Data Protection Rights of the Child in the Digital Environment

Yordanka Noneva-Zlatkova, Suzana Rangelova, Petya Hadzhieva

South-West University "Neofit Rilski", Faculty of Law and History, Blagoevgrad, Bulgaria
noneva@law.swu.bg, rangelova@law.swu.bg, petyahadzhieva8@gmail.com

DOI
https://doi.org/10.18690/um.pf.8.2025.10

ISBN
978-961-299-056-5

Protecting children's personal data from a digital perspective is essential for preserving their privacy and ensuring their online security. The European Union's legal framework ensures the children's data protection by mandating parental consent for processing the personal information of minors under the age of 16 (Article 8, par. 1, Regulation 2016/679). This guarantees that children's personal data is handled with the highest level of care. These protections aim to limit the collection of unnecessary data and provide clear information on how children's data will be used. In addition, platforms are required to implement measures to protect children from exploitation, exposure to harmful content, and unauthorized sharing of data. The authors trace the latest penalties that are imposed on well-known internet platforms concerning the protection of children's data by various supervisory authorities. In this paper, the authors analyse the practice of the CJEU and the ECHR related to the protection of children's personal data and conclude the main challenges and opportunities for solutions in the current digital reality.

Keywords:
digital rights,
parental consent,
child-centric,
AI,
privacy

University of Maribor Press

1 Introduction

The importance of protecting children's personal data has grown exponentially over the past decade. Studies show that more and more children aged 6-16 spend time online. The largest study conducted in Europe on this topic is made by the international network "EU Children Online".[1] The 2020 study stands out as one of the few comprehensive sources of information on how children and youth in Europe use the Internet.[2] Furthermore, the Bulgarian State Agency for Child Protection, together with the Bulgarian Security Academy, conducted a survey among nearly 1,000 students from school grades 6, 7 and 8, which shows that the preferred social network among children is TikTok, followed by Instagram and Snapchat. Over 61% of the children surveyed say that they use them more than five times a day. Including the time on them, 70.8% of the students are online for one to three hours every day. 31% spend two to four hours of their day online. The analysis shows that over 83% of children know how to set their privacy settings themselves. Compared to the last similar study in Bulgaria conducted in 2016, this one shows a trend towards increasing this use, and from an increasingly early age.[3] In addition, it is observed that their skills for critical assessment, communication and cooperation are significantly lagging, most likely due to the slow adaptation of the education system to the new conditions and insufficient intervention and support from parents.

The above facts show that it is vitally important for children to feel fully protected in the digital environment, to conduct a comprehensive review of the law-making agenda, the existing case law on the key normative acts EU Charter of Fundamental Rights[4] and European Convention on Human Rights (ECHR)[5], among the actions taken by the individual administrative supervisory authorities to protect personal data in their defence. Accordingly, authors conclude about the challenges and future possible solutions to the maximum extent for the protection of children's personal data and the unique vulnerability of children, as well as their developmental needs.

[1] This is a research network surveying the kids digital participation.
[2] Smahel et al., 2020, p. 10.
[3] Bulgarian Agency for Child Protection, 2023.
[4] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT
[5] European Convention on Human Rights, available at: https://www.echr.coe.int/european-convention-on-human-rights

The legal framework at the EU, Council of Europe, UN level is decisive in protecting children's rights. Three legal instruments are essential for safeguarding children's personal data and their privacy rights, however, they have different legal bases, scope, and hierarchy. They set out the main criteria and guidelines for protecting children's personal data in the digital age.

2 Legal Framework of Children's Data Protection Rights under the General Data Protection Regulation, ECHR and Convention on the Right of Child in Digital Environment

GDPR[6], ECHR and Convention on the Rights of the Child (CRC)[7] serve as the primary framework governing the protection of children's personal data in the digital era. Although GDPR and ECHR have different legal status, scope and hierarchical value in the European legal system, they are of fundamental importance in deriving the basic principles on which the legal framework for the protection of children's personal data is based. The GDPR is adopted on the basis of Article 16 of the Treaty on the Functioning of the European Union (TFEU). Therefore, it is directly applicable and enforceable in all EU Member States in the field of data protection and is also related the principle of primacy.[8] Meanwhile the ECHR has a wider scope. It is an international treaty developed by the Council of Europe and is binding on 46 Member States, including all EU Member States. Oppositely, the GDPR regulates all individuals' personal data protection in the EU, including children, and sets uniform standards for such data administration and protection. Controversy, the ECHR is legally binding on the States that have ratified it and provides a basis for individual complaints to the European Court of Human Rights (ECtHR). It guarantees that the fundamental human rights, including the right to privacy (Article 8), which in turn is the basis of data protection legislation. Also, it follows that the GDPR has a more direct and binding effect on Member States, while the ECHR provides fundamental principles that indirectly influence legislation. For example, the GDPR can be seen as a concretisation of the right to privacy enshrined in Article 8 of the ECHR. The GDPR is therefore a specialised and legal act with direct

[6] 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. (2016). *Official Journal of the European Union*, L119, pp. 1–88 (GDPR).
[7] Convention on the right of child was adopted by the United Nations in 1989 and entered into force on September 2, 1990.
[8] Miąsik, 2023, pp. 201-224.

applicability for data protection at EU level, with advantage over national laws. The ECHR, in turn, is a fundamental international treaty that provides general principles for privacy protection and influences national and European legislation. While the GDPR deals with the details of data protection, the ECHR provides broader protection for fundamental human rights.

