharine Sarikakis, Angeliki Chatziefrimidou

Artificial Intelligence and Privacy: The Urgent Need for Children's Media Literacy

Inteligência Artificial e Privacidade: A Urgente Necessidade da Literacia Mediática das Crianças

Inteligencia Artificial y Privacidad: La Urgente Necesidad de la Alfabetización Mediática de los Niños

Revista Comunicando

vol. 14, no. 1, e025003, 2025

Associação Portuguesa de Ciências da Comunicação,
Portugal

comunicando@sopcom.pt

ISSN: 2184-0636

ISSN-E: 2182-4037

DOI: <https://doi.org/10.58050/comunicando.v14i1.422>



CC BY 4.0 LEGAL CODE

Creative Commons Attribution 4.0 International.