A Comparative Study of the Online Privacy and Data Protection of Children in the European Union and the United States

Synopsis of Ph.D. Dissertation

Aslı Alkış Tümtürk

Supervisors:
Dr. Zsolt Nagy
Dr. Szilvia Váradi Dr. Kertészné

University of Szeged
Faculty of Law and Political Sciences
Doctoral School

Szeged
2023

Table of Contents

1. **Background of the dissertation** **1**
2. **Objective and significance of the dissertation** **3**
3. **Hypothesis and research questions** **4**
4. **Methodology** **6**
5. **Structure of the dissertation** **7**
6. **Scientific results** **8**
7. **List of publications of the author on the subject of the dissertation** **17**

1. Background of the dissertation

The contemporary culture exhibits a pervasive reliance on data, which compels individuals to provide personal data in order to get certain services. For instance, we share our health-related data with hospitals to receive health care services, our credit or debit card information to order food, and our personal information (at least username, email address and most likely credit/debit card information to pay for the service if it is not free) to access online music or video platforms. This information will be used to provide products and services, but it should not be used for reasons that the data subjects did not expect or intend when they consented to the sharing of their information.

Data protection, as a fundamental right, ensures the protection of natural persons with respect to the processing of personal data. The second objective of data protection is to govern the free flow of personal data among individuals, organisations, and countries as a result of the societal and economic benefits of data sharing.

Long-standing issues concerning privacy and personal data have become much more interesting as a result of the increasing internet use of not just adults but also children around the world. Especially with the introduction of social media networks including YouTube, Facebook, and Instagram, the privacy and data protection of children have become significant concerns, since parents may now share their children's photo albums and videos with the entire online community. Therefore, being a minor celebrity or child influencer is now remarkably easy for any child.

This thesis thus focused on a subset of the much broader issue of privacy and data protection, namely the privacy and data protection of children. However, this does not indicate that the topic of children's privacy and data protection is narrow; on the contrary, when we delved further, we discovered several insufficiencies and gaps between the law in text and law in practise.

The first problem we have observed is that one in three internet users worldwide are children and that 80% of children in developed Western countries have digital footprints before the age of two, largely due to the actions of their families. However, lawmakers are not taking this issue seriously, because they prioritize more economically attractive concerns, such as data transfers and profiling, over protecting vulnerable data subjects who may not contribute as much to the Digital Single Market economically. Similarly, websites, particularly social media

networks, ignore the existence of children on their platforms and turn a blind eye to the fact that children under the age of consent are utilising their services.

The second issue identified is the limited number of academics who exhibit interest in the online activities of children. Consequently, there exists a limited amount of academic literature pertaining to this subject matter. One of the obstacles encountered throughout the research for our thesis was the scarcity of scholarly material available. However, we successfully addressed this challenge by carefully picking research questions that are in accordance with the existing sources and using a multidisciplinary approach. The latter was achieved by including case studies from civil law and doing comparative analyses to explore specific concerns within different legal disciplines. Furthermore, our statements have been supported by sociological sources including surveys and studies. Therefore, it is our contention that this doctoral thesis has the potential to provide a unique and advantageous contribution to the realm of academia and the body of knowledge within the field.

Thirdly, the real-life example of *Amanda Todd*, a young girl who committed suicide, because her data was not protected properly, convinced us that children are naiver and more vulnerable than adults and thus require more specialised protections. This was a milestone factor that prompted us to conduct extensive study on this issue.

The fourth problem is that while the GDPR and the COPPA include data protection and privacy standards for children, these requirements are not comprehensive. For instance, neither the GDPR nor the COPPA impose any restrictions with respect to parental sharing.

The difference between the legal text and its application in practice is the fifth problem we have identified.

The last and most significant issue that will be addressed in this thesis is the overreliance on parental consent and responsibility under both legislations. In situations when parents lack awareness regarding the potential hazards and repercussions associated with their children's online activities, depending only on parental accountability may exacerbate the well-being concerns regarding children.

Nonetheless, it is possible that the final three problems listed have not yet become readily apparent. The children of today who suffer/will suffer from their parents' and data controllers' online activities are not yet mature enough to comprehend the risks and consequences of excessive online sharing of their personal information and private lives. Consequently, Internet-victimized children now lack the maturity to take legal actions against their parents and/or the relevant data controllers. In the near future, however, we expect legal cases from today’s children regarding violations of their privacy and data protection rights.

