UiO : Faculty of Law
University of Oslo

Children´s Online Privacy Rights and Internet Governance: A Closer Look at Cases Where Parents in Norway Share Sensitive Information About Their Child Welfare Cases On Social Media. Does The GDPR Offer Adequate Protection for Such Children?

Candidate number: 8007

Submission deadline: 01.12.2017

Number of words: 17 734

Table of contents

1 INTRODUCTION

1.1 Background, Purpose and Scope of the Study

In recent times, the Norwegian Child Welfare Services (Barnevernet) has garnered a lot of attention and sparked a lot of debate around the world. The case of a young Norwegian-Romanian couple in Norway whose five children were placed in care order by the child welfare services gave rise to increasing concern abroad and within the country about Norway´s child protection policies and practices. Leading Norwegian experts and demonstrators around the world claim that child welfare workers are generally too quick to take children away from their families, often with little justification, especially when the parents are immigrants. A documentary was made about this case and in this documentary, the cases of other families were also presented. This documentary was available on YouTube at the time of writing of this thesis.[1]

Also, in July 2016, the Australian Special Broadcasting Service (SBS) aired a documentary called *Norway´s stolen children?*. In this documentary, several parents and children who have had to deal with the Norwegian Child Welfare Services were interviewed and their cases were discussed in much detail. For instance, the kind of neglect or abuse the children were supposedly subjected to, and which led the Child Welfare Services to remove them from their homes were discussed. Also, the faces of some of the children were blurred out, whilst the faces of other children were shown clearly. This makes these children easily identifiable by anyone who watches the documentary. The documentary is available on the SBS online network[2] and on Youtube[3], and is openly accessible to the public.

These are a just two examples of instances where Norwegian child welfare cases have been made available on social media, to an unlimited number of viewers and where no attempts were made at anonymizing or protecting the identity of the child or children involved.

---

[1] https://www.youtube.com/watch?v=owGTvlU9Nkw. Accessed 14.07.16.

In this case, the child welfare services had removed the children from the home because it had received reports that the parents were using corporal punishment on the children. Physical punishment of children is regarded as child abuse in Norway and is prohibited by law. According to the parents, their religion as Pentecostal Christians allows for physical punishment of children, and they therefore did not see anything wrong with administering that kind of punishment. The family believed that their faith as Pentecostal Christians was the main reason why the children were taken away from the home. Consequently, the international community of Pentecostal churches around the world mobilised and protested this case at the various Norwegian embassies in their respective countries. In the documentary, several aspects of the family´s daily activities were discussed. Most of the recording took place in the home of the family, where they spoke about their daily activities and their faith, and how the parents themselves believed they were great parents to the children.

[2] http://www.sbs.com.au/news/dateline/story/norways-stolen-children. Accessed 26.07.16

[3] https://www.youtube.com/watch?v=C-PzrwliUk4. Accessed 26.07.16

There are several other examples of parents blogging about their child welfare cases, or creating Facebook pages dedicated to such cases. On these platforms, they update their audiences about events that occur in the case. Some of them go as far as sharing the decisions of the courts in its entirety on these platforms without any attempt to anonymize the identity of the child or children involved. Others also post videos of the children concerned.

The parents' motivation behind the publication of such sensitive personal information is usually to garner attention on, and to obtain sympathy for what the parents believe is wrongful or unnecessary interference of the State in their private lives. However, no matter what the motive behind such publications may be, this raises questions about the data privacy rights of the child or children in question.

Many parents do not often foresee the possible long-term repercussions of making their child welfare cases public by sharing sensitive details of the case on social media platforms. The majority of parents do not consider the probability that the content they share (whether it is photographs, video or text documents) can be copied and stored on third-party computers, basically outside their control. They may not fully understand the power that search engines have to allow access to any piece of information that is put out there. Most importantly, many parents are largely not aware of the "eternity effect"[4] of electronic memory. When sharing such information, parents may not be conscious of the fact that they leave traces of their content, which can be rather difficult to remove.[5] Ciavarella and De Terwangne[6] rightly observe that "due to the expanding possibilities to collect, store and use personal data, we have dismantled the world in which our past is ´forgettable´ and we have begun to live in a society of permanent memory".

There could be several consequences to parents disclosing sensitive information about their own children online. The sharing of such sensitive information about children could result in them suffering life-long consequences of an image affected by their parents' activities on the Internet. There is no doubt that having such information out there in cyberspace can become "baggage" that the child has to carry along with him/her the rest of his/her life, and can later lead to problems for the child in relation to friends and in relation to future employers.
Furthermore, and not negligible, is the fact that the digital footprints that parents leave behind could be used for behavioural and contextual advertising.[7]

[4] Walz 1997, p. 3 in Ciavarella and De Terwangne (2014) p. 158

[5] Ciavarella and De Terwangne (2014) p. 158

[6] Ibid p. 159

[7] Ibid

In today's society, a person´s digital reputation is equally important as his/her real life profile.[8] A negative *online reputation* has the potency to create major problems for children and young people. It is therefore important that their parents control the kind of information they share about them on social networks. The extent to which the law effectively protects children when their own parents fail them in this regard, is the focus of this study.

In debates regarding children´s rights and Internet governance, policy makers and regulators as well as technology designers are given massive pressure to create measures (be it legal, technological or educational) to counter the dangers to which children and minors may be exposed on the Internet. A topical solution to the governance of harmful or inappropriate content, conduct and contact is that parents and guardians bear the main responsibility for their children´s online encounters. Some argue that parents are generally in a better position to assess what their child should do or see (online as well as offline), and that "parental mediation is surely the most adaptable and flexible form of governance".[9] This responsibility is described by some authors as *"parental empowerment*."[10]

Even though in many instances where there is a question of protecting children from external influences parents may be the best people to evaluate the best interests of the child, the topic of discussion in this thesis is cases where there is no doubt about the ability of the parents to protect the child from external influences online, but their ability to protect the child´s privacy from being exposed on the Internet by the parents themselves. In many cases, parents may be able to protect the child adequately whereas in other cases, parents will not have the ability to ensure such adequate protection. The above-mentioned examples of parents publishing information about their own children´s child welfare cases on social media gives reason to call into question the extent to which parents can be regarded as adequate protectors of children´s online privacy. The fact that a child welfare case has already been initiated against the parents is in itself an indication that there at least is reason to question whether or not these parents are sufficiently capable of protecting the child´s privacy interests from being exposed on the Internet.

Based on this, questions may also be raised as to whether the law should assume that parents have full authority with regard to this issue, or whether the law should restrict the parents' right of determination in such cases. There is no doubt that considerations of the best interests of the child and of the child´s need for protection of his/her interests indicate that legal

[8] Ibid

[9] Livingstone and O´Neil (2014) p. 31

[10] Ibid

measures will be needed to ensure adequate protection of such children. Accordingly, one of the questions discussed in this thesis is whether the EU´s new General Data Protection Regulation protects children in these situations. (see chapter 3.)

It is important to point out that this dissertation focuses on parents who share information about their child welfare cases on social media platforms by for instance making videos about the case, by putting the decision of the courts online, or by in any way exposing the case to an unlimited audience, without any attempt at anonymizing the case. Anonymizing the case implies taking out all information that could identify the child or children in question. Should the State intervene in such situations in order to protect children´s privacy from violation by their own parents? This is the question I attempt to answer in this dissertation.

Cases where information about the child is anonymized so that the child cannot be identified, entail just a general criticism of the child welfare system on the Internet, and are therefore not discussed in this thesis. It goes without saying though that totally anonymizing the identity of the child in a child welfare case will be nearly impossible since the fact that the parents are the parents of the child in itself is enough to identify the child in question.

Worthy of observation is that the arguments in this study may be relevant to the disclosure of other types of information about children, such as pictures, health information, etc. However, even though these are major and important themes, the limited framework of the dissertation will not permit me to discuss the exposure of every type of sensitive information about children on the Internet. Furthermore, such topics have already been covered in other types of literature.[11] The applicable rules on privacy will be discussed to the extent that they are of particular relevance to the data privacy rights of children in child welfare cases.

A central part of this dissertation is a discussion of the extent to which the European Union´s (EU) General Data Protection Regulation (GDPR), which will be the main data privacy regulation applicable in Norway from 25th May 2018, can be said to provide adequate protection of children´s data privacy rights from violation by their own parents. And if that is not the case, whether other legal basis' will have to be relied upon in order to take care of Norway's obligations under article 16 of the UN Convention on Children´s Rights (UNCRC), which gives children the right to the protection of the law against interference in their privacy. These discussions are found in chapters 3 and 4 respectively.

[11] **See for instance Tørgesen (2015) who has published a paper about this topic in *Tidsskrift for familierett, arverett og barnevernrettslige sspørsmål. Gyldendal Rettsdata.* P. 202-219. The article is based on a master thesis she had previously written on the topic.**

If the conclusion in chapters 3 and 4 is that the GDPR does not provide effective protection of the data privacy rights of children in the child welfare system, the duty of the State to ensure effective protection of the child's right to private life according to article 8 of the European Human Rights Convention (ECHR) will also be discussed. Effective protection means that legal provisions alone are not enough, but that the State must have an enforcement body or a real possibility of enforcing the applicable rules.

1.2 Terminology – Definition of Key Terms in the Study

A number of key expressions used in this dissertation are quite vague. In this section I try to clarify the most essential of these expressions for the purpose of my study.

1.2.1 Legal age of Maturity and Right to Consent

The main topic of discussion in this dissertation is whether children have the right to protection against exposure of their privacy online by their own parents pursuant to the GDPR, the UNCRC and the ECHR. This brings to the forefront the question of which legal subjects are protected by these rules as "children." According to the Norwegian Guardianship Act section 2 paragraph 1(a),[12] a person under guardianship is a person below the age of 18 years. This is also the age of maturity that is assumed in the UN Convention on the Rights of the Child (UNCRC), c.f. article 1. For the purpose of this thesis, I rely on the definition of a child as provided in the Norwegian Guardianship Act and the UNCRC.

Children have the same right to protection of their privacy as their parents. For adults, the disclosure of personal data requires consent from the person in question, c.f. the Norwegian Personal Data Act section 2. The GDPR defines *consent* of the data subject as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her", cf. article 4 number 11.

The difference between children and adults regarding consent is that even though a child is a legal entity on its own, the right to consent is granted to the parents (or legal guardian) to protect them. The person who has parental responsibility therefore usually has the competence to consent to the publication of personal information about the child. This, of course, also means that the person has the right to refuse that such information be published. Interesting issues arise when parents and children disagree whether or not to disclose such information.

[12] Lov om vergemål for umyndige av 26. mars 2010 (vergemålsloven)

And when the child is too small to understand, the question becomes who will protect the child's data privacy rights from abuse by the parents?