On the other hand, the CRC is also an international treaty. It is the most widely ratified international instrument for the protection of children's rights, except for the United States. Countries that have ratified the CRC are required to align their laws and policies with its principles and provisions. In most EU Member States, the CRC is binding at the national level upon ratification. It covers a wide range of children's rights, including the right to privacy (Article 16) and protection against abuse and exploitation, including in the digital space. The CRC provides a common framework for children's rights at the global level, influencing national legislation and international standards such as the GDPR and the ECHR. It does not have direct application, as the GDPR does, but requires implementation through national laws and policies. The GDPR provides specific and technical protection of personal data, including for children, while the ECHR and the CRC establish broader principles on the right to privacy and protection of children. The CRC is a fundamental international instrument that sets standards for the protection of children's rights, inspiring and complementing EU law, including the GDPR.

2.1 Legal Framework in the GDPR

The GDPR is a regulation with crucial role in the EU. It oversees the protection of personal data, including information belonging to children.[9] Provisions specifically relating to children in the digital environment are consistently addressed in several provisions of the GDPR. Such a clause, which has an important role for child protection rights, is Article 8 of the regulation. In the event of processing of a child's personal data in information society services (e.g., social networks, applications), the regulation requires the presence of consent. The GDPR stipulates that the child must give consent if they are 16 years old. In some Member States, the age may be lower, but not below 13 years. If the child is under the specified age, consent is required from a parent or guardian. Another provision of the regulation is that

[9] Voigt & von dem Bussche, 2024, pp. 9-36.

information on data processing must be presented in a language understandable to children. Controllers are also required to provide information on whether and how the principle of transparency is respected (Article 12 of the GDPR). Different controllers of children's personal data must design their services in such a way that they must have a high level of protection of personal data by default, especially for children (Article 25 of the GDPR). Besides, to minimize data collection and limit their processing. The GDPR regulates and encourages the creation of special codes of conduct for the protection of children's data, ensuring that they are easily understandable and applicable (Article 40 of the GDPR). As well, the European legislator grants the supervisory authorities the power to promote the creation of educational programs for the children's personal data protection (Article 57 of the GDPR). As a good example, the Bulgarian Authority prepares a manual on the rights of children while working with different digital platforms.[10]

2.2 Legal Framework in the ECHR

The right to protection of children's personal data in the ECHR is derived from the right to respect for private and family life (Article 8 of the ECHR). Children have rights against unlawful interference with their private and family life, among because of unlawful processing of personal data. Relating to the digital environment, this provision requires protection against unregulated surveillance, collection, and use of data.[11] Special care is required when processing data of groups exposed to vulnerability, such as children. Subsequently, freedom of expression comes (Article 10 of the ECHR). There, we guarantee the children's right to express their views, including surfing on different digital platforms. This right must be balanced against the need to protect against abuse and exploitation. Vis-à-vis the protection of children, the ECtHR has rendered judgments in cases brought under these provisions and based on them. It can be derived from principled statements that are of fundamental importance for the protection of children's personal data.

2.3 Legal Framework in the CRC

The CRC contains several specifics concerning data protection and children's digital rights. The right of the child to protection against random interference with his privacy, family, home or correspondence is proclaimed in Article 16 of the CRC.

[10] Bulgarian Commission for Personal Data Protection, 2022.
[11] O'Mahony, 2019, pP. 660-693.

Controversial Article 17 of the CRC highlights the significance of the child's access to information, while demanding safety against risky content. We cannot forget that the general principles for the child's best interest (Article 3 of the CRC), right to participation and expression of views (Article 12 of the CRC) and prohibition of discrimination (Article 2 of the CRC) are proclaimed also. The CRC clearly states the principled maxim that the physical, psychological, and social well-being of children goes hand in hand with ensuring the defence of their data and secrecy.

To cut a long story short of the above legal analysis, it can be reasonably concluded that the three instruments are compatible with each other. The GDPR concretizes the principles of the CRC in the context of digital data. It is observed that parental consent for processing children's data under the GDPR reflects a specific measure in the execution of the conditions of the CRC in safeguarding the child's best interests[12]. On the other hand, based on the principled formulation of the protection of privacy in the ECHR, the specific provisions for children in the CRC are specified and built upon. In conclusion, in the EU Member States, the GDPR has a direct and binding effect on national law, while the CRC influences through implementation, and the ECHR is fundamental in the European context. It can therefore be said that the GDPR provides specific and technical personal data protection, involving children, whilst the ECHR and the CRC determine wider assumptions on the right to privacy and the protection of children. The CRC is a fundamental international instrument that sets standards for the protection of children's rights, encouraging and balancing EU law, involving the GDPR.