2. Objective and significance of the dissertation

In this thesis, we intend to compare the COPPA and the GDPR and their practices regarding children's online data protection and privacy in the EU and the US in a number of areas, including the historical background of the GDPR Article 8 and the COPPA involving the recent history of transatlantic data transfers, concept of consent and particularly the consent of the parents, the rights of children and parents and the obligations of data controllers as determined by the laws, the social media practises of children and parents, and the extent to which social media sites follow and apply the laws.

The reason why we chose the COPPA rule to compare it with the GDPR is that the US is where privacy discussions began in the world, and Article 8 of the GDPR partially adopted the COPPA's approach to children's data protection. It is evident that the two legislations share similarities since both the GDPR, and the COPPA hold parents/legal guardians accountable for their children's online actions and require parental consent for sharing children's personal data online. Additionally, they also implement a similar age of digital consent for children. By making these comparisons, we will attempt to highlight both the weaknesses and the strengths, and in doing so, we will provide remedies for the flaws and seek the ideal solutions.

The primary objective of this thesis is to highlight the importance of protecting children's online data and privacy. Additionally, it aims to examine the potential limitations associated with relying heavily on parental consent for protecting online data and the privacy of children. We aim to make a valuable contribution to the existing body of literature by addressing this significant and broad research question.

Our long-term objective is to influence the viewpoints of lawmakers. Therefore, we expect that our research will help to the future creation of more child-friendly and child-centred policies, as well as more child-friendly social media rules and restrictions. In addition, we will emphasise that these laws and restrictions must always be implemented with the best interests of children in mind. Last but not least, given the vulnerability of children, we would like to emphasise the significance of collaboration between parents, lawmakers and law enforcers, data controllers (particularly online service providers in the context of our thesis), and even schools.

3. Hypothesis and research questions

The overarching question of this thesis is:

Does an excessive reliance on parental authorisation and consent effectively protect the personal data and privacy of children?

In order to address this inquiry, we have investigated the level of comprehension among children and parents about the significance of privacy and data protection for children. This investigation was enhanced by the utilisation of studies and surveys, together with the analysis of replies to other research questions which will be stated below. We ascertained the degree to which they are aware of the potential hazards associated with relinquishing control over children's personal data. It was important to consider the insights gained from the chapters of this thesis in order to address the extent of parental awareness of the privacy and data protection rights of children, together with their ability to effectively exercise these rights. Additionally, it was crucial to examine the knowledge of parents about the responsibilities of data controllers in relation to safeguarding these rights. Ultimately, we have addressed the mentioned overarching question. We have also put forward prompt and enduring measures to attain optimal practices for protecting the personal data and privacy of children.

We began this thesis by analysing the background of the COPPA and Article 8 of the GDPR in Chapter 2. We will inquire as to the historical context and evolution of the definitions and standards related to the privacy and data protection of children in these legislations, as well as the emergence of the necessity to adopt such rules for children.

In Chapter 3 regarding the concept of consent, we have examined whether the COPPA and GDPR provide methods for obtaining parental consent. If so, what are they? If not, what are the potential methods to obtain parental consent in light of current technology, and if just one of the legislations uses such methods, is a legal transplant conceivable to incorporate them into the other?

After Chapter 3.1 and 3.2 related to the scope of the concept of consent and parental consent, we have examined in Chapter 3.3 how the threshold ages are implemented in practise and whether they are functional. In this chapter, we addressed our first and second research questions:

Under the GDPR and COPPA, do the threshold ages for parental consent have any logical basis?

Do these threshold ages have any practical effects on children's internet activity habits and behaviours?

As stated above, parents have the primary responsibility for their children's safety in accordance with the COPPA and the GDPR. The parents of a child, however, cannot be expected to keep a close eye on them all the time. Therefore, there are internet technologies that make it easier to keep an eye on children while their parents are not available. The purpose of these age verification systems is to use technology to ensure that only individuals of a specific age are allowed to see online content that is restricted by law or by the website's policy. As a result, age verification might be useful in making the Internet safer for children.

Accordingly, we investigated the age verification methods in Chapter 3.4 of this thesis and within this chapter, we answered the third research question:

Could commonly deployed methods of age verification for preventing children's access to inappropriate online content be both trustworthy and respecting children's privacy and data protection rights?