The age limit for children's consent when using information society services is set at 16 years in the GDPR, but the GDPR also gives room for member states to set this age limit to as low as 13 years, c.f. article 8 number 1. Processing the data of children below this age requires consent from the parents of the child in question. In the Norwegian Ministry of Justice´s proposal for a new Personal Data Act based on the GDPR, the Ministry proposes that the age of consent be set to 13 years[13]. If this proposal is adopted, it will mean that children who have reached the age of 13 can generally consent to the collection and use of their personal data.

Accordingly, cases where the child is over 13 years old and where the parents receive the child´s consent before publication fall outside the scope of this thesis. On the other hand, cases where the State believes that the child´s privacy is being violated despite the fact that the child has granted his/her consent to publication (i.e because the child does not understand what is in his/her own best interest) fall within the scope of the dissertation. The question then becomes to which extent should the State be able to intervene on its own initiative in such cases?

1.2.2 Sensitive personal data

The issues discussed in this thesis raise questions about what types of data are regarded as sensitive personal data. It is therefore necessary to clarify the extent to which child welfare cases can be classified as sensitive personal data, and whether children´s need for protection regarding such data goes beyond the need for protection of other types of personal data.

The general rule under section 3 of the Norwegian Freedom of Information Act (offentleglova)[14] is that all government documents are open for public scrutiny. Exceptions to this general rule require a legal basis in law. Child welfare cases are exempted from this general rule because they are regarded as sensitive personal information pursuant to section 6-7 of the Child Welfare Act.[15]

The term sensitive personal information or sensitive personal data is not defined specifically in the Child Welfare Act, and neither is it defined in the GDPR. However, paragraph 51 of the preamble to the GDPR states that "personal data which are, by their nature, particularly

[13] Høring om utkast til ny personopplysningslov (2016) p. 112 ff.

[14] Lov om rett til innsyn i dokument i offentleg verksemd av 19. Mai 2006 nr. 16

[15] Lov om barneverntjenester av 17. Juli 2002 nr. 100

sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms." The current Norwegian Personal Data Act also does not give a clear definition of what sensitive personal data is but instead lists up certain information as sensitive information. Examples of these are information about race and ethnicity, political, philosophical and racial affiliation, health conditions, sexual orientation, etc, cf. section 2 number 8 of the Data Protection Act.

In chapter 5, I discuss whether the private parties in a child welfare case should also be subject to a duty of confidentiality in the Child Welfare Act, because of the sensitive nature of such cases.

1.2.3 The Right to Data Protection

The right to data protection "establishes and underpins an individual´s right to control the storage and circulation of data about himself."[16] This definition presupposes that storage and circulation of data about an individual requires consent from the person (see 1.2.1 above). For children who are too young to give their consent, the right to consent is granted to the parents (or the person with parental responsibility for the child), who have to consent on the child´s behalf. The concern that this raises with regard to the object of this study is whether parents who share sensitive information about child welfare cases online, give adequate consideration of the child´s right to data protection when sharing such information.

In its consideration of the fourth periodic report of Norway,[17] the UN Committee on the Rights of the Child[18] expressed concern about information that parents may violate their children's right to privacy when revealing the particulars of their children's lives on webpages, sometimes in order to support positions in custody conflicts.[19] The committee therefore recommended Norway to mandate the Norwegian Data Protection Authorities (DPA) to prevent parents and others from revealing information about children, which violates children's right to privacy and is not in their best interests.[20]

---

[16] Report of the Committee on data protection (Cmnd 734,1978), chairman: Sir Norman Lindop, para 2.04 in Tugendhat, et al. (2002) p.154

[17] The Committee´s consideration of the fourth periodic report of Norway (CRC/C/NOR/4) 11-29 January 2010

[18] The Committee on the Rights of the Child (CRC) is a body of 18 Independent experts that monitors implementation of the UNCRC by its State parties. It also monitors implementation of the two Optional Protocols to the Convention. Source: http://www.ohchr.org/EN/HRBodies/CRC/Pages/CRCIndex.aspx. Accessed 03.11.17

[19] Ibid para. 28

[20] Ibid para. 29

In adhering to this recommendation and also the recommendation of other leading experts on the subject matter (see chapter 3), Norway made an amendment to section 11 of the current Personal Data Act with a third paragraph which states that "personal data relating to children shall not be processed in a manner that is indefensible in respect of the best interests of the child". How the upcoming GDPR affects this provision is at the core of this study and is discussed in detail in chapter 3.

1.3 Legal Issues and Structure of Thesis

The main topic of discussion in this paper is the extent to which the law protects children whose parents disclose sensitive information about their child welfare cases on social media. The Norwegian Personal Data Act imposes upon anyone dealing with children´s data to not handle it in a way that is indefensible. However, the upcoming GDPR will be replacing the current Norwegian Personal Data Act from 25th May 28, (see 2.2.2.1 below). In chapter 3, I critically discuss the GDPR´s provisions on children´s rights to data privacy in an effort to find out whether the GDPR ensures a better protection of the data privacy rights of children in the child welfare system from abuse by their own parents, as compared to the current Norwegian Personal Data Act. As part of this discussion, I assess whether the GDPR represents a setback or an advancement in the endeavours for better privacy protection for these children.

If it is found that the GDPR does not provide adequate protection of the data privacy rights of children in the child welfare system, the question then becomes whether other sources of international law such as the UN Convention on Rights of the Child and the European Human Rights Convention can be relied upon for a better protection of the data privacy rights of such children. Will a child who claims inadequate protection of his data privacy rights by the Norwegian State prevail in the European Court of Human Rights in light of these international human rights conventions? This is the topic of discussion in chapter 4.

A consideration of the rights that parents have to free speech and free expression assumes that parents have the right to criticise the State (and the child welfare services as such). The state may therefore be reluctant to prevent parents from sharing information about their own children online. This situation implies that there are conflicting interests. Alderson[21] rightly observes that "…anyone´s claim to a right automatically states concern for everyone else´s equal claim to it". The endeavours to protect children´s data privacy rights from abuse by their own parents has a tendency to go against liberal and libertarian attempts to keep the

[21] Alderson (2002) p. 442 in Livingstone and O´Neil (2014) p. 21

Internet open and free. Accordingly, the promotion of children´s online protection in general appears to contrast with the prevalent liberal view that the Internet should not be controlled or regulated if this weakens freedom of expression. Some argue that the Internet cannot efficiently be governed through legislation, and/or that there are more important priorities than those of children´s Interests.[22] Further in chapter 4, I make an assessment of the child´s right to privacy and the parent´s right to freedom of speech. How far can the state go in protecting the data privacy rights of children in the child welfare system without violating the parents´ right to freedom of speech?

In chapter 5, I give my concluding remarks.

In order to answer the above mentioned questions, a variety of sources were consulted.

[22] Livingstone and O´Neil (2014) p. 21

2 Methodological Issues and Sources of law

This dissertation falls within two main areas of law, namely data privacy law and international human rights law. Since the focus is on the data privacy rights of children in the Norwegian child welfare system, I have consulted both local Norwegian sources of law as well as international sources of law. Because of the future-oriented nature of the topic of study, some methodological issues were encountered as I did my research. In the following I account for these issues as well as the relevant sources of law.

2.1 Methodological issues

The GDPR which is the regulation at the centre of this thesis entered into force on 24th May 2016, but will start applying from 25th May 2018. Thus, there is yet to be practical case studies based on it. I have therefore had to rely on case law pertaining to other sources of law, even though the GDPR is the central focus in the study. Also, because most countries (including Norway) are still in the process of making law proposals to implement and complement the GDPR, many background materials and evaluations by lawmakers were not yet complete at the time of the writing of the thesis.

For instance, during the initial stages of my research, the Norwegian Ministry of Justice was yet to send out the law proposal for implementation of the GDPR, for public consultation. When it was finally circulated for public consultation, the deadline for consultative bodies to submit their comments was set to the 16th of October 2017. The opinion of important consultative bodies such as the Ombudsman for Children, the Norwegian DPA and the Norwegian Ministry of Children and Equality, were documents I needed in order to make a comprehensive assessment of the proposal. Even though these were available before the deadline for submission of the thesis, the Ministry´s final version of the proposal was not yet available at the time of the writing of this thesis. The extent to which the Ministry of Justice took the opinions of such important consultative bodies into consideration in the final version of the proposal would have served as a good point of discussion for this paper.

Furthermore, most of the literature pertaining to the GDPR are online articles and papers that are the opinions of certain individuals. The reliability of such articles as analytical tools is therefore uncertain since not all of these articles are written by prominent authorities in the field. Nevertheless, online background materials on the GDPR were found useful for the object of my study. Despite these challenges, I was able to find ample good sources of material for the purpose of my research.

2.2 Sources of law

2.2.1 The EU´s General Data Protection Regulation (GDPR)[23]

The GDPR was adopted on 27th April 2016 and becomes enforceable from 25th May 2018. It is a regulation through which the European Union (EU) aims to strengthen and unify data protection for all individuals within the EU. [24] The main goal of the GDPR is to give control back to data subjects over their personal data[25] and also to simplify the regulatory atmosphere for economic and social progress. [26]

When the GDPR enters into force, it will repeal the current EU Data Protection Directive (DPD)[27] and the national data privacy regulations of member states. A noteworthy difference between the DPD and the GDPR is the fact that the DPD is a directive whereas the GDPR is a regulation. A directive "sets out a goal that all EU countries must achieve" but each member state is free to make its own laws on how to achieve that goal[28]. A regulation on the other hand has binding legal force and "must be applied in its entirety across the EU" after its entry into force.[29] Consequently, the GDPR is the main legal framework in this study as it is going to be the future Data privacy regulation in Norway from 25th may 2018. All the legal issues raised in this thesis are discussed in light of the GDPR.

2.2.2 UN convention on the rights of the child (UNCRC)[30]

The UNCRC is an international treaty which was ratified by Norway on 8th January 1991, and was together with its two optional protocols integrated into Norwegian national laws on 1st august 2003[31], thereby giving it a special status in Norwegian law in the sense that it prevails over domestic Norwegian laws in case of conflict.

The UNCRC lays down fundamental principles that apply without prejudice to all children, delineates basic rights that national governments should implement, and offers a practical

[23] (Regulation (EU) 2016/679)
[24] C.f Preamble to the GDPR nr. 10
[25] Ibid nr. 7
[26] Ibid nr. 2
[27] Directive 95/46/EC
[28] http://europa.eu/eu-law/decision-making/legal-acts/index_en.htm Accessed 28.03.16
[29] Ibid
[30] Available at: http://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx. Accessed 19.08.17
[31] see lov om styrking av menneskerettighetenes stiling i Norsk rett av 21.05.1999 section 2, paragraph 4

guide to policy action[32]. Although other human rights conventions apply to all human beings, including children, e.g. the UDHR[33], the OSCE[34], the SP[35] and the ECHR[36], the UNCRC clarifies the position of the child as a legal entity and emphasises that children count in terms of human rights, thereby laying down individual rights for children in areas where necessary. Children´s right to privacy is enshrined in article 16 of the UNCRC, which states that no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation, and that the child has the right to the protection of the law against such interference or attacks. The UNCRC is therefore one of the main international sources of law I rely on in this thesis.