3 Children's Data Protection Rights Under GDPR and Administrative Measures by National Authorities on Personal Data Protection

The breakdown so far shows that the regulatory act with the highest reasonable significance for child data subjects is the GDPR. Within its application period, guidelines for the forthcoming development of the legal approach are taken established on concrete cases of children's rights breach to personal data protection. They are obtained from practical cases of infringements of the children's right to personal data protection. Thus, authors present a brief overview, without claiming

[12] März, 2022, pp. 3805-3816.

to be complete, of the most prominent cases of violations documented by national supervisory authorities concerning the children's personal data.

Actuality reveals that children are progressively spending more time online and on their mobile devices, playing games or having fun. This is why platform giants have become notorious for their unregulated gathering and use of children's data with no identifiable consent. This evidence has indicated the necessity to reinforce the care and accountability of technology companies that process children's data. Here are several of the cases:

a) First notable instance involved *YouTube (Google)* in 2019, where the platform was found to be collecting data from children under 13 years old who were using the platform. This data was then used for targeted advertising without obtaining verifiable parental consent, violating GDPR's strict rules regarding the processing of children's data. YouTube allegedly used cookies to track children's online behaviour, creating profiles to target ads, a practice that is explicitly restricted under GDPR. In response, YouTube implemented stricter policies, limiting data collection and ad targeting for content aimed at children. This case raised global consciousness about the threats of data misuse and the significance of parental consent.
b) Another troubling example *is Clearview AI*, a facial recognition company that scraped images from social media platforms and public websites, including those of minors, without obtaining consent. The company incorporated this data into a vast biometric database, violating GDPR's principles of explicit consent and data minimization, especially for sensitive data like biometric information. Therefore, Clearview AI faced cease-and-desist orders from EU data protection authorities, who also imposed fines. The company was ordered to delete all data related to EU citizens, including minors, and cease further data collection activities in the EU.
c) Similarly, *TikTok* came under inspection for its lack of proper age verification and transparency regarding children's data. Investigations in the UK and Netherlands revealed that TikTok's privacy notices and settings were not child-friendly, and children under 13 could easily create accounts without parental consent. This exposed young users to potential risks of tracking and profiling. The UK Information Commissioner's Office (ICO) fined TikTok £12.7 million

in April 2023. In response, TikTok strengthened its age verification processes and improved its privacy settings to ensure better protection for younger users.

d) *Instagram (Meta)* also faced issues with handling children's data. The platform, owned by Meta (formerly Facebook), was investigated by the Irish Data Protection Commission (DPC) for allowing children as young as 13 to create business accounts, which made their contact information publicly available by default. This violated GDPR's "privacy by default" principle, which mandates that platforms must prioritize high privacy settings for minors. Meta was fined €405 million in 2022, one of the largest fines under GDPR now. In response, Meta introduced more robust privacy measures, including making child accounts private by default and addressing the exposure of minors' personal information.

e) In conclusion, *Disney* was found to be collecting data from children through its mobile apps and online games without obtaining verifiable parental consent, violating GDPR's rules for users under the age of consent. Disney's apps used tracking technologies to gather children's behavioural data for analytics and targeted advertising without parental approval. Accordingly, Disney overhauled its apps and online services to fulfil the GDPR, implementing clearer privacy policies, requiring parental consent, and limiting data tracking features for children.[13]

These examples highlight the critical role of GDPR in protecting children's rights in the digital age. All serve as reminders of the dangers posed by digital platforms when companies fail to adopt proper data privacy practices. Tech companies must remain accountable for how they collect, process, and use children's data. The cases also underscore the requirement for strong, child-centric[14] privacy measures and more vigorous enforcement of regulations like GDPR to confirm that children's personal information remains protected. The study of GDPR violations across platforms like *YouTube, TikTok, Instagram, Clearview AI, and Disney* reveal recurring issues in handling children's data. Common breaches include insufficient age verification mechanisms, lack of transparency in data collection, and failure to obtain verifiable parental consent, as mandated by GDPR. Platforms also often violate GDPR principles like "privacy by default" leading to public exposure of children's data and improper

[13] FTC press releases or articles on the case from sources like The Verge or BBC News. The New York Times, Wired, or legal websites like Privacy International. The Guardian, TechCrunch, or official statements from the Irish Data Protection Commission. Articles from CNBC, Reuters, or TechCrunch.
[14] Milkaite, 2021, p. 5.

targeting through behavioural advertising. Significant fines and regulatory actions have pressured companies to improve their policies, highlighting the necessity for tough protection for minors' confidentiality in a digital perspective.

4 Analysis of the ECHR Case Law on Children'S Data Protection Rights

The case law of the ECtHR has consistently recognised in its judgements the obligation of the State to keep the rights of children versus interference with their privacy by third parties in the online world. Likewise, the Court identifies children as a vulnerable group in cases involving targeted advertising, algorithmic decision-making, tracking, and surveillance. In this regard, the decisions analysed below are of fundamental importance for the potential protection of children's rights in the online world.