In Chapter 4, we listed the main rights of the children and the parents under the GDPR as well as COPPA. We addressed the fourth research question in this chapter:

Taking into account the best interests of children, should data protection and privacy rights be provided directly to children by law, or should parents exercise them on their behalf?

Following the data subject's rights, we outlined the obligations of data controllers and processors in Chapter 5, as they are interrelated. In this chapter, we answered to our fifth and sixth research questions:

Do the GDPR and the COPPA impose obligations specific to children on data controllers? If so, do these obligations enable direct communication between data controllers and children?

When and how could data controllers directly engage with children (instead of their parents) and offer them more control over their data?

In Chapter 6, we addressed real life examples such as social networking sites, privacy policies, child influencers, and parental sharing. We began this chapter by discussing the sociological and cultural changes brought about by the rise of social media websites. In the recent past, sharing images and videos was limited to close family and friends via photo albums and videotapes. However, following the advent of the Internet and social media networks such as Facebook, Instagram, and YouTube, the situation has altered considerably. Since individuals now have the opportunity to share their material online with millions of random strangers,

everyone has the potential to become celebrities or, as the term has evolved, influencers. Given the fact that the GDPR and the COPPA restrict children's online sharing of personal information without parental consent if they are under a certain age, social media platforms do not allow children under the age of consent to create accounts on their platform. Nevertheless, the frameworks do not impose restrictions on parents regarding the disclosure of their children's personal information on the Internet. This chapter addressed our seventh research questions:

How do the requirements of the GDPR and the COPPA affect the practises of social media sites and the sharing activities of parents concerning their children?

To answer the seventh question, we have examined the case law, surveys, statistics, and real-world examples from social media sites (e.g., a child influencer's photo on Instagram or Facebook, a family prank video on YouTube, etc.). By doing so, we determined whether the prohibited content specified in the data protection and privacy policies of these social media sites as a consequence of the GDPR and the COPPA requirements, as well as whether these social media sites' policies are reflected in practice.

4. Methodology

This thesis was written using the comparative law method and to strengthen and deepen our research, we employed this method focusing not only on the similarities, but also on the differences between the GDPR and the COPPA. In order to accomplish this, we compared equivalent phrases and understand their variances in meaning.

The comparative law method enriches the research by analysing the importance of similarities and differences not only in light of the legal systems of both jurisdictions, but also considering their respective cultures. Likewise, this method enables us to identify the discrepancies between written legislation and actual law enforcement. Consequently, this methodology helped us in enhancing our research by allowing us to focus not only on the letter of the law but also on law in action by analysing the historical contexts of privacy and data protection, the case law, the works of scholars, conducted surveys and statistics in the literature, and social media examples in order to better comprehend the implementation of legal text into practise.

It is important to highlight at this stage that one of the most challenging aspects of researching the doctrine and case law was the difficulty in locating appropriate sources. This is because the great majority of academics write about general topics and issues linked to the

privacy and data protection of adults, rather than focusing on the privacy and data protection rights of children. In addition, there are not many cases involving children's online data protection and privacy, because online sharing of children's data and children's use of the Internet is such a recent topic that it will take time for today's child influencers to reach adulthood and, for instance, exercise their right to be forgotten before the courts.

The analytical method was also fruitful for analysing the legal rules and concepts of these two different legal systems. It did not only enable us to detect the common parts and variations between these legal systems, but also to compare them to the "ideal type." Detecting and searching for the *ideal* allowed us to design solutions and make suggestions.

Legal transplant is a highly significant and useful concept in the subject of comparative law, which was addressed in this thesis. Although *Alan Watson* created the term in 1974, this practise has been around for ages. Accordingly, in this thesis, we discussed a legal transplant case adopted from the COPPA to the GDPR in the digital era related to our topic which is the online age threshold for obtaining parental consent. We also proposed a new legal transplant from the COPPA to the GDPR addressing the methods of verifying parental consent, since it would guide data controllers on how to determine if the given consent is from a parent or not.