A keystone of the UNCRC is the assertion that "in all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration", cf. article 3. An assessment of the best interest of the child is therefore the most important issue to be considered when making decisions in any child welfare case. This is also enshrined in the Norwegian Child Welfare Act section 4-1. The extent to which the GDPR not permitting the establishment of national legislation on the treatment of children's personal data with a general scope of activity, can be said to be in the best interest of the child, is discussed in chapter 3.

2.2.3 The European Convention on Human rights (ECHR)

The European Convention on Human Rights (ECHR) which entered into force in Norway on 3rd September 1953 is the most important convention in place to protect fundamental freedoms and rights in Europe and is therefore essential for this thesis. Like the UNCRC, it is incorporated into Norwegian national laws, and therefore has priority over domestic Norwegian laws in case of conflict[37].

---

[32] The UNCRC is ratified by 194 countries, making it the most rapidly and widely ratified human rights treaty in history. Somalia, South Sudan, and the United States are the only countries that have not yet ratified the treaty. Source: https://www.hrw.org/news/2014/11/17/25th-anniversary-convention-rights-child. Assesed 20.08.17.

[33] Universal Declaration of Human Rights

[34] UN Convention on Economic, Social and Cultural Rights

[35] UN Convention on Civil and Political Rights

[36] European Convention on Human Rights

[37] see lov om styrking av menneskerettighetenes stiling i Norsk rett av 21.05.1999 section 2, paragraph 1.

Pursuant to article 8 of the ECHR, "everyone has the right to respect for his private and family life, his home and his correspondence" and the state has an obligation to respect this right.

2.2.4 Case law

The above-mentioned European Human Rights Convention established the European Court of Human Rights (ECtHR). Anyone who believes their rights have been violated under the Convention by a State Party can bring their case to the Court.[38] Judgments finding violations are binding on the State concerned and the State is obliged to execute the judgement.[39] Cases from the ECHR play a central role in this study. In this regard, the focus is on the positive obligation of the State to put measures in place, be it legislative or otherwise, in order to ensure that children´s rights to protection against online privacy violations by their own parents is secured.

[38] See ECHR article 34

[39] Ibid article 46

3 To Which Extent Does the GDPR Ensure Effective Protection of the Data Privacy Rights of Children from Abuse by Their Own Parents?

The state as the primary protector of the rights of its citizens has a duty to ensure that children´s rights to data privacy is protected from abuse by all data processors including their own parents. The current Norwegian Personal Data Act ensures that children's interests in this regard are secured to a large extent. The question I seek to answer in this dissertation is how the GDPR will affect this state of the law from 25th May 2018, given that the GDPR will be totally harmonised across EU/EEA nations. As noted in chapter 1, the Norwegian Personal Data Act did not have any specific regulations for children's data privacy until April 2012. Before then, it was assumed that the general regulations in the Data Privacy Act were also applicable to children.

In this chapter, I take a critical look at how the legislation on children´s data privacy rights in Norway has developed over the years, and discuss the extent to which the GDPR represents an improvement or setback in the developments that have been made so far. If I find that the GDPR does not provide adequate protection of children´s data privacy rights from abuse by their own parents, then I will discuss whether Norway may have to find a way of highlighting children's data privacy rights when complementing the GDPR.

3.1 Development of the Legislation on Children's Rights to Data Protection from Their Own Parents

3.1.1 Legal Provisions on Children´s Rights to Data Privacy Before 20th April 2012

It is important to understand the state of the law on children´s privacy rights in Norway before 2012, in order to understand why the legal status is as it is today. Before April 2012, namely before section 11 of the Norwegian Personal Data Act was amended with a third paragraph concerning the processing of children´s data, Norwegian legislation on privacy was not very much concerned with children´s privacy. The basic principle was that children and adults had the same rights to data protection under the Personal Data Act. However, in the case of minors, the parents or the person with parental responsibility would usually be the person acting on behalf of the child. Consequently, the general provisions in the Personal Data Act had to be supplemented with the rules of the Children´s Act (Barneloven) in order to give a full picture of children´s legal status with regard to data privacy.

Pursuant to section 30 of the Children´s Act, parents have the right and duty to make decisions on behalf of their child in personal matters. Whether this right includes the right to consent to the processing of the child´s personal data does not follow directly from the provision. However, some legal scholars assume that the right to consent on behalf of the child also includes consenting to the processing of the child´s personal data.[40]

With the emergence of social media platforms such as Facebook and blogs, leading children´s rights scholars started asking questions about possible legal limitations on parents' rights to consent on behalf of the child, to the sharing of pictures and sensitive information about them on the Internet[41].

Section 2 of the Personal Data Act states that the Act does not apply to the processing of personal data carried out by a natural person for exclusively personal or other private purposes, c.f. section 3 paragraph 2 of the Act. On the basis of this provision, the Norwegian Data Protection Authorities (DPA) regarded the publication of pictures on personal websites as exempted from the scope of the Act in its practices.[42]This was the situation until the European Court of Justice (ECJ) made its ruling in the *Bodil Linquist*[43] case. In this case, Mrs. Bodil Lindqvist, a Swedish church worker had published a local parish magazine on her personal website. She set up Internet pages on her home computer to help parishioners getting ready for their confirmation. The pages included information about other parish workers, such as their names, telephone numbers and hobbies. She had not obtained the consent of the individuals concerned and was therefore found to not have complied with the EU´s current Data Protection Directive.[44] The court held that the Data Protection Directive applies to the publishing of personal data on the Internet, no matter how inoffensive or trivial the information is.[45]

After the ruling in the *Bodil Linqvist* case, the Norwegian DPA changed its practices, and the publication of pictures on private home pages was no longer exempted from the provisions in the Personal Data Act. However, the exception in section 7 of the Personal Data Act regarding the processing of personal data exclusively for artistic, literary or journalistic purposes implied a limitation on the DPA´s ability to intervene in online privacy violations. When the DPA received inquiries about situations where parents had published information

[40] See for instance Smith Smith (2011) Om Barns Personvern p. 106-126

[41] See for instance Smith (2011) p. 106-126 who criticised the situation at the time especially with regard to parents sharing their children´s health information in newspapers and sharing unflattering pictures of children on Facebook.

[42] ibid

[43] Case of Bodil Lingqvist v. Sweden. Judgement of 6. 11. 2003 — Case C-101/01

[44] Directive 95/46/EC

[45] Ibid paragraph 47 and 48

about their child welfare cases on the Internet, the DPA assumed that such publications were for the purposes of public opinion, and therefore fell outside the competence of the DPA[46]. This was despite the fact that child welfare cases often contain a lot of sensitive information.

Several experts in the field were of the opinion that parents´ right to share children´s personal data online must also be subject to certain absolute restrictions, even if pursuant to the Personal Data Act, they fell outside the scope of the DPA´s jurisdiction. Examples of experts who raised this issue are Smith in her publication on children´s data privacy[47], Bygrave and Schartum in their report of 2006[48], and the Data Privacy Commission´s report of 2009.[49]

The general consensus was that there must be certain restrictions on parental consent to the online publication of children´s personal data by parents. However, there was uncertainty as to which rules applied and which should apply. For instance, Smith suggested that changes should be made in the Personal Data Act, which as far as possible ensures the prevention of such publications and also ensures that there is a legal basis for deletion if it happens anyway.[50] Bygrave and Schartum on the other hand proposed a general regulation of the relationship between children and parents within the framework of the Personal Data Act[51].

In addition to these recommendations by experts in the field, the UN Committee on the Rights of the Child also expressed concern about the fact that some parents violate their children's right to privacy by sharing sensitive information about ongoing custody cases online, and recommended changes in the existing regulation in order to prevent parents and others from revealing information about children, which violates children's right to privacy and is not in their best interests.[52]

Based on these concerns raised about the protection of children´s data privacy and recommendations from the experts in the field, the Norwegian Ministry of Justice agreed to strengthen the data privacy rights of minors by amending section 11 of the Personal Data Act with a third paragraph which states that *"personal data relating to children shall not be*

---

[46] See page 8 of the DPA´s consultative comments to NOU 2009: 1.

[47] Smith (2011) Om Barns Personvern p. 106-126

[48] The Ministry of Justice gave professors Dag Wiese Schartum and professor Lee Bygrave of the University of Oslo the task of investigating various issues related to the current DPA. As a result of this investigation, two reports *"Utredning av behov for endringer I personopplysningsloven" (2006)* and *"Utredning om fødselsnummer, fingeravtrykk og annen bruk av biometri i forbindelse med lov om behandling av personopplysninger § 12" (2008)* were submitted to the Ministry. These are available at https://www.regjeringen.no/contentassets/daad3dbe61c74f5c9240d16478b088ba/rapport_g-390.pdf and https://www.regjeringen.no/contentassets/daad3dbe61c74f5c9240d16478b088ba/g-0406.pdf respectively.

[49] NOU 2009:1 *Individ og Integritet- Personvern i det digitale samfunn.* See chapter 14 on data privacy for children and youth.

[50] Smith (2011) p. 106-126

[51] Prop. 47 L (2011-2012) Proposisjon til Stortinget (forslag til lovvedtak)

[52] The Committee´s consideration of the fourth periodic report of Norway (CRC/C/NOR/4) 11-29 January 2010

processed in a manner that is indefensible in respect of the best interests of the child".[53] What is meant by the term "indefensible" in this provision and how the provision contributes to ensuring an effective protection of children´s data privacy rights is the topic of discussion in the next section.

3.1.2 The Current Rule of Law on Children´s Right to Data Privacy in Norway According to the Personal Data Act

The fundamental principle according to the current Data Privacy Act is still the same as it was before the amendment of section 11 in 2012, namely that children and parents have the same rights to protection of personal data. Children´s personal data is nevertheless given special protection pursuant to section 11 paragraph 3 which states that children´s personal data shall not be processed in a manner that is *indefensible* in respect of the best interests of the child. This provision was as already observed, adopted to strengthen the rights of minors in the processing of their personal data.