4.1 K.U. v. Finland[15]

The case of *K.U. v. Finland* of the ECtHR is of great importance for the children's personal data protection in the digital sphere. It sets the grounds for the positive duties of States to guarantee the protection of minors' privacy. This case establishes fundamental principles that States must take strengthened and proactive measures to protect children's rights online. The case concerned an incident in which a 14-year-old Finnish child took intimate photographs of himself and sent them to a man with whom he had established a connection online. These photographs were published online without the child's consent. This had serious consequences for their private interests. In this case, the ECtHR judged whether the State had concluded its obligations to protect the child's right to privacy and the protection of personal data online. Therefore, the State identifies itself as a violator of the pact, meanwhile, it, through its authorities, should have taken measures not only to recognise the perpetrators but also to guarantee that analogous cases do not occur again, ensuring the safety of children who are exposed to threats in the digital age.

[15] *K.U. v. Finland, 2008*, app. no. 2872/02, 2 March 2009.

The ECtHR underlines two main principles:

f) States must not only abstain from violating the privacy right of citizens but must also take active steps to protect these rights. Through the prism of children, who are predominantly at risk in the online sphere, States must guarantee the protection of their personal integrity and data.
g) The ECtHR acknowledged that States must require adequate mechanisms to avoid harm caused by modern technological dangers such as cyberbullying, sexual exploitation and the infringement of the children's privacy. This includes creating policies that prevent the spreading of personal data and intimate images without consent.

So, the judgment explicitly highlights that the State has obligations to protect children's right to privacy and to take actions versus risks correlated to digitalization. In the digital age, where children are exposed to various types of abuse of personal data (such as the distribution of private photos, online violence, cyberbullying, etc.), states must provide effective legal protection. The ECtHR reports that states must take sufficient steps to provide legal protection for victims of online crimes, including through criminal and civil sanctions for those who execute such abuses. Subsequently, Council of Europe Member States, including those of the EU, are persuaded to develop stricter and more specific laws to protect children online. This includes establishing stronger regulations on the gathering and use of children's personal data online, alongside instruments to prevent online harassment and sexual exploitation. The judgment also suggests the necessity for learning and preventive programmes to inform children, parents, and schools about the risks associated with online activities and the significance of protecting personal data. The worldwide implications of the case relate to encouraging cooperation between different jurisdictions to protect children's personal data, especially when they are located outside the countryside where the breach occurred.

In conclusion, the aforementioned case law establishes an important precedent regarding the positive obligations of states to protect personal data and the children's right to privacy in the digitalization process. It highlights the prerequisite for active measures to protect children against the risks that may arise from technology and obliges States to guarantee that children's rights are adequately protected, including by creating legal frameworks and mechanisms to prevent online abuse. This case is

a substantial step in the process of legal protection for children in the modern digital world.

4.2 S.W. v. United Kingdom[16]

The case of *S.W. v. the United Kingdom* before the ECtHR analyses the right to privacy and the protection of personal data in the context of the digital perspective, with a distinct emphasis on the rights of the child and the protection of his or her personal data. Though this is not a case that straight concerns the processing of data online, it stresses the value of protecting personal data and the privacy of the most vulnerable groups, in particular children. The case concerns a woman known as S.W., who complained against the United Kingdom that the authorities had failed to take the required measures to protect her personal data and her right to privacy after sexually explicit intimate photographs were distributed without her consent. She alleged that she had not received effective protection from the authorities, even though these actions had seriously violated her right to privacy, including data protection. The present case is also applicable to children, although the case in question does not involve a minor. It provides an essential illustration of the responsibilities of States to guarantee the protection of personal data and the right to privacy, including for children. This is because of the expanding importance of digitalisation, where children and youth are at risk of misuse of their personal data. In the current case, ECtHR initiated that the United Kingdom had violated the applicant's right to privacy by failing to stipulate suitable instruments to protect her personal data and by failing to take the necessary actions to avoid the dissemination of her photographs without her consent. The Court emphasised that a State must not only avoid allowing violations of the right to privacy of its citizens, but also be obliged to actively take steps to protect personal information, particularly where vulnerable individuals are at risk of online abuse and exploitation. The Court further emphasised the importance of implementing adequate legal and technological tools to protect personal data in the digital environment. Such mechanisms include effective procedures for identifying, blocking, and removing unlawfully disseminated data, particularly where it contains sensitive information such as intimate photographs or videos. Although the case in question does not directly concern children, it sets out fundamental principles that are essential for the protection of

[16] *S.W. v. United Kingdom*, app. no. 87/18, 22 September 2021.

data and the right to privacy of children in the digital environment. These principles oblige States to ensure effective protection of the personal data of all individuals, including children. In cases of dissemination of intimate images or other sensitive information, children may not only be legally vulnerable but also be exposed to serious psychological consequences. States should, therefore, put in place effective mechanisms to prevent such violations and take action to protect personal data both after such violations have occurred and preventively. This may include educational initiatives and the progress of a legal framework to protect children from online exploitation and misuse of their personal information. The exploration of this judgment plays a key role in creating new policies and legal instruments to protect children's personal data online. This includes introducing stricter requirements for platforms and services that collect information from children and requiring them to obtain clear and explicit parental consent for the processing of the specific data. The judgment could lead to the imposition of new security standards, such as mandatory age verification, effective parental consent mechanisms, and transparency about how data is collected and used. The Court also stresses the importance of raising public awareness, particularly among parents and children, of their rights to privacy and data protection. This includes promoting educational initiatives that teach children how to protect their personal information in the digital environment.