5. Structure of the dissertation

In Chapter 2, we analyse the historical context of both the GDPR and the COPPA, as well as the reasons and movements behind the privacy and data protection of children in both legal systems. Furthermore, this chapter examines the significance of transatlantic data transfers and provides a historical analysis of the agreements pertaining to the free movement of data that have been established between the EU and the US. In Chapter 3, the concept of parental consent to make the processing of underage children's data lawful and verifying the parental consents will be examined in detail. In Chapter 4, main rights of children and parents will be outlined and analysed in both legislations. In Chapter 5, main obligations of data controllers under the GDPR and the COPPA will be discussed. In Chapter 6, we will compare and evaluate the privacy policies and terms of service of three social media platforms (YouTube, Facebook, and Instagram), as well as the use of these social media sites by parents and children, in order to determine how legal texts manifest themselves in online practise.

6. Scientific results

In Chapter 2 of this thesis, we began with a background analysis of the COPPA rule and Article 8 of the GDPR. Using a historical perspective, we analysed the emergence and evolution of the concepts of privacy and data protection. Since the historical legislative developments of privacy and data protection started in the US, the EU followed in their footsteps but built a protection that was more comprehensive.

The backdrop of the GDPR and the COPPA has been explained in Subchapter 2.1, accompanied by an examination of the provisions that necessitate enhancement. In contrast to the US, we stated, data protection became a fundamental right in the EU. Convention 108 of the Council of Europe was the first legislative framework related to data protection, but it was ineffective in harmonising the legislation of the Member States. Therefore, Directive 95/46/EC established by the European Parliament and the Council of the European Union came into effect. However, due to its nature, it enabled EU Member States to have varying domestic data protection rules, and it was unsuccessful in establishing a uniform legal framework across the Union. Consequently, the GDPR was established, and it became uniformly (except the facultative specifications clauses) and entirely applicable in all Member States upon its entry into force.

We suggested that after becoming aware of children's internet presence, it became necessary to develop specific rules for them. First, the COPPA was created in the US to safeguard the online privacy of children. The EU then followed suit and incorporated Article 8 into the GDPR. The GDPR transplanted the COPPA's requirements concerning the age threshold and parental consent.

In Subchapter 2.2, the significance of the free movement of personal data across the Atlantic between the EU and the US was analysed, as it is a fundamental element of the transatlantic digital economy and cooperation. Due to the US being the EU's primary commercial partner and being the most globally integrated economy, this relationship has significant importance. Consequently, over an extended period, they have engaged in negotiations to establish accords that facilitate the unrestricted movement of data.

In Subchapter 2.2.1, we have conducted a comprehensive analysis of the Safe Harbour, Privacy Shield, and the new EU-US Data Privacy Framework, with a particular focus on their historical context. The examination of the Schrems I and II cases aimed to gain insights into the termination of the Safe Harbour and Privacy Shield by the CJEU. Furthermore, an analysis has

been conducted on the outstanding matters pertaining to the recently implemented EU-US Data Privacy Framework.

This chapter contributes to the literature by tracing the origins of the COPPA and Article 8 of the GDPR and investigating the historical context of transatlantic data transfers. We also compared the different approaches to privacy and data protection on both sides of the Atlantic. Besides, we have provided an overview of the strengths and drawbacks inherent in both legislations.

In Chapter 3, we defined consent and underlined that it is a concept that grants data subjects control over their data. We noted that consent must be freely provided, explicit, informed, and unequivocal for the processing of personal information concerning data subjects. We continued by comparing the concept of parental consent of the GDPR with the COPPA. The most notable distinctions between these two legislations are the age thresholds for obtaining parental consent (13-16 under the GDPR and 13 under the COPPA) and the methods for obtaining parental consent.

In Subchapter 3.3, concerning the first difference, *we discussed the first research question of this thesis which is whether threshold ages for parental consent have any logical basis.* Accordingly, we criticised the fact that the age of digital consent is neither standardised nor well-justified between Member States. It was transplanted for economic reasons and to lessen the burden on data controllers, but because to the variable threshold ages, it should now put a more burden on data controllers. Hence, we suggest the following:

> Policymakers should review whether imposing age limits is useful or whether there are other solutions to provide children with a safe online environment. One important alternative is education and awareness-raising. Other solutions include a combination of parental supervision with software solutions, and ethical design principles for online service providers (including creating more child-friendly content and platforms). However, since age restrictions currently exist under both legislations, it is important to establish a uniform threshold age for online consent under the GDPR across Member States. This is particularly important due to data transfer within the EU and to the US. Besides, a uniform age threshold for digital consent online would offer clarity, consistency, and simplicity of compliance inside the EU for both individuals and companies. The uniform threshold age should also be well-justified. For instance, comparisons with other legal disciplines could help determine a consistent and reasonable age for all Member States.