It is necessary to define the term "indefensible" in section 11 paragraph 3, in order to find out the extent to which child welfare cases are encompassed by this provision. According to the Norwegian Ministry of Justice, what qualifies a processing of data as "indefensible" in light of section 11 paragraph 3 will depend on a concrete assessment of the particular case, and that the term "indefensible" refers first and foremost to the more reprehensible kinds of processing of personal data.[54] The Ministry further observes that data processing that is obviously offensive to the child will fall into this category, and explicitly mentions cases where parents expose information in an ongoing child custody or child welfare case as examples of processing that will be clearly contrary to the child's interests.[55]

Accordingly, the preparatory works of the law strongly indicate that publishing sensitive material about children online, such as child welfare cases, can, depending on a concrete assessment of the individual case, be in breach of the provision in section 11 paragraph 3 of the current Personal Data Act. It is therefore unlawful for parents to share sensitive information about child welfare cases on social media, and when such a clear violation and abuse of children´s personal data occurs, the law mandates the DPA to demand that the information be deleted.[56]

---

[53] Prop. 47 L (2011–2012) chapter 5

[54] Ibid p. 18

[55] Ibid

[56] Ibid

It is noteworthy that the provision does not contain any restriction on who can invoke it. Therefore, anyone who is concerned about the privacy of a minor can contact the DPA, and the DPA can also act on its own initiative when it observes serious cases of violation of children´s data privacy. Consequently, one can safely conclude that the provision in section 11 paragraph 3 protects many children whose views are not taken into consideration by their parents, or are unable to form their own opinions in situations where their privacy is clearly not respected.

Also, even though the provision may to a lesser extent, be directly applicable to children who share information about themselves online, the provision may apply to a website that uses such shared information, if it uses the information irresponsibly.[57] Therefore, for children in the child welfare system (and for children in general) the current Personal Data Act section 11 paragraph 3 serves as a "safety net" to protect their privacy rights from violation or abuse by others, including their own parents. To my knowledge, there is yet to be available case law on the basis on this provision.

3.1.3 The Rule of Law on Children´s Rights to Data Privacy According to the GDPR

In the section above, it was concluded that the current Data Privacy Act has a "safety net" in its section 11 paragraph 3, that protects children´s data privacy rights from violations by their own parents. However, this Act will be replaced by the GDPR when it enters into force on 25th May 2018. In this section I discuss how the GDPR will affect the current state of the law when it enters into force.

The GDPR does not have any uniform regulation of children's data privacy rights. The treatment of children´s personal information is scattered in different articles and in various sections of the preamble. As part of the process of incorporating the GDPR into national law, the Norwegian Ministry of Justice sent out a draft proposal for a new Personal Data Act, for public consultation[58]. The GDPR will be incorporated into the EEA Agreement [59] and implemented in Norwegian law. The provisions of the Regulation will in essence have to be

[57] Ibid.

[58] Høring om utkast til ny personopplysningslov – gjennomføring av personvernforordningen i norsk rett. 06.07.2017. Available at https://www.regjeringen.no/contentassets/c907cd2776264a6486b8dd3ee00a4e3d/horingsnotat--ny-personopplysningslov--gjennomforing-av-personvernforordningen-i-norsk-rett.pdf

[59] The Agreement on the European Economic Area, which entered into force on 01.01.94, brings together the EU Member States and the three EFTA States (Iceland, Liechtenstein and Norway) in a single market, referred to as the "Internal Market." Source: http://www.efta.int/eea/eea-agreement. Assessed 08.11.17

applied as they stand, but the Regulation also leaves room for national regulation in certain areas.

In the proposal for a new Personal Data Act, the Ministry of Justice states that the GDPR does not open for the establishment of national laws regarding the processing of children's personal data with a general scope of activity.[60] This, according to the Ministry implies that the GDPR does not permit Norway to maintain the provision in section 11 paragraph 3 of the current Personal Data Act which states that *"personal data relating to children shall not be processed in a manner that is indefensible in respect of the best interests of the child".* The Ministry further states that in cases where parents violate their own children´s privacy online, the GDPR does not give the Data Protection Authorities a clear legal basis to intervene, as they can today because of the provision in section 11 paragraph 3 of the current Personal Data Act.[61] Whether the DPA will be able to intervene in such cases within the framework of the GDPR must, according to the Ministry be assessed on a case by case basis.[62] The Ministry refers to section 31 of the Children's Act regarding children's right of participation in cases concerning them, and the parents´ duty to listen to children before making decisions about their personal circumstances, as possible legal basis to rely on in such cases.[63]

Based on this, it can be safely concluded that when the GDPR starts applying from 25th May 2018, there will no longer be an explicit rule of law in Norwegian legislation that protects children in the child welfare system whose parents (or legal guardians) violate their data privacy rights by sharing sensitive information about their case on the Internet. Thus the GDPR may entail a limitation in children´s rights to protection of their online privacy as compared to the protection they enjoy today pursuant to the current legislation.

The effect this development will have on children´s rights to data privacy is discussed in the next section, and other legal basis one can rely on in order to protect children in such situations is discussed in chapter 4.

[60] Høring om utkast til ny personopplysningslov (2017) p 115.

[61] Ibid

[62] Ibid

[63] Ibid

3.2 Does the GDPR Provide Adequate Protection of Children´s Data Privacy from Abuse by Their Own Parents?

In the section above, it was concluded that the GDPR does not permit explicit national provisions on children´s rights to protection of personal data from violations by their own parents. Based on this conclusion, the topic of discussion in the following is the extent to which the GDPR can be said to provide adequate protection of children´s online privacy.

It is an indisputable fact that specific data protection rules for children are immensely welcome in a world where people of all age groups are avid users of online services and therefore run risks of having their own and others personal data used and abused.[64] Many applaud the GDPRs provisions on children´s privacy rights because as compared to the EU´s current Data Protection Directive, it highlights children´s right to privacy and acknowledges children as more autonomous and independent when growing up, and does not require parental consent for data processing when children are above the age of 13.[65] Also, recital 38 of the preamble to the GDPR mentions children as a particularly vulnerable group that deserves special protection. Even though the GDPR emphasizes on children´s need for special protection, it nonetheless does not specify how this special protection of children´s privacy is intended in practice when the person the child needs protection from, is the child´s own parents.

One could argue that the provision in section 11 paragraph 3 of the current Personal Data Act may only be applicable in a few and particularly serious cases, especially given the fact that the provision has been dormant since it entered into force. However, there is reason to be concerned that not having a similar provision in the future Personal Data Act will de facto reset the state of the law back to how it was before this provision was amended to the law. This means that the possibilities of protecting children from data privacy violations by their own parents will be basically non-existent.

I agree with the ministry of Justice that the provision in section 11 paragraph 3 of the current Personal Data Act cannot be maintained because the GDPR does not permit the establishment of national legislation on the treatment of children's personal data with a general scope of activity. It must nevertheless be noted that it is a regrettable consequence of this otherwise well-meant Regulation. How then can the State protect children whose parents publish sensitive information about them online? Which legal basis can the state rely on in such situations?

[64] van der Hoff (2014) p.139

[65] Ibid

In the above-mentioned consultation paper on the implementation of the GDPR, the Ministry of Justice highlights the children's Act as the future legal basis on which to rely when parents share sensitive information about their own children online.[66] In particular, the Ministry refers to section 31 that emphasises on children´s right to be heard in matters that concern them. However, as shown in the criticisms that led to the inclusion of section 11 paragraph 3 in the current Data Protection Act, (see 3.1.1 and 3.1.2 above), neither the Child Welfare Act nor the Children's Act can protect children from the most serious violations of their data privacy by their own parents. This, despite the fact that such violations are considered to be in breach of both the Children's Convention and the Children's Act. It goes without saying that if it had been possible to rely on the Children´s Act alone for effective protection of children´s data privacy, there would have been no need for an amendment of the current regulation in the first place.

Worthy of note is that the Children's Act is a private law that regulates the relationship between parents and children and that the law does not open for state control or sanctions related to how parental responsibility is exercised in accordance with the Act. The fact that the Children's Act is a private law without state control or possibility of sanctions means that it is hard to imagine a provision in the Children's Act that can protect a child from a parent who chooses to share sensitive personal data about them on the Internet. I therefore believe that there is a need for a more thorough account and discussion of how children's privacy can be safeguarded in other ways, such as how information can be deleted when publishing information contrary to section 31 of the Children's Act.

My assessment therefore is that the GDPR does not provide adequate protection of the data privacy rights of children in the child welfare system (and other children in general). If parents themselves do not take into consideration the best interests of the child when disclosing their personal data online, neither the Children's Act, the Child Welfare Act nor the future Data Privacy Act contains sufficient legal basis and mechanisms to ensure that this type of personal information is deleted after it has been posted online. This lack of remedies for children in such situations was the basis for the mandate granted to the DPA in section 11 paragraph 3 of the current Data Protection Act, to demand such information removed if they are deemed contrary to the best interests of the child.

In my opinion, the Ministry of Justice in its review of how the GDPR will affect children´s right to data protection from violation by their own parents attaches too much importance to the Children's Act even though it is evident that the Children´s Act does not provide sufficient

[66] Høring om utkast til ny personopplysningslov (2016) p 115

legal basis for the protection of children in such situations. What I find interesting though is that important consultative bodies such as the Ombudsman for children, the DPA and Save the Children commented[67] on this issue in their response to the Ministry of Justice´s consultation paper. However, the Ministry of Children and Equality which is the main ministry in charge of protecting children´s rights in Norway was totally silent on the matter, and had no comments whatsoever to the consultation paper. What this silence from the Ministry of Children and Equality signifies is not easy to tell, but it gives reason to question the extent to which the data privacy rights of children in the child welfare system can be said to be of importance to the Ministry. It could also be simply because the Ministry has not fully understood the importance of this issue.

3.3 Conclusion

In this chapter, I have discussed whether the GDPR provides the same or better protection for children's privacy interests as the current Norwegian Personal Data Act. I have undoubtedly concluded that the GDPR does not, and thus, the introduction of the GDPR results in limitations in the protection of children´s data privacy rights from violations by their own parents. It may be that this conclusion will not be supported by the European Court of Justice if the issue were brought before it. However, whatever the correct interpretation of the GDPR is and no matter how the GDPR will be practiced by the European Court of Justice, it is now a fact that the Ministry of Justice in Norway is of the view that the GDPR does not permit Norway to provide the Data Protection Authority with competence to protect children in the situations discussed in this dissertation. This will be decisive for children's rights in Norway in practice and consequently, the introduction of the GDPR will actually entail constraints in children's rights as compared to the current state of the law.

The principle of the best interest of the child will therefore still have to be relied upon if one wants to make a convincing argument as to why children´s sensitive data published by their own parents online should be removed. In my opinion, the child's right to the protection of his/her privacy should be an adequate justification for limiting parental consent to publishing of such data. Preventing parents from disclosing children´s personal information to the public is essential even if the disclosure cannot be said to be directly harmful to the child. It is therefore a sad development that instead of an explicit legal provision, the best interest of the child still has to be used as an argument for the protection of children's online privacy in a Regulation as modern and comprehensive as the GDPR. As will be seen in the next chapter,

[67] A complete list of consultative bodies that had comments to the consultative paper (and the comments they had) is available at: https://www.regjeringen.no/no/dokumenter/horing-om-utkast-til-ny-personopplysningslov--gjennomforing-av-personvernforordningen-i-norsk-rett/id2564300/. Accessed 13.11.17.

even the European Court of Human Rights (ECtHR) does not rely on the principle of the best interest of the child when dealing with cases on children´s right to privacy. It relies solely on the right that children have to privacy as enshrined in article 8 (1) ECHR, and also stresses upon the fact that children need special protection because of their vulnerability.