The judgment under this case of *S.W. v. the United Kingdom* establishes basic principles on the commitments of States to defend personal data and the right to privacy of citizens, including in the perspective of the Internet. Although the case does not directly concern children, its conclusions have serious implications for their safety in the digital space. The decision highlights the responsibility of states to provide effective tools to protect personal information and prevent abuses that may affect the most vulnerable groups, such as children. This highlights the significance of protective measures, increased awareness, and adequate legal protection for adolescents in the online environment, as well as the necessity for specific policies to guarantee their rights and security.

5 Analysis of the CJEU Case Law on Children's Data Protection Rights

Several key cases can be drawn from the case law of the CJEU, which are of primary importance for the protection of children's personal data and for the more efficient application of their rights. In view of the major principles outlined, the view

expressed in the scientific literature that the decisions of the CJEU serve as a fundamental model for the protection of personal data can be reasonably supported.[17]

5.1 Case Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González[18]

In 1998, a Spanish newspaper published a notice of a public auction of assets related to the outstanding debts of Spanish lawyer Mario Costeja González. Even though the information was lawfully published, it remained available online long after his debts had been settled. In 2010, González discovered that links to these publications still appeared when searching for his name on Google, which he claimed violated his right to privacy. This provoked him to file a claim to the Spanish Data Protection Agency (AEPD), requesting that Google Spain and Google Inc. remove the relevant links from search results. The AEPD supported González's complaint, but Google challenged the decision, and the case went to the CJEU. The case raises several important questions. First, is Google subordinate to European data protection law, even though it is based in the United States? Second, is the search engine in charge of processing personal data included in search results? Finally, is there a "right to be forgotten" that allows individuals to request the deletion of data from the Internet? In its ruling, the CJEU ruled that European law is applicable. The argument is that Google Spain is part of the economic activity of Google Inc. in the EU, and the processing of data through the search engine is directly related to that activity. Google is, therefore, subject to European data protection laws, although the parent company is based outside the EU. The Court also concluded that Google, as the operator of a search engine, processes personal data when it reveals search results including personal information. Although Google does not control the content of the links published, it controls the way in which that data is presented in the results and is therefore liable for them. The CJEU also ruled that citizens have the right to request the removal of links containing personal data if the information is "inappropriate, outdated or excessive". However, this right should maintain equilibrium against the public interest in the information concerned. In the specific case of González, the Court found that his right to privacy balanced the public

[17] Marin, 2023, pp. 211-217.
[18] *Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, case no. C-131/12, ECLI:EU:C:2014:317, 13 May 2013.

interest. The Google Spain case was a landmark in the development of EU data protection law, as it established the principle of the "right to be forgotten". This principle was later enshrined in Article 17 of the GDPR. Consequently, Google introduced a mechanism through which European citizens can request the removal of links from search results, which has led to the processing of millions of such requests. The Google Spain case clearly shows that technology companies have an obligation to respect the right to data protection and privacy within the EU. The ruling of the CJEU underlines that citizens' digital rights are not limited to control over the information they publish themselves, but also include the way in which their personal data is processed and disseminated through search engines. This judgment sends a clear message to the big tech companies that European data protection standards will be applied strictly and without exception.

The 2014 case of *Google Spain SL v AEPD and Mario Costeja González* has a significant, albeit indirect, impact on the protection of children's personal data. It establishes the principle of the "right to be forgotten", which is of particular importance for more vulnerable groups such as children in the digital environment. This principle is particularly relevant for minors and minors, who often do not fully understand the consequences of publishing information about themselves online. Many children share personal data or create digital profiles that can have long-term consequences for their reputation and privacy. The "right to be forgotten" allows children or their parents to request the removal of inappropriate or sensitive information that has become public, even if the children themselves posted it. Leaving children's personal data available online for long periods can lead to risks such as cyberbullying, discrimination or abuse. The decision in this case demonstrates the need to balance the individual right to the protection of personal data with the public interest in information. However, in the context of children, the GDPR explicitly stresses that their protection must be a priority. Article 17 of the regulation specifies that the processing of children's data requires additional care, and that data removal must be easy and accessible. Following the decision, Google and other platforms have introduced mechanisms to remove search results, which is of particular importance for children. Parents or legal guardians can now request the removal of information relating to their child, including publications by third parties without the parents' consent, such as photos or personal data.

The principles thus established create a basis for future court decisions on issues relating to children's personal data. In cases of inaccurate use of children's data online, these principles provide important safeguards. Furthermore, the case forces companies that process children's data to put in place measures to comply with the right to erasure, which is a fundamental element of protection in the digital environment. In conclusion, the Google Spain case highlights the importance of the right to control personal data, which is very critical for children. Assigned their weakness and the risk of long-standing negative effects, the perception of trustworthy mechanisms for using the "right to be forgotten" is an important step towards ensuring greater protection for children in the digital world.