Accordingly, we discussed the findings of the study completed by *Livingstone et al. (2020)* pertaining to the online data and privacy of children in the digital era in Chapter 6.

This analysis is also evaluated with the information shown in Table 1 under Subchapter 3.3, which outlines the varying ages of consent across different areas within the Member States. It has been determined that individuals between the ages of 15 and 16 exhibit the highest level of awareness regarding the potential ramifications of their online actions. Furthermore, they possess a greater aptitude for digital media literacy and demonstrate an inclination to inquire about the data processing practices employed by online service providers. These inquiries often relate to the adherence of mentioned providers to legal principles such as data minimization and purpose limitation (while the teenagers may not use precise legal terms, the intended message remains unchanged.) Moreover, the age of 16, as set by the GDPR, aligns with the ages of consent established in other fields, such as consent for medical treatment, working part-time, and sexual intercourse. Hence, it is deduced that the age threshold of 16, as established by the GDPR, may be considered suitable. However, it is recommended that the phrase in Article 8 of the GDPR, which allows Member States to reduce the age threshold to 13, be eliminated due to the resulting lack of uniformity among the Member States. Current studies also indicate that children aged 13 exhibit distinct differences, which are disadvantageous, in their level of awareness and comprehension compared to children aged 16.

In addition, according to our perspective, it would be ideal if the COPPA were to raise the age criterion from 13 to 16. This proposed amendment would offer a higher level of protection for teenagers and foster the alignment between the EU and the US.

Regarding the second difference, we noted that the COPPA covers non-exhaustive approaches, but the GDPR does not mention any methods. We criticised the fact that the GDPR did not transplant any methods for validating parental consent from COPPA. It would have been ideal to involve at least some of them in order to provide guidance to data controllers.

We argued that the mechanisms used to validate parental consent under COPPA do not need to be directly applied to the GDPR, since they may lose their effectiveness as technology progresses. Nevertheless, it is conceivable to establish a rule that serves as a general standard and is not biased towards any specific technology. However, it may still include certain instances, as the provisions outlined in Article 32 pertaining to data security criteria.

We drafted a prototype rule in the following manner:

"Taking into consideration the state of the art, the controller and the processor should adopt adequate technologies to guarantee the consent is given or authorised by the holder of parental responsibility over the child, including inter alia as appropriate:

(a) conducting a video conference with the parents to verify their official IDs

(b) confirming the electronic identification (eID) of the parents compared with the eID of the children

(c) Where the processing is unlikely to pose a high risk (e.g., subscribing to a newsletter), consent can also be given through email."

Then, *the second research question of this thesis was how the threshold ages are applied in practise and if they are effective on children's internet activity habits and behaviours.* To answer this question, we compared the age of digital consent to other ages of consent in a variety of circumstances, including entering the workforce, receiving medical care, including diagnosis and surgery, and participating in lawful sexual behaviour with others.

We found out that the correlations between various consent ages in different contexts are illogical and may confuse children.

We analysed the surveys done by the Pew Research Center and the EU Kids Online studies to see whether there is any evidence that lowering the minimum age for accessing specific online services has any practical effect. However, decreasing (or raising) the threshold age has no influence on the outcomes. In Germany, the minimum age for parental consent is 16, although in Spain it is 14. However, children ages 12 to 14 and 15 to 16 are less likely to use social media networks in Spain than in Germany. It indicates that increasing the age threshold in Germany did not deter children under 16 from using social media platforms.

On one hand, Member States who oppose lowering the age of consent online assert that they do so to protect children. On the other hand, those who advocate lowering the age of consent on the Internet (to as low as 13) argue to support children's freedom of speech and press. Considering all the findings mentioned in Subchapter 3.3 regarding the second research question, this thesis claims as follows:

> These regulatory standards do not have sufficient response in practise. In other words, these findings imply that differences in the digital age of consent have no direct impact on use or internet safety in practise. Besides, it seems that lowering the age barrier has no direct impact on the motivation of children to engage in online activities. Moreover, the likelihood of children experiencing injury is not directly proportionate to their age.

Additionally, in Subchapter 3.3, we argued that there is a discrepancy between the law in text and the law in practise, and that this discrepancy is a result of age verification procedures that are easily deceived, particularly the widely used self-verification methods, and as we can see from the aforementioned surveys, children have, for example, social media or Gmail accounts before the age of consent.