In conclusion, I would maintain that the GDPR may provide better protection for children in relation to commercial actors, but as compared to the current Norwegian Personal Data Act, it definitely represents a setback in the efforts to ensure better online privacy protection for children, against violations by their own parents. By focusing mainly on the processing of personal data by companies and commercial actors, the GDPR overlooks the right that children have to protection of their personal data from violation by their own parents.

Since it is have found that neither the GDPR nor other national sources of law ensure adequate protection of children´s data privacy rights, one may have to rely on international human rights law for adequate protection. The international instruments children may rely on in such situations is the topic of discussion in the next chapter.

4 Is the Right to Data Privacy for Children a Human Right?

In chapter 3, I found that neither the GDPR nor other national sources of law provide adequate protection of the data privacy rights of children from online violation by their own parents. The GDPR therefore entails a setback for the protection of the data privacy rights of children. Consequently, one may have to rely upon other relevant international sources of law for adequate protection of children´s online privacy rights.

Apart from the current Personal Data Act, which will be repealed by the GDPR in May 2018, the most important general rules on privacy in Norwegian law are article 16 of the UN Convention on the Rights of the Child (UNCRC), article 8 of the European Human Rights Convention (ECHR), and article 17 of the International Convention on Civil and Political Rights (ICCPR). All these provisions are, as noted in chapter 1, incorporated into Norwegian law, and therefore apply as Norwegian law pursuant to section 2 of the Human Rights Act (menneskerettsloven)[68]. This implies that they have priority over domestic Norwegian laws in case of conflict, c.f. section 3 of the Human Rights Act. Accordingly, in the absence of national laws on the protection of the privacy rights of children in the Norwegian child welfare system, one will have to rely on the provisions in these international conventions.

The focus of this chapter is two-fold. First of all, because the GDPR does not allow for a legal provision on children´s rights to protection of personal data from abuse by their own parents, this chapter discusses the extent to which the UNCRC, which lays out minimum entitlements and freedoms that governments have to fulfil regarding children´s rights, offers a recommendable legal basis for the effective protection of children´s data privacy. Secondly, I critically discuss the development of the case law of the European human rights courts (ECtHR) on children´s rights to respect for their data privacy. The goal is to analyze the extent to which a child who claims inadequate protection of his/her protection by the state because of the GDPR would prevail in the ECtHR. At the end of the chapter, I discuss how to resolve the conflict between children's rights to privacy protection, and parents' rights to freedom of expression.

[68] Lov av 21.05.1999 om styrking av menneskerettighetenes stilling i norsk rett

4.1 Children´s right to privacy according to the UN Convention on the Rights of the Child

Article 16 of the UNCRC states that:

"1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.

2. The child has the right to the protection of the law against such interference or attacks."

This article is equivalent to the provision in article 17 of the International Convention on Civil and Political Rights (ICCPR). Although children are also protected by the ICCPR, it was considered desirable to include the most important provisions on civil rights in the Children's Convention. This was done first and foremost to make it clear that these provisions also apply to children and that children are individuals with independent rights and the right to respect for their physical and mental integrity.[69] Apparently, this was not an obvious thing back in 1989.

It is important to note that article 3 (2) of the Children´s Convention imposes upon the State to ensure the child such protection and care as is necessary for his or her well-being, taking into account the rights and duties of his or her parents, legal guardians, or other individuals legally responsible for him or her, and, to this end, shall take all appropriate legislative and administrative measures. This provision read together with article 16 and the ECHR article 8, accentuate the need to protect children from violation of personal integrity, both online and offline. In other words, the most important international human rights conventions regarding children´s rights specify that children are entitled to respect for their physical and/or moral integrity and personal identity, and that they have the right to state protection, in the form of legislative or policy measures, to protect them against serious violations of their personal integrity through inter alia online publication and spreading of sensitive information about them. Children´s right to protection of their online privacy from abuse by others including their own parents is therefore a human right that the international community seeks to protect.

[69] Smith (2011) p. 106-126

This also brings to the forefront the question of the extent to which the GDPR, by not permitting States to have legislation that can provide efficient protection of children´s data privacy from abuse by their own parents, may be contrary to the provisions in the UNCRC.

Interpretative data regarding article 16 of the Children´s Convention is scanty, and as mentioned in chapter 2, there is no individual right of appeal relating to the Convention as there is for several other international human conventions. There are therefore no decisions to support the interpretation of Article 16. In addition, the Committee on the Rights of the Child has not prepared any general comments on Article 16. However, the Committee has given recommendations to States on this article. In its consideration of the 4th periodic report of Norway, the Committee had the following remarks:

"The Committee is concerned at information that parents may violate their children's right to privacy when revealing the particulars of their children's lives on webpages, sometimes in order to support positions in custody conflicts.

The Committee recommends the State party to mandate the Norwegian Data Inspectorate to prevent parents and others to reveal information about children which violates children's right to privacy and is not in their best interests."[70]

With this remark, the Committee addressed the issue where parents violate their children's right to privacy on the Internet. This piece of advice from the Committee, shows that the Committee aims to prevent parents or others from disclosing information about children, that violates children's right to privacy, by encouraging the State to give the DPA the power to prevent this from occurring. This also shows that the Committee assumes that article 16 provides protection of children's rights in the situations that are discussed in this dissertation. The committee also seems to assume that there is no doubt that this is the duty of the State. Based on the wording of the article and the Committee's interpretation, one can safely conclude that article 16 is to be understood as protecting the privacy of children from violation by their own parents.

[70] The Committee´s consideration of the fourth periodic report of Norway (CRC/C/NOR/4) 11-29 January 2010 numbers 28 and 29

The Committee has also expressed its concern about the media's breach of the right to privacy in connection with court proceedings and, moreover, the negative impact of the press on children and adolescents. The committee told the UK in 2008:

"37. The Committee recommends that the State party:
(a) Ensure, both in legislation and in practice, that children are protected against unlawful or arbitrary interference with their privacy, including by introducing stronger regulations for data protection;
(b) Intensify its efforts, in cooperation with the media, to respect the privacy of children in the media, especially by avoiding messages publicly exposing them to shame, which is against the best interests of the child;
(c) Regulate children's participation in TV programmes, notably reality shows, as to ensure that they do not violate their rights."[71]

The recommendation in number a) indicates that the Committee considers having stronger regulation for data protection as important to protect interference with children's privacy.

In light of these recommendations by the Committee, article 16 of the Children´s Convention can be considered to cover all forms of violations of personal privacy and the right to privacy, including personal data. It concerns improper publication of both images and printed text. It may be safe to say that children are considered to need more protection than adults.[72] This is also confirmed in the case law of the ECtHR (see below). The recommendations also indicate that it is not sufficient that the authorities themselves do not violate children´s right to privacy. Instead, it is also a requirement under article 16 that the authorities must take concrete measures to ensure that the rights are realized, including by legislation, and also by implementing such legislation. Consequently, a future law on data privacy that does not include a provision similar to that of section 11 paragraph 3 of the current Personal Data Act, may be in breach of the Children´s Convention. Given that the Children´s Committee has

[71] The Committee´s consideration of the third and fourth periodic report of the United Kingdom of Great Britain and Northern Ireland (CRC/C/GBR/CO/4) 20 October 2008. Pp. 8-9

[72] In the 2008 case of *S and Marper v. The United Kingdom* on the legality of retaining personal data after acquittal of a criminal offense, the ECtHR stated that" the Court further considers that the retention of unconvicted person's data may be especially harmful in the case of minors."

explicitly given a recommendation to Norway regarding this provision, and the provision was enacted partly due to this recommendation, I find it quite remarkable that it may be abandoned in the near future, thereby leading the state of the law back to where it was before this significant improvement was made.

The lack of legal basis to protect children´s privacy from abuse by their own parents in the GDPR is therefore not in conformance with the Committees recommendations, since it will rather contribute to weakening children´s legal position, instead of strengthening it.

The discussion above exhibits that the Children´s Convention article 16 provides a strong legal basis for children who want to claim a right to protection of their data privacy by the state. However since the Convention does not have an individual appeal system for children, children do not have an international organ before which they can invoke this right. A child who claims violation of his/her right to privacy by his/her own parents, but does not prevail before the Norwegian courts will therefore have to seek protection under the European Human Rights Convention, c.f article 34 ECHR. In the following, I critically discuss the development of the case law of the ECtHR with regard to children´s rights to online privacy. The question I seek to answer is whether the ECtHR has interpreted article 8 in a manner that gives children protection in situations where their online privacy is violated by their own parents.

4.2 Children´s Right to Privacy According to the European Convention on Human Rights

On the European level, the duty of the State to protect citizens from illegal and arbitrary interference in their privacy and family life, is enshrined in article 8 of the European Human Rights Convention. The ECHR article 8 regarding the rights of individuals to respect for private life has a direct impact on children's privacy, but it does not extend beyond the provision in article 16 of the Children´s Convention. It nevertheless is of utmost relevance for the purpose of this study because case law emanating from the ECtHR on this provision sheds light on children's right to legal protection of their privacy. In its application of article 8, the ECtHR has taken a versatile approach to the definition of the individual rights that the provision seeks to protect. Consequently, the scope of the provision continues to expand. In this section, I examine the right to privacy of children online, and the focus is on the extent to

which the provision protects children´s right to privacy when parents are violating their privacy on the Internet.

Article 8 ECHR states that:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 8 of the ECHR imposes upon states the obligation to respect a broad area of interests, namely: 1) private and family life and 2) home and correspondence. The set-up of the article suggests that its application requires a two-step test,[73]the first of which entails an evaluation of whether the complaint falls within the scope of article 8 number 1 as described above. If that is the case, the second state involves examining whether the interference with the right to privacy is consistent with the provisions of article 8 number 2. The questions that arise in this regard are as follows:
1) is the interference "in accordance with the law?"
2) does it pursue a legitimate aim, and
3) is the interference necessary in a democratic society?

Harris et al[74] rightly observe that a close look at the development of case law from the court shows that there are at least 6 classifications of activities and interests which the Court has held to be within the scope of "private life". These are: 1) private space[75] 2) personal identity[76], 3) collection and use of information[77] 4) moral or physical integrity[78] 5) social life[79]

[73] Harris et. Al. 2009, p. 363 in Groothuis 2014 p. 145

[74] Harris et al. 2009, pp. 366-371; cf. White and Ovey 2010, pp. 358-359 in Groothuis 2014 p. 145

[75] Von Hannover v. Germany No. 1, no. 59320/00, 24 June 2004.

[76] Gaskin v. United Kingdom, no. 10454/83, 7th July 1989.

[77] White v. Sweden, no. 42435/02, 19th September 2006

and 6) sexual activities.[80] The classification that is most relevant for the purpose of this study is the collection and use of information.