5.2 Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Schrems II)[19]

Case *C-311/18* between the Data Protection Commissioner, Facebook Ireland and Maximilian Schrems (known as Schrems II) plays a key role in regulating international data transfers, drawing precise supervision to the privacy risks associated with these practices. The case highlights the question of the legitimacy of transfers of personal data from the EU to the US and centres attention on the potential access of US security services to data of EU citizens. Impact on children: Children are particularly at risk in the perspective of transnational data transfers, as their digital footprints often start to form at an early age. This information can be used for marketing, tracking, or other unethical purposes if it is dropped into inappropriate hands. On 16 July 2020, the CJEU ruled that the Privacy Shield mechanism used to govern data transfers between the EU and the US does not meet the protection requirements set out in the GDPR. This ruling affects all users, including children, whose data may be administered by US companies. While CJEU confirms the validity of standard contractual clauses (SCCs) as a means of transfer, it stresses that companies must ensure that data recipients in third countries provide protection equivalent to that in the EU. US law allows government authorities to access personal data of foreigners without providing protection comparable to that in the EU, which highlights the need for stronger mechanisms. Platforms such as Facebook, which process large amounts of data, including children's data, are required to demonstrate that their transfers to third countries comply with the

[19] *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* (Schrems II), case no. C-311/18, ECLI:EU:C:2020:559, 21 August 2020.

GDPR. Services that children frequently use must minimise the threat of unlawful access to data. Following the Schrems II ruling, companies must implement additional safeguards, such as storing data in the EU or encrypting it before transfer. Parents and children must be informed in a clear and accessible manner about how their data is processed and transferred. This case demonstrates the importance of transparency and highlights that protecting children's personal data must be a priority. The established principles require technology companies to guarantee that children – as the most vulnerable group in the digital world – are adequately protected.

5.3 Case C-210/16 Wirtschaftsakademie Schleswig-Holstein GmbH v. Facebook Ireland Ltd.[20]

Case C-210/16 - *Wirtschaftsakademie Schleswig-Holstein GmbH v. Facebook Ireland Ltd.* is of fundamental importance in defining the obligations of data controllers, including when it comes to processing children's data. The judgment of the CJEU clarifies the obligations of all parties included in the processing of such data. Wirtschaftsakademie Schleswig-Holstein used a Facebook page for marketing purposes. The German data protection authority discovered that Facebook collected data by installing cookies on visitors' devices, without their consent or knowledge. Since social networks such as Facebook often attract children and young people, the handling of their data is a particularly sensitive issue. The main issue raised by the case relates to who is liable for defending the personal data of young users. On 5 June 2018, the CJEU ruled that responsibility for data processing is shared. As stated by the ruling, the administrator of the Facebook page (Wirtschaftsakademie) is considered a joint controller together with Facebook. This means that all participants who determine the purposes and means of processing must jointly ensure that they are in accordance with the conditions of the GDPR. They are obliged to inform users about the collection of data and how it will be administered, in compliance with the principle of transparency. The CJEU stresses that cookies can only be applied with users' explicit and informed consent. For platforms aimed at children, this requires additional safeguards. The GDPR requires parental consent for the data processing of children under a certain age (usually 16 in the EU). Administrators of pages must ensure compliance with these requirements by providing clear and

[20] *Wirtschaftsakademie Schleswig-Holstein GmbH v. Facebook Ireland Ltd.*, case no. C-210/16, ECLI:EU:C:2018:388, 5 June 2018.

accessible information to children and their parents. Platforms such as Facebook must review their practices to protect minors' personal data better. Organizations such as companies, schools, or other institutions that use social media to communicate with children must also comply with the GDPR regulations. They are required to implement appropriate mechanisms that ensure the safety and transparency of data processing. This case highlights the shared responsibility between platforms and administrators of social media pages. For children who use these services, the decision is of great importance, as it requires increased transparency, clear communication about data processing and protection against possible abuse. It stresses the necessity of highlighting the protection of young users in the digital world and reminds us that all players in the digital world have a role to play in guaranteeing their safety.

6 Endeavours and Chances for Protecting Children's Data Right's in the Digital Age and Main Conclusions

The modern digital environment poses major challenges to the protection of personal data, especially for children. With the penetration of Internet services into everyday life and the increasing use of digital technologies by youth, their data turn into particularly at risk to unregulated collection, misuse and manipulation. This problem is even more acute as children are often unaware of the risks connected with revealing private information online. This needs those existing regulations, such as the GDPR, be adapted to the ever-changing digital landscape. The presentation will analyse the main problems and opportunities for developing the legal bases linked to the protection of children's data. A significant issue is that children have difficulty understanding what information is collected about them and how it is administered. They often do not fully appreciate the dangers of sharing personal information, such as photos, location and preferences. Although the GDPR obliges platforms to provide understandable privacy policies, these are often complex and inaccessible to young audiences.