Following that, we addressed age verification systems in Subchapter 3.4, which would use technology to ensure that only individuals of a certain age may access age-restricted information online. However, one should be aware that age verification systems include imperfections and cannot be depended upon to protect children from all potentially harmful content. In Subchapter 3.4, *we addressed the third research question of this thesis, which is whether commonly deployed methods of age verification for preventing children's access to inappropriate online content be both trustworthy and respecting children's privacy and data protection rights:*

There are relatively accurate methods for estimating children's age, but they are not privacy-friendly, such as the personal ID or biometric features (e.g., fingerprint) scanning method. There are some methods that may violate data protection and still they are not useful to estimate the exact age, such as voice recognition or face ID tools. Besides, there are some which are privacy-friendly, however, useless because they are so easy to deceive, such as self-verified information. In addition, there is a knowledge-based authentication method that does not breach privacy and yet is useless at determining an individual's exact age. Therefore, we noticed that there is no method that simultaneously protect children from dangerous content and their personal data.

The EU, however, acknowledged this issue and urged Member States to develop age-verification systems in accordance with its eID plan. According to the European Commission, children can use their eIDs to verify their age without giving any further personal information (such as their name or address), which is compliant with the data minimization principle of the GDPR. Besides, it would be a reliable solution because it is based on reliable government databases. This technology, nonetheless, would raise security and privacy issues due to the large quantity of official papers and biometric user data that would be maintained. Thus, if the potential security and privacy issues (such as cyber-attacks and hacker activities) are mitigated, this eID solution will result in a trustworthy EU-wide age verification method that respects privacy.

Within the Chapter 4, we detailed the main rights of children and parents under the GDPR and COPPA. *The fourth question of this thesis was whether data protection and privacy rights should be provided directly to children by law, or parents shall exercise them on their behalf.*

Children have the same data protection rights as adults under the GDPR. We discovered, however, that neither the children nor their parents are provided with instructions on how to exercise these rights. Accordingly, this thesis advocates the following:

Some of the rights may be too complicated for children to exercise on their own; thus, it would be ideal if parents could do so on their behalf if necessary. Others, including as the right to access, rescission, and deletion, may be easier for children to exercise without parental consent if they are mature enough to understand the repercussions of their online actions. At this point, the cooperation of data controllers and the service provider (e.g., third party suppliers) is also crucial because they can make these rights very clear and understandable for children, so that children are aware of their rights and may decide to exercise them or urge their parents to do so.

The COPPA, unlike the GDPR, does not identify any specific rights for children to exercise, but rather provides these rights to parents. It offers parents with notification and review rights, as well as the ability to seek the erasure of personally identifiable information belonging to their children. Likewise, this thesis recommends:

Under the COPPA, children should have at least the right to access, rectification, and deletion, and should not be subject to decisions based only on automated processing (especially profiling). And these rights should be given to children as soon as they can consent to the processing of their personal information. We also claimed that while being underage to provide consent, children could nonetheless exercise certain rights that entail little risk, such as the right to access, terminate (e.g., a data transfer), and delete. Children who possess a sufficient level of maturity to understand the repercussions of their online behaviour might find it less challenging to use these rights without requiring consent from their parents. Children should not lose control over their data since it may lead to a variety of dangerous outcomes, as seen by Amanda Todd's suicide, which occurred because she lost control over her data and was unable to delete it herself.

Along with the legislative rights, we closed this chapter by emphasising the necessity of collaboration between data controllers, third-party service providers, and parents. Parents should provide their children with Internet access, secure their children's personal information from hazardous third parties by interacting, when necessary, without breaching their children's privacy, and be able to maintain this delicate balance.

Following the rights of children and their parents, we discussed the interrelated obligations of data controllers and processors in Chapter 5. *The fifth research question of this thesis was whether the GDPR and the COPPA impose obligations specific to children on data controllers.*

The sixth question of this thesis was when and how data controllers could directly engage with children (instead of their parents) and offer them more control over their data.

We have analysed all the obligations of the data controller under the GDPR and the COPPA in detail. Comparing the two approaches, we claim:

It is evident that the GDPR is more comprehensive and detailed in terms of data controllers' duties and how they protect the personal data of data subjects by making it possible and easy for data subjects to exercise their rights, cooperating with supervisory authorities when necessary, and reducing the risks of processing by conducting data protection impact assessments.