4.2.1 Analysis of Case Law Emanating From ECtHR

The ECtHR has confirmed that the term "private life" is a broad concept that is "not susceptible to exhaustive definition, which covers the physical and physiological integrity of a person and can therefore embrace multiple aspects of a person´s identity…"[81] However, the Court has in its case law given some guidelines regarding the meaning and scope of this concept. In the 1992 case of *Niemietz v. Germany*, the Court observed that:

"the court does not consider it possible or necessary to attempt an exhaustive definition of the notion of "private life." However, it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings."[82]

The Court has also emphasized that a child is entitled to respect for privacy as soon as the child is born. The 2009 case of *Reklos and Davourlis v. Greece*[83] concerned images that a professional photographer had taken of a new-born baby at a maternity clinic, without the consent of the child´s parents. The photographer´s intention was to sell the picture to the parents. The image was taken in a sterile room where the child was placed after birth. The clinic had refused to hand over the negatives of the parents. The court maintained that:

"private life" was a broad term that *"encompassed the right to identity. It stresses that a person's image revealed his or her unique characteristics and constitutes one of the main attributes of his or her personality."* The court found that Greek courts *had not taken*

---

[78] X and Y v. the Netherlands, no. 8978/80, 26th March 1985

[79] Slivenko et al v. Latvia, no. 48321/99, 9 October 2003.

[80] Dudgeon v. United Kingdom, no. 7525/76, 22nd October 1981.

[81] Axel Springer AG v. Germany, no. 39954/08, 7th February 2012 para 83

[82] Niemietz v. Germany, no. 13710, 16th December 1992.

[83] Reklos and Davourlis v. Greece. no. 1234/05. 15th January 2009

sufficient steps to ensure the child's "right to the protection of his private life" and that this was contrary to Article 8 of the ECHR.[84]

This case is particularly interesting because it is based exclusively on the child's right to protection of his/her unique identity. The Court by interpreting article 8 so that the child's identity includes the right to own his/her own images from birth even in situations where only the photographer/clinic had access to the image, indicates that the protection of identity as enshrined in article 8 must also include the right of children to protection against exposure of their child welfare cases online. This is particularly important when the information is posted on the Internet, to an unlimited number of people.

The case also illustrates that privacy applies from day one, and that even new-borns are entitled to the protection of their privacy. In this case, it was a matter of protection from being photographed. It is noteworthy that the best interest of the child was not mentioned by the Court.

The next question I look at is whether article 8 only prohibits the State from publishing such information online or whether the provision also imposes a positive obligation on the state to prevent such publications. This can for instance mean that the State may be obliged to provide regulations and policies that efficiently dissuade and prevent violation of the right to privacy. The 1985 case of *X and Y v. the Netherlands* and the 2008 case of *K.U v. Finland* are demonstrative in this regard.

The positive obligation for the State to protect the child´s right to privacy was formulated by the Court for the first time in the landmark case of *X and Y v. the Netherlands (1985)*[85]. In this case, the father of a mentally ill 16-year-old girl who had been raped in a privately-run mental home for handicapped children, filed a complaint to the police. Because the victim was mentally ill, she could not sign the complaint and the father was not allowed to sign on her behalf since he was not the victim and therefore could not file a complaint under Dutch Criminal law. The police therefore refused to file the complaint and institute criminal proceedings. Due to this procedural hindrance, the victim could not have any remedies under

[84] Case summary available at: http://www.5rb.com/case/reklos-and-davourlis-v-greece/. Accessed 17.11.2017.

[85] X and Y v. the Netherlands, no. 8978/80

the Dutch criminal code. The father filing a complaint under article 8 ECHR on behalf of his daughter argued that his daughter had been subjected to inhuman and degrading treatment, within the meaning of Article 3 of the Convention, and that the right of both his daughter and himself to private life, guaranteed by Article 8 had been infringed. He further maintained that the right to respect for family life, also guaranteed by the same Article meant that parents must be able to have recourse to remedies in the event their children have been victims of sexual abuse, particularly where minors[86]

The Court found that the Dutch Criminal Code did not provide the victim with practical and effective protection, and

"also, the protection afforded by civil law in the case of the wrongdoing in the kind inflicted on the victim was insufficient because this is a case where fundamental values and essential aspects of private life are at stake. Effective deterrence is indispensable in this area and it can be achieved only by criminal law provisions." [87] *The Court therefore concluded that "taking account of the nature of the wrongdoing in question, the victim was a victim of a violation of article 8 of the Convention.*"[88]

Even though this case is not directly about children´s online privacy, this ruling shows that the Court makes a concrete assessment of the given case and lays much emphasis on how fundamental the values at stake are. The extent to which these values should be safeguarded in other ways is also emphasized by the Court.

More than 20 years after this ruling, the Court expressed a positive obligation for states to protect children´s **online privacy** in the 2008 case of *K.U v. Finland*[89]. In this case, an advertisement of a sexual nature was made using the name of a 12-year-old boy, without his knowledge. The advertisement was linked to the boy's own website and stated that he wanted intimate contact with boys of the same age group or older. The boy's father contacted the police but Finnish legislation in place at the time, prohibited Internet Service Providers (ISPs) from disclosing user identity. The police and the courts could therefore not require the ISP to

[86] Ibid para 18.

[87] Ibid para 27 and 30

[88] ibid

[89] K.U. v. Finland, no. 2872/02, 2nd December 2008

identify the person who had posted the advertisement. The applicant relying on Article 8 of the ECHR claimed that his right to respect for private life under the ECHR had been violated and that the state of Finland had failed to provide him with an effective remedy pursuant to article 13 ECHR.

The ECtHR unanimously held that the boy's right to privacy according to the EHRC had been violated. The Court reiterated that:

"*although the object of Article 8 is essentially to protect the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life.... These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves. There are different ways of ensuring respect for private life and the nature of the State's obligation will depend on the particular aspect of private life that is at issue*.[90]

The Court further emphasised that *"children and other vulnerable individuals must be entitled to State protection, in the form of effective deterrence, from such grave types of interference with essential aspects of their private lives"*, and that that *"both the public interest and the protection of the interests of victims of crimes committed against their physical or psychological well-being require the availability of a remedy enabling the actual offender to be identified and brought to justice."*[91]

Several notions that are relevant for our topic can be inferred from this ruling. First, it indicates that article 8 ECHR does not only seek to protect citizens against government interference, but also seeks to protect citizen´s privacy from violation by other citizens. Also, the ruling imposes positive obligations upon the State to ensure that the rights citizens have to respect for their private life is effectively guaranteed, especially through legislation.

One way of ensuring this is through criminal sanctions. In the case of *M.C. v. Bulgaria*[92] the court stated that

[90] Ibid para 42 and 43

[91] Ibid para 46 and 47

[92] M.C. v. Bulgaria, no. 39272/98 4th December 2003.

"positive obligations on the State are inherent in the right to effective respect for private life under article 8; these obligations may involve the adoption of measures even in the sphere of the relations of individuals between themselves."[93]

This case indicates that States may also be obliged to establish efficient criminal law provisions against violations where essential aspects of private life are at stake.

Even though in the above-mentioned cases the violation of the child´s privacy was committed by someone other than the child´s own parents, it is noteworthy how the Court emphasizes on children´s special need for protection of their private lives because of the potential threat to their physical and mental welfare and their vulnerability. Accordingly, the ECtHR has established strong protection to children´s online privacy in its case law. While stressing upon the vulnerability of children, particularly young children, in the digital environment, the ECtHR has prescribed a positive duty, implicit in article 8 ECHR, upon States to enact laws to protect minors from serious violations of their private lives. Moreover, as Groothius rightly observes, "it follows from the case law of the Court that the Member States to the ECHR are under an obligation to permanently update and amend their national legislation in order to protect children and other vulnerable individuals against forms of abuse enabled by the newest technology and social development"[94]

The final question here is whether article 8 also protects children when the violation of the rights is carried out by the parents. In *E.S. and Others v. Slovakia*[95]the Court held that Slovakia had failed to provide the first applicant and her children with the immediate protection required against her husband's violence, in violation of article 3 (prohibition of inhuman or degrading treatment) and article 8 (right to private and family life) of the Convention. This is just one of many similar cases. Based on this it is safe to conclude that art 8 holds no exception from parents´ privacy infringements.

[93] Ibid para 150.

[94] Groothius (2014) p. 155

95 no. 8227/04

It follows from this that Norway has an obligation to enact legislation that will ensure adequate protection of children from violation by others, including their own parents.

4.3 The Balance of the Right to Privacy and the Right to Freedom of Expression

It is important to remember in these discussions about parent´s exposure of sensitive information about their children´s child welfare cases online, that we are talking about digital technology and the Internet, which are technologies and platforms that facilitate free speech and free expression.[96] One can therefore argue that having regulation that prevents parents from sharing such cases online would limit the parents´ rights to free speech and expression, which is enshrined in article 10 of the European Human Rights Convention. In this section, I review the case law of the ECtHR regarding issues pertaining to the intersection of the right to privacy and the right to free speech. The goal is to find out whether having a legal provision that prohibits parents from sharing sensitive information about their child welfare cases on social media platforms can be said to be in violation of article 10 ECHR. If this question is answered in the affirmative, it would mean that the GDPR is right in not allowing States to have a legal provision that gives the DPA the mandate to take down sensitive information shared by parents about their children online. A negative answer on the other hand will mean that such a provision should be allowed in national legislation.

In the above-discussed case of *K.U v. Finland*, the Court noted that *"although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others."*[97]

From this statement, it can be inferred that in some cases, the right to respect for one´s private life trumps the rights that others have to freedom of speech and expression.

[96] Thierer (2014) p. 51.

[97] KU v. Finland para 49

In balancing the right to freedom of expression against the right to respect for private life a review of the case law of the European Court of Human Rights shows that the Court has developed at least 5 criteria that are relevant.[98] These are criteria which were laid out by the courts in the 2012 cases of *Von Hannover v. Germany*[99] and *Axel Springer AG v. Germany*[100] are:

1) How well known is the person concerned and what the subject of the information is
2) The conduct of the person concerned prior to publication of the information or the fact that the information has already appeared in an earlier publication
3) The content, form and consequences of the publication, also taking into account the extent to which the information has been circulated.
4) The verity of the information and the way in which the information was acquired
5) Whether the published information contributes to a debate of general interest.

In the 2012 case of *Krone Verlag GmBH & Co KG and Krone Multimedia GmBH & Co KG v. Austria* (2012)[101] news articles about a 10 year old girl who had been sexually abused by her biological father and step mother were published by two national newspapers, Krone Verlag and Krone Multimedia. The identity of the girl was revealed in the published articles, and one of the newspapers[102] had in addition, published the articles also online and included photographs of her. The Austrian courts found that the articles published by the newspapers constituted an intrusion into the strictly private life of the victim, a minor, and awarded the victim compensation of a total of 20 000 euros from both newspapers. The newspapers, relying on article 10 (freedom of expression) of the ECHR filed a complaint with the ECtHR claiming that the interference with their right to impart information had not been necessary in a democratic society as there had been an overriding public interest in reporting in every detail on the case in issue.