Furthermore, although the GDPR requires parental consent to process data on children under 16 (or those of a lower age in different countries), many platforms do not have trustworthy age verification methods in place. This allows children to circumvent the restrictions, leading to their data being collected unlawfully. Another crucial issue is the application of social networks and mobile apps, which often use

children's data for targeted advertising despite the GDPR explicitly prohibiting this. While some platforms are striving to comply with the law, significant gaps in their policies remain. International data transfers are also an important aspect. Large platforms such as Facebook, TikTok and Instagram collect data from children in the EU and relocate it to third countries where data protection standards may not be as high as those in the EU. The Schrems II ruling makes it transparent that these allocations need to be more strictly regulated. The GDPR expects the administration of children's data to be carried out under provisions of a high level of protection "by default", but many services provide privacy settings that do not provide sufficient security. This leaves children's profiles vulnerable to unauthorized access. Solutions include developing privacy policies adapted for children, using easy-to-understand formats, such as animations or interactive tools, to explain the concerns and status of personal data. Furthermore, it is vital to implement reliable age verification systems, such as biometric technologies or other innovative approaches. These measures can provide better protection for children's personal data and strengthen their safety online. Changing the approach to targeted advertising[21] is a key step on enhancing the protection of children online. The ban on advertising directed at children must be strictly enforced and should include all forms of profiling and personalisation of content. Regulations such as the GDPR need to be revised to address new technologies and methods used to target children. This could mean introducing a ban on the use of algorithms that collect and analyse data to create advertising profiles for children, as well as compulsory transparency constraints on the data gathered and its purpose. Following the Schrems II ruling, greater emphasis needs to be kept on the protection of children's personal data in international transfers. This implies introducing strict regulations to control the relocation of personal data outside the EU to guarantee that this data is not bargained. It is also required to establish international agreements and standards that oblige third countries to apply data protection rules comparable to those in the EU. EU Member States should strengthen regulation of online platforms and introduce stronger penalties for non-compliance with children's rights. This could include a legal possibility for collective complaints on behalf of children, their parents or guardians, and a review of punishments to confirm that any breach carries serious consequences for those who breach the GDPR. In an era of rapidly evolving technologies and digitalisation, governments, regulators, online platforms, and

[21] Morton & Treviño, 2021, pp. 50-71.

industry need to work together to ensure the welfare of children. Existing tools, such as the GDPR, present a robust foundation, but to be successful, they need to be altered to the realities of the digital age. Ensuring children's safety and privacy online is a key step towards ensuring a secure and ethical digital future.

7 Conclusion

The protection of children's personal data in the digital era is a priority for modern legal systems, with the EU and its Member States leading the way in producing laws and rules that respond to the new challenges occurring from the fast growth of technology. After examining key cases involving violations of children's rights to their personal data and analysing the legal framework, including the GDPR and other international instruments such as the ECHR and the CRC, we can draw important conclusions on the current state of data protection and on the options for improving the legal framework. The GDPR, as the main EU data protection regulation, provides a basis for protecting children by requiring parental consent for the handling of data of children under the age of 16 (or a lower age limit set by Member States). However, the application of these rules is not always effective, as several court cases (for example, those related to platforms such as YouTube, TikTok, and Instagram) have shown. The main problems lie in the fast progress of data collection technologies that outpace the pace of the legal system. While the GDPR provides safeguards, its implementation has been challenging, specifically regarding parental consent on online platforms, where children can easily circumvent age verification. The ECHR protects children's privacy but does not contain precise provisions on the protection of personal data in the digital age, emphasizing the need for legal modernization. The CRC also secures the right to privacy, but the performance of these rights remains challenging from the perspective of fast-developing technologies. Key challenges to protecting children's personal data include the lack of effective age verification mechanisms, unclear and incomprehensible information policies, targeted advertising and profiling of children, and issues with international data transfers. Many online platforms cannot ensure that children do not establish accounts without parental consent, which puts them at risk of data collection without their understanding. Privacy policies written in language that children do not understand also do not give adequate knowledge about the threats of data collection. Additionally, the use of data for targeted advertising violates the core principles of the GDPR. To improve the protection of