Nevertheless, regarding the obligations of data controllers to protect children's data, the GDPR falls behind. The GDPR draws a little distinction between data subjects as adults and data subjects as children, despite the fact that children require more specific protection due to their unique and more vulnerable status as data subjects. Therefore, it would be ideal to incorporate an article providing child-specific data controller obligations in the GDPR. The article would be presented as follows:

> "1. Children may lack awareness regarding privacy policies and their rights pertaining to privacy and data protection. In accordance with best practises, data controllers shall employ simple video presentations or visually engaging images accompanied by easily comprehensible language to enhance children's understanding of their data protection rights, particularly with regard to the right to be informed and the right to access their personal data.
>
> 2. The use of the rights to ratification, erasure and prohibition or termination of data transfers shall be allowed in cases when children possess the necessary level of maturity to independently request such actions, hence eliminating the requirement for parental consent.
>
> 3. The practise of profiling may be subject to prohibition unless there exists a compelling or public interest that may outweigh the interests of the child in question. However, in the event that such a situation arises, it shall be still possible for a child to object to this profiling. In this scenario, it is imperative for the data controller to take prompt action, without delay, even in the absence of parental consent.
>
> 4. In the event of data breaches, data controllers are required to inform parents and children concurrently, even if the children are at an age where they can provide consent, as a precautionary measure. In addition, it is essential that they provide parents with information and assistance to assist them in mitigating the negative consequences of personal data breaches on their children. The exemptions specified in Article 34(3) shall not be applicable in cases where the individual whose data is being processed is a child.

5. The Regulation shall reserve all other responsibilities of data controllers and all other rights of children."

In contrast, all of the obligations of operators under COPPA concern the protection of children's privacy and how operators should ensure parental control over their children's personal information. When children are young and unable to make decisions or realize the repercussions of personal data processing, it is plainly advantageous.

Nonetheless, if they are able and willing to do so, children should be allowed to participate in less dangerous actions such as deleting data from a website, unsubscribing, or restricting the transfer of personal data to other parties without parental consent in both legislations. Therefore, operators should give these options to children who choose to exercise control over their data and engage in less harmful online activities. Finally, given the significant risk associated with processing children's personal data, the COPPA should require operators to work with supervisory authorities and implement data protection/privacy impact assessments for such processing, as does the GDPR.

In the last chapter of this thesis, we discussed real-world examples such as social media sites, their privacy policies, child influencers, and parental sharing. We started this chapter with a discussion of the sociological and cultural changes caused by the development of social media platforms. In the past, sharing photographs and movies was limited to close family and friends through photo albums and videotapes. With the introduction of the Internet and social media platforms such as Facebook, Instagram, and YouTube, the situation has changed significantly. Due to the fact that individuals may now share their content online with millions of strangers, everyone has the potential to become so-called celebrities (i.e., influencers).

In Chapter 6 of this thesis, *we addressed the seventh research question pertaining to the impact of the GDPR and the COPPA on the operational procedures of social media platforms and the sharing behaviours of parents with regards to their children. This chapter also addresses the last and overarching question of this thesis, which examines whether an excessive reliance on parental consent and responsibility may efficiently protect the personal data and privacy of children.* Regarding the answer of the seventh research question, this thesis argues the following:

Given that the GDPR and the COPPA restrict children under a specific age from revealing personal information online without parental consent, social media networks do not allow children under the age of consent to register accounts on their platform. However, neither of these legislations set restrictions on parental sharing. In other words, the GDPR

and the COPPA impose no penalties on parents who disclose personal information about their children on the Internet. Nonetheless, social networking platforms prohibit the sharing of some types of information involving sexual abuse and violence against children.

For example, YouTube restricts the posting of nudity or sexual exploitation content, prank videos, content in the most private places of children (such as their bedroom and bathroom), and actions that may draw the attention of dangerous users. Both Instagram and Facebook restrict the content related to child exploitation and nudity.

Nevertheless, it is still possible to access restricted information on social networking sites, as illustrated by the real-world examples presented in Chapter 6. For example, you may discover an example of a barber pranking a child by pretending to cut off his ear and it is revealed that the boy's parents gave their consent for this content. The parents of a very famous child influencer are sharing their daughter's bikini images with complete strangers, and there are several improper comments under the photos, which will disturb her when she is mature enough to comprehend them.