[98] Von Hannover v. Germany (no.2) and Axel Springer v. Germany

[99] Von Hannover v. Germany no. 2, nos. 40660/08 and 60641/08

[100] Axel Springer AG v. Germany, no. 39954/08, 7th February 2012

[101] Krone Verlag GmBH & Co KG and Krone Multimedia GmBH & Co KG v. Austria (2012), no. 33497/07, 17th January 2012. See also: Kurier Zeitungsverlag und Duckereri GmBH v. Austria, no. 3401/07, 17th January 2012.

[102] Ibid para 41.

The ECtHR agreed with the Austrian courts and considered that the interference with the applicant companies' right to impart information was proportionate. The court took into account *"the particularly wide circulation of the applicant companies media"*. (Criteria 3 mentioned in the 2012 cases of *Von Hannover v. Germany* and *Axel Springer AG v. Germany).* The Court considered further that

"the articles at issue dealt with a matter of public concern, a crime involving violence against a child and sexual abuse committed within the family and could well give rise to a public debate on how the commission of similar crimes could be prevented." (Criteria 5) "However, given that neither the offenders nor the victim were public figures or had previously entered the public sphere," (criteria 1) "it cannot be said that the knowledge of the identity of these persons was material for understanding the particulars of the case". Hence the Court noted that *"the applicant companies were not prevented from reporting on all the details concerning the case of the victim, only from revealing her identity and publishing a picture of her from which she could be recognised".*[103]

The newspapers´ right to freedom of expression under article 10 ECHR could not prevail over the child´s right to respect for privacy under article 8 ECHR. The Court´s ruling in this case shows that in some cases it takes into account the internet´s ability to create a substantial impact due to its high accessibility and worldwide reach (criteria 3). Also, for the purpose of this paper, it indicates that one can criticize the child welfare system without necessarily publishing the entire child welfare case online, and revealing the identity of the child and the details of the case.

In the 2005 case of *Perrin v. United Kingdom*[104], a man who had published obscene articles on an internet website was convicted and sentenced to 30 months in prison under the United Kingdom´s Obscene Publications Act. He complained under article 10 of the ECHR, arguing that the conviction and sentencing constituted interferences with his right to freedom of expression, which were not prescribed by law and/or were not necessary in a democratic society.

[103] Ibid para 57

[104] Perrin v. United Kingdom no. 5446/03. 18th October 2005

In its judgement, the court noted that
"the web page in respect of which the applicant was convicted was freely available to anyone surfing the internet and that, in any event, the material was, the very type of material which might be sought out by young persons whom the national authorities were trying to protect". The Court further observed *"that it would have been possible for the applicant to have avoided the harm and, consequently, the conviction, while still carrying on his business, by ensuring that none of the photographs were available on the free preview page (where there were no age checks). He chose not to do so, no doubt because he hoped to attract more customers by leaving the photographs on the free preview page".* The Court concluded that *"the applicant's criminal conviction could be regarded as necessary in a democratic society in the interests of the protection of morals and rights of others".*

This ruling indicates that if exposing children to obscene content (that has nothing to do with them) warrants lawful interference from the State, and one cannot enjoy the protection of article 10 ECHR in such contexts. Also, it shows that the court takes into account the level of accessibility of the web page on which the information is published. This implies that if parents make available child welfare cases on platforms that is easily accessible by everyone, and do not make any attempt at anonymizing the case, they cannot invoke article 10 ECHR.

The cases discussed above indicate that the court is aware of the different traits of the internet, such as the ability it has to create a major impact, because of to its worldwide reach. The Court therefore takes these traits into account when balancing the interest of protecting the privacy and personal integrity of minors against the interest of protecting freedom of speech and expression.

4.4 Conclusion

A review of case law emanating from the ECtHR shows that the court emphasizes on the vulnerability of children online and the positive obligation of the state to protect them. What I find quite remarkable though is that the court hardly refers to the UNCRC in its case law. I take this to be an indication that the court regards children´s right to privacy as enough reason to protect them, and that they do not need to resort to arguments about the best interest of the child in order to establish violation of the child´s privacy.

A very important aspect of the *K.U v. Finland* case is the question regarding from which moment in time the State authorities could be expected to enact legislation to protect children from paedophiles online. The Finnish government had argued that any legislative shortcoming on the side of the State to protect children such as the victim in the case, should be regarded in its social context at the time (which was the late nineties), when a rapid increase in the use and abuse of the cyberspace had just began. The Finnish government therefore argued that the legislature could not be expected to already have enacted legislation and policies to protect children online.

The Court rejecting this argument, referred to the then ongoing negotiations for the Convention on Cybercrime, which was already at an advanced stage back in 1999. The Court further considered that in the 1990s, the United Nations and the council of Europe had adopted many political declarations and resolutions on cybercrime. National authorities had therefore had enough opportunity to put in place a system to protect child victims from being exposed as targets for paedophilic approaches via the internet.[105]

Groothius[106] rightly observes that "this element in the reasoning of the court has a wider meaning than for the K.U. case by itself: it indicates that the member states to the ECHR are under an obligation to permanently amend and update their national legislation in order to protect children and other vulnerable individuals against forms of abuse enabled by the newest technological and social developments on the internet".

Consequently, the Norwegian State cannot blame its lack of effective legislation and mechanisms on the fact that the GDPR does not permit the establishment legal provisions that can secure the privacy rights of children from violation by their own parents. If the GDPR does not permit this to be established in the Personal Data Act, could such a provision be made in another legislation, such as the Child Welfare Act for instance? In any case, the State has a positive obligation to ensure that children´s rights to privacy is effectively protected. How the state intends to ensure this is up to the individual state, but the most important thing is that legal provisions have to be put in place.

[105] K.U v. Finland Para 48

[106] Groothius 2014 p. 148

5 Findings and suggestions

The purpose of this thesis has been to examine the extent to which the EU´s new General Data Protection Regulation (GDPR) provides adequate protection of the data privacy needs of children in the child welfare system against violation by their own parents. In order to achieve this goal, I aimed at answering the following questions:

1) What is the rule of law regarding children´s rights to protection of personal data from violation by their own parents, according to the current Norwegian Data Privacy Act?
2) What is the rule of law regarding children´s rights to protection of personal data from violation by their own parents, according to the GDPR?
3) Does the GDPR provide adequate protection of children´s right to data privacy from violation by their own parents?
4) If question 3 is answered in the negative can children rely on international conventions such as the UN Convention on the Rights of the Child and the European Convention on Human Rights for adequate protection of their right to online privacy?

In this chapter, I give a summary of my findings as I tried to answer the above-listed questions. The chapter is divided into two parts. In the first part, I present summaries of the findings of my research. In the second part, I propose measures through which the Norwegian government can despite this unfortunate development in light of the GDPR, can ensure an effective protection of children´s right to respect for their online privacy.

5.1 Findings of my research

In my attempt to answer the above-listed questions, I first looked at the historical development of the legislation regarding children´s rights to data privacy in Norway (in chapter 3). It was found that up until August 2012, there was no specific mention of the treatment of children´s personal data in the Norwegian Personal Data Act. However, after criticisms from experts on children´s rights and data privacy experts, and the UN Committee on the Rights of the Child, an amendment was made to the Personal Data Act, which states that *"personal data relating to children shall not be processed in a manner that is indefensible in respect of the best interests of the child"*, c.f section 11 paragraph 3 of the Act. Even though the assumption before this legislation was that children and adults have equal rights to respect and protection of their data privacy, with the introduction of this provision,

Norwegian legislators made it abundantly clear that children are a vulnerable group that needs special protection. Furthermore, this provision serves as a legal basis for the Norwegian DPA to delete inappropriate information published by anyone, be it a parent or an outsider, about a child. In other words, this provision guarantees that children´s online privacy rights are effectively protected, and in case of violation, it guarantees that the information be deleted and (probably) forgotten. This is a provision which is sorely needed with regard to the fact that many parents publish information about their child welfare cases online with no attempt at anonymizing the case.

After examining the historical development of the legislation, I critically examined the EU´s GDPR´s provisions on children´s right to privacy. My observation is, as rightly pointed out by the Norwegian Ministry of Justice in its draft consultation on implementation of the GDPR, that the GDPR does not permit States to establish national laws regarding the processing of children's personal data, with a general scope of activity. Put differently, Norway cannot maintain section 11 paragraph 3 of the current Personal Data Act as part of its implementation of the GDPR. The conclusion I draw from this development is that when the GDPR starts applying from 25th May 2018, the state of the law on children´s rights to privacy in Norway will return to the way it was before section 11 paragraph 3 of the Personal Data Act was introduced. This means that there will be no remedies for children whose privacy is violated by their own parents online. The GDPR thus restricts the protection of children's interests in the area I have discussed.

It is commendable though that the GDPR strengthens children´s rights to privacy in relation to the processing of their personal data by commercial actors. However, this does not change the fact that children still need better protection against parents who make choices on social media that may conflict with the best interests of the child. Furthermore, the increased digitalization in schools, child-upbringing arenas and other services requires society to work even systematically to ensure children's privacy and children's rights in digital arenas.

In light of the conclusion in chapter 3, I had to examine whether international sources of law can be relied upon to ensure effective protection of children´s privacy against violations by their own parents.

One cannot have a discussion on children´s right to data privacy without discussing the UN Convention on the Rights of the Child and the European Human Rights Convention. These are conventions that have been signed, ratified and incorporated into Norwegian law. Therefore, in chapter 4, I examined the extent to which children can rely on the provisions in these conventions for effective protection of their privacy from violation by others, including their parents. I found out that both of these conventions prescribe an positive obligation on the states to ensure that children and other vulnerable individuals in particular are guaranteed effective protection. It is therefore a sad development that the GDPR is putting such an unnecessary hindrance in the way of the individual State, thereby practically preventing children from getting the effective protection they deserve. This raises questions about how children's human rights can be safeguarded. In the next and last chapter, I will give some suggestions.

5.2 Suggestions for Effective Protection of the Online Privacy Rights of Children in the Child Welfare System after Implementation of the GDPR

Parents may think that sharing their children´s child welfare cases online is in the best interest of the child in a particular case, especially if they believe that the state has wrongfully taken custody of the child. Nevertheless, this information is of such private and sensitive nature that in my opinion, it is only the child himself/herself who should be entitled to consent to publication. However, the child will only be able to do so when he/she is matured enough to assess the question in the short and long term. I believe that child welfare cases are of such a personal nature that no one other than the child concerned should be able to allow online disclosure. Therefore, if a child does not have the degree of maturity needed to make an informed decision to consent to publication, then publication should not be allowed.

It can be argued that some parents share information about their child welfare cases as part of the endeavours to protect their family, when they are being investigated by the child welfare services or when they are fighting for custody of the child. However, parents' rights to the protection of family life must not be at the expense of the child's privacy and the state must have legal authority to intervene if the parents have disclosed information about the child in violation of the child's privacy. In my opinion, the best place to have specific rules regarding children´s right to privacy protection from abuse by their own parents or legal guardians

should be enshrined in the future Personal Data Act, which will be based on the GDPR. This raises the question of whether GDPR allows Norway to introduce such rules.

In its reply to the Ministry of Justice´s consultation paper, the Norwegian DPA recommended that the Norwegian government should assess whether the provision in section 11 paragraph 3 of the current Personal Data Act can be maintained in another form, for instance, as a specific restriction on the processing of sensitive personal data pursuant to Article 9, paragraph 4 of the GDPR[107]. Though this may seem like a good suggestion for lack of better options, it is noteworthy that article 9 paragraph 4 only allows member states to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. This means that apart from genetic, biometric and health data, other forms of data cannot be included, should the Ministry of Justice opt for this solution. This further implies that inappropriate photos of children and any other kinds of inappropriate information about children, such as detailed information about their child welfare case cannot be protected under this "solution."

The Norwegian DPA further remarks that the Article 29 Working Party has pointed out that "the principle of the best interest of the child may be classified as a public interest as well"[108] in accordance with article 7 (e) of the current Data Privacy Directive. The DPA therefore assumes that the same applies to Article 6 (1) (e) of the GDPR, which states that processing shall be lawful only if and to the extent that processing is necessary for carrying out a number of tasks including "the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller." Based on this, the DPA believes that therefore is a leeway for the State to maintain section 11 paragraph 3 of the current Personal Data Act in one way or the other. Just like the first suggestion provided by the DPA, I do not believe that the provision in Article 6 (1) (e) of the GDPR can ensure an effective protection of the data privacy rights of children in the Norwegian child welfare system from abuse by their own parents.

[107] The Norwegian DPA´s consultation response. Available at: https://www.regjeringen.no/no/dokumenter/horing-om-utkast-til-ny-personopplysningslov--gjennomforing-av-personvernforordningen-i-norsk-rett/id2564300/?uid=84c953f2-30a4-44ce-a03e-f5a0afbed298. Accessed 18.11.2017.

[108] WP 160 p. 9

Whether or not these suggestions by the Norwegian DPA are viable options will nevertheless be up to Norwegian legislators to decide, but I believe it is important that the Norwegian government in the future works on various measures to ensure children's right to online privacy. I particularly call for measures that provide better protection for children from harmful exposure online by their own parents.

As noted by the ECtHR, the positive obligations on the State are inherent in the right to effective respect for private life under Article 8. These obligations may involve the adoption of measures even in the sphere of the relations of individuals between themselves. While the choice of the means to secure compliance with Article 8 in the sphere of protection against acts of individuals is in principle within the states margin of appreciation, effective deterrents against actions where fundamental values and essential aspects of private life are at stake, requires efficient criminal-law provisions.[109]

Article 84 of the GDPR leaves it to national law to determine the penal provisions for breach of the Regulation, and article 83 allows the Data Privacy Authorities to impose fines for breach of the substantive provisions of the Regulation. These fines are significantly high. Because of this, in the draft proposal for a new data privacy regulation, the Norwegian Ministry of Justice proposes that violations of the future Data Privacy Act should no longer be punishable under the criminal code. The Ministry also assesses whether the DPA should be given access to administrative confiscation. The ministry believes that such a regime will have the necessary deterrent effect and that a threat of criminal sanctions will not have any further general or individual preventive effect.[110]

I support this suggestion with regard to parents who violate their own children´s privacy online and I hope it will be implemented in such a way that children can have effective remedies to protect their privacy in light of this. I believe that except in very serious cases, punishing parents for disclosure of such information may be a poor solution, for many good reasons. This is especially because of the family bond that exists between children and parents. This is why it is important to focus on information work, supplemented with adequate and easy access to delete information that is in violation of children's privacy. If the parents

[109] Ibid para 150

[110] Høring om utkast til ny personopplysningslov (2016) p. 99

have disclosed information contrary to the best interests of the child, the Data Privacy Authorities must have the competence to undertake deletion on its own initiative. This should, in my opinion be clarified before the GDPR starts applying from 25th May 2018.

Whether the European Commission's failure to address this issue in the GDPR was intentional or by oversight, I believe that special rules would be desirable given the digital age we live in and the fact that children are amongst the most vulnerable groups of people in society. The GDPR´s unclear stance is unfortunate in such an important area because it does not provide a satisfactory representation of the kind of protection children need. Any future rules must on children´s right to privacy must be based on the rules of the Children´s Convention, especially Article 16, and take into account the child's increasing right to self-determination, which has been expressed several places in Norwegian and international law.

I will keep monitoring how the Norwegian authorities safeguard children's right to protection in situations where parental consent or choice clearly contrary to the child's obvious interests and the fundamental interests of the child.

6 REFERENCES

6.1 Norwegian Sources of Law

Kongeriket Norges Grunnlov av 17. Mai 1814 (Grunnloven)

Lov om barn og foreldre av 8. april 1981 nr.7 (Barneloven)

Lov om barneverntjenester av 17. Juli 2002 nr. 100 (Barnevernloven)

Lov om behandling av personopplysninger av 14. April 2000 (personopplysningsloven)

Lov om rett til innsyn i dokument i offentleg verksemd av 19. Mai 2006 nr. 16 (offentleg-lova)

Lov om Straff av 20. Mai 2005 (Straffeloven)

Lov om styrking av menneskerettighetenes stiling i Norsk rett av 21.05.1999 (menneskerettsloven)

Lov om vergemål for umyndige av 26. mars 2010 (vergemålsloven)

Prop. 47 L (2011–2012) Endringer i personopplysningsloven. Høring om utkast til ny person-opplysningslov-gjennomføring av personvernforordningen i norsk rett. Available at https://www.regjeringen.no/contentassets/c907cd2776264a6486b8dd3ee00a4e3d/horingsnotat--ny-personopplysningslov--gjennomforing-av-personvernforordningen-i-norsk-rett.pdf

Rundskriv Q-24, mars 2005 *Barnevernet og taushetsplikten, opplysningsretten og opplysningsplikten* https://www.regjeringen.no/globalassets/upload/kilde/bfd/rus/2005/0002/ddd/pdfv/243383-q-24_rundskriv_taushetsplikt.pdf. Accessed 03.11.2017

6.2 International Sources of Law and Related Documents

European Convention on Human Rights

United Nations Convention on Economic, Social and Cultural Rights

United Nations Convention on the Rights of the Child

United Nations on Civil and Political Rights

Universal Declaration of Human Rights

Regulation (Eu) 2016/679 Of The European Parliament And Of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the

free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Article 29 Data Protection Working Party Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) Adopted on 11 February 2009 (WP 160). Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_en.pdf

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

About Committee on the Rights of the Child (CRC): http://www.ohchr.org/EN/HRBodies/CRC/Pages/CRCIndex.aspx. Accessed 03.11.2017

Committee On The Rights Of The Child. Forty-Ninth Session Consideration of Reports Submitted By States Parties Under Article 44 Of The Convention Concluding Observations: United Kingdom Of Great Britain And Northern Ireland. (CRC/C/GBR/CO/4 20 October 2008) Available at: http://www2.ohchr.org/english/bodies/crc/docs/AdvanceVersions/CRC.C.GBR.CO.4.pdf. Accessed 16.11.2017.

Consideration of reports submitted by States parties under article 44 of the Convention, Concluding observations: Norway. Available at: http://www2.ohchr.org/english/bodies/crc/docs/CRC.C.NOR.CO.4.pdf. Accessed: 31.10.2017.

Difference between directive and regulation: http://europa.eu/eu-law/decision-making/legal-acts/index_en.htm. Accessed 28.03.2016

Information about countries that have ratified the UNCRC: https://www.hrw.org/news/2014/11/17/25th-anniversary-convention-rights-child. Assesed 20.08.2017.

The Committee on the Rights of the Child: consideration of the third and fourth periodic report of the United Kingdom of Great Britain and Northern Ireland (CRC/C/GBR/CO/4) 20 October 2008. Pp. 8-9

UNCHR guidelines on determining the best interests of the child. Available at http://www.unhcr.org/4566b16b2.pdf.

6.3 Case law

Axel Springer AG v. Germany, Application no. 39954/08, 7th February 2012

Case of Bodil Lingqvist v. Sweden. Judgment of 6. 11. 2003 — Case C-101/01

Case of K.U. v. Finland (Application no. 2872/02)

Dudgeon v. United Kingdom, Application no. 7525/76, 22nd October 1981.

Gaskin v. United Kingdom, Application no. 10454/83, 7th July 1989.

Marper v. the UnitedKingdom, Application 30562/04, 14th December 2008 30562/04

Niemietz v. Germany, Application no. 13710, 16th December 1992.

Perrin v. United Kingdom. Application no. 5446/03. 18th October 2005

Reklos and Davourlis v. Greece. Application no. 1234/05. 15th January 2009

Slivenko et al v. Latvia, Application no. 48321/99, 9 October 2003.

Von Hannover v. Germany No. 1, Application no. 59320/00, 24 June 2004.

Von Hannover v. Germany no. 2, Application nos. 40660/08 and 60641/08, 7th February 2012

White v. Sweden, Application no. 42435/02, 19th September 2006

X and Y v. the Netherlands, Application no. 8978/80, 26th March 1985

E.S. and Others v. Slovakia, Application no. 8227/04

6.4 Literature

Allstrin, Nina Tøgersen, ”Barns rett til beskyttelse mot at foreldrene offentliggjør personlig informasjon om dem på sosiale medier-Er barn tilstrekkelig beskyttet?”, Tidsskrift for familerett, arverett og barnevernrettslige spørsmål 03 (2015) volume 13, pp 202-219

Available at: https://www.regjeringen.no/contentassets/daad3dbe61c74f5c9240d16478b088ba/rapport_g-390.pdf. Accessed 15.08.2017

Ciavarella, Rachel and **De Terwangne, *Cécile*** (2014) ”OnlineSocial Networks and Young People´s Privacy Protection: The Role of the Right to be Forgotten” In: *Minding Minors Wandering the Web: Regulating Online Child Safety,* Simone van der Hof, Bibi Van den Berg and Bart Schermer (eds.), vol. 24, The Hague, 2014 pp.157-171

Groothius M. Marga ”The Right to Privacy for Children on the Internet: New developments in the Case Law of the European Court of Human Rights” In: *Minding Minors Wandering the Web: Regulating Online Child Safety,* Simone van der Hof, Bibi Van den Berg and Bart Schermer (eds.), vol. 24, The Hague, 2014, pp. 143-156.

Harris D, **O´Boyle** M, **Bate** E, **Buckley** C (eds) (2009) Harris, O´Boyle & Warbrick