children's personal data, stronger age verification mechanisms, including biometric technologies, should be established. Law should be altered and written in language that children can understand, using innovations such as videos and interactive formats to help them understand how their data is collected and used. Companies should introduce information policies that not only explain children's rights, but also inform them about the potential risks of online interactions. A ban on targeted advertising to children should be introduced into the regulation of online platforms, which would prevent the collection of personal data for the aim of establishing marketing profiles. Targeting technologies should be strictly controlled and stopped when it comes to children. A global initiative is needed to protect children's personal data, including international agreements between countries and technology companies that ensure a level playing field regardless of jurisdiction. The design of universal standards for the protection of children's data, like those in the GDPR, could strengthen global protection and reduce the risks associated with international transfers of personal data. Legal norms need to be adapted to new technologies such as artificial intelligence, machine learning, and the Internet of Things. These technologies offer new opportunities for the gathering of personal data, but they also create new risks for children. The legal basis should contain instruments to refer to these new risks and to safeguard the safety of children. The problems related to the protection of children's personal data in the digital sphere are complex and multifaceted. Existing legal mechanisms, including the GDPR and international conventions, provide an excellent foundation for protection, but they require to be further improved and adapted to meet new challenges. The use of new technologies poses a number of risks to children's autonomy and psychological well-being. In this sense, AI-driven tracking can collect a large database of data on children's behavior, preferences, and interactions. On the other hand, profiling can lead to the manipulation of children's choices without them realizing it. Platforms then personalize content to maximize engagement, often at the expense of children's well-being. This constant scrolling can have an addictive effect and lead to children's impulsive behavior. As a result of algorithmic profiling, children can reinforce incorrect stereotypes about themselves, influencing their choices before they can critically evaluate them. There is a legal framework to protect children's rights in Article 8 and Article 22 of the GDPR, Article 8 and Article 10 of the ECHR and Articles 16, 17 and 31 of the CRC, but some improvements are needed. Such as obligations for large social platforms to account for shared content and mental health safeguards.

From the analysis, we can conclude that existing legal frameworks partially address the risks of AI for children, but stricter interpretations or new guidance are needed. The GDPR could introduce stricter prohibitions on algorithmic profiling of children, and the ECHR and CRC could provide legal challenges against manipulative AI in digital environments. The authors believe that strong platform transparency, ethical AI design, and child-specific protection are necessary.

Acknowledgment

The research was conducted and funded under project No. 101047808 entitled "European Data Protection: Post pandemic effects and new dimensions" (EDP-PPEND), which is implemented by South-West University "Neofit Rilski" with the financial support of the Erasmus + Programme 2021-2027, an action under the Jean Monnet Initiative in the field of higher education.

References

Bulgarian Agency for Child Protection, (2023). Retrieved from https://sacp.government.bg/%D0%BD%D0%BE%D0%B2%D0%B8%D0%BD%D0%B8/%D0%BD%D0%B0%D0%B4-70-%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D0%BD%D1%82%D0%B0-%D0%BE%D1%82-%D0%B4%D0%B5%D1%86%D0%B0%D1%82%D0%B0 (accessed: 30 January 2025).

Bulgarian Commission for Personal Data Protection. (2022) *The rights of children and young people when working on digital platforms*. Retrieved from: https://cpdp.bg/userfiles/file/Documents_2022/Pravata_na_decata_KZLD_brochure.pdf (30 January 2025).

Convention on the rights of child, UN, 1989. Retrieved from: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child (accessed: 30 January 2025).

Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Schrems II), case no. C-311/18, ECLI:EU:C:2020:559, Judgment of the Court (Grand Chamber) of 16 July 2020.

European Convention on Human Rights [1950], available: https://www.echr.coe.int/european-convention-on-human-rights.

FTC press releases or articles on the case from sources like The Verge or BBC News. The New York Times, Wired, or legal websites like Privacy International. The Guardian, TechCrunch, or official statements from the Irish Data Protection Commission. Articles from CNBC, Reuters, or TechCrunch.

Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, case no. C-131/12, ECLI:EU:C:2014:317, 13 May 2013.

K.U. v. Finland, app. no. 2872/02, 2 March 2009.

Marin, N. (2023) *The jurisprudence of the Court of the European Union on the personal data protection – a new paradigm*. Blagoevgrad: Neofit Rilski Press, pp. 211-217.

März, J. W. (2022) 'What does the best interests principle of the convention on the rights of the child mean for paediatric healthcare?'. *European Journal of Pediatrics*, 181(11), pp. 3805-3816.

Miąsik, D. (2023) *The principles of primacy and direct effect in the case-law of the Supreme Court. In National Courts and the Application of EU Law* (pp. 201-224). Routledge.

Milkaite, I., De Wolf, R., ... Martens, M. (2021) 'Children's reflections on privacy and the protection of their personal data: A child-centric approach to data protection information formats'. *Children and Youth Services Review,* 129. doi:10.1016/j.childyouth.2021.106170

Morton, F. & Treviño, T. (2021) *Targeting kids in the digital age: The ethics of online marketing towards children*. In Humanistic management in Latin America (pp. 50-71). Routledge.

O'Mahony, C. (2019) 'Child Protection and the ECHR: Making Sense of Positive and Procedural Obligations'. *The International Journal of Children's Rights*, 27(4), pp. 660-693.

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. (2016). *Official Journal of the European Union*, L119, pp. 1–88.

S.*W. v. United Kingdom*, app. no. 87/18, 22 September 2021.

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. doi: 10.21953/lse.47fdeqj01ofo

Voigt, P. & von dem Bussche, A. (2024). *Scope of Application of the GDPR. In: The EU General Data Protection Regulation (GDPR)*. Springer, Cham, pp. 9-36, https://doi.org/10.1007/978-3-031-62328-8_2

Wirtschaftsakademie Schleswig-Holstein GmbH v. Facebook Ireland Ltd., case no. C-210/16, ECLI:EU:C:2018:388, 5 June 2018.