Based on the comprehensive analysis presented in the thesis, it is highly recommended that the following be considered as a response to the overarching research question:

Both parents and children might not possess an adequate awareness of the significance associated with privacy and data protection. Furthermore, their understanding of the potential ramifications and risks associated with relinquishing control over children's data on the Internet could be limited. Both children and parents may possess a lack of knowledge of the privacy and data protection rights of children, as well as the mechanisms via which these rights might be exercised. They could lack information regarding the responsibilities of data controllers in relation to the exercise of their rights. Hence, it is imperative for lawmakers to adopt a more precise, specific, and instructive approach when establishing the rights of children and the corresponding responsibilities of data controllers.

As previously stated, it is important that children have the opportunity to exercise their rights autonomously, without requiring parental approval whenever possible, and that they have the ability to directly communicate with data controllers when appropriate. Besides, lawmakers need to consider implementing more stringent regulations on shared material pertaining to children. This approach would prioritise the establishment of immediate measures, rather than excessively relying on parental consent and delegating the responsibility of determining the sharing of child-related information only to parental authority. Furthermore, these limitations would require social media sites to enhance their

privacy practices in relation to potentially harmful or sensitive information pertaining to children.

As a prospective long-term strategy, the government may provide financial resources to facilitate the implementation of educational seminars and lectures on digital literacy inside schools, targeting both children and their parents. Additionally, it is essential to ensure that the legislations are executed in a way that is conducive to the needs and understanding of children. Moreover, it is crucial for the courts in both the EU and the US to interpret these legislations in a manner that safeguards the privacy and data protection rights of children. Accordingly, they could have the ability to serve as models for other legal systems and jurisdictions.

In summary, it can be inferred that fostering cooperation among governments, parents, schools, and data controllers is the optimal approach for protecting children's privacy and ensuring data protection in the realm of the internet, rather than only burdening parents with this responsibility.

7. List of publications of the author on the subject of the dissertation

- Asli Alkis Tümtürk: Implications of Parental Sharing of Children's Personal Data Online, ArsBoni Jogi Folyoirat, X. evfolyam 2022/1-2 (2022), 11 available at https://arsboni.hu/wp-content/uploads/2022/09/Arsboni-foly%C3%B3irat_2022_1_2.pdf (last visited 29 September 2023).
- Asli Alkis Tümtürk: The Threshold Age for Children's Online Consent in Light of the Watson/Legrand Debate: Is Legal Transplant Possible in the Digital Era?, The Journal of Comparative Law vol. 17/1 (2022), 243.
- Asli Alkis, Investigating the usefulness of online age verification methods, Studia Iurisprudentiae Doctorandorum Miskolciensium, (2021) vol.1, 8.
- Asli Alkis: The impact of the Privacy Shield's invalidation on the EU-US dataflows, Studia Iurisprudentiae Doctorandorum Miskolciensium, (2022) vol.1, 34.
- Asli Alkis-Tümtürk: Uncertain future of transatlantic data flows: Will the United States ever achieve the 'adequate level' of data protection?, Hungarian Journal of Legal Studies, vol. 63 issue. 3 (2022) 294-311.

- Asli Alkis: WTO's impact on GDPR's Cross-Border Data Flows: ensuring the balance between privacy and trade? Forum: Publicationes Doctorandorum Juridicorum 10 (2020), 5-13.
- Asli Alkis: Investigating privacy issues of (COVID-19) contact tracing apps In: Hajdu Gábor (Hajdu Gábor Befektetésvédelem) CSS/Institute for Legal Studies; USZ/DI/Doctoral School of Law and Political Sciences (eds.) Rendkívüli helyzetek és jog : Kalandozások a jog peremvidékén a COVID-19 apropóján Szeged: Iurisperitus Bt., (2021), 159-170.
- Asli Alkis: Protection of Youtuber Kids Against Child Labour and Exploitation In: Ristivojević Branislav R (eds.) Harmonizacija srpskog i mađarskog prava sa pravom Evropske unije = A szerb és a magyar jog harmonizációja az Európai Unió jogával = Harmonisation of Serbian and Hungarian Law with the European Union Law Нови Сад, Újvidék: Faculty of Law of the University of Novi Sad, (2020), 357-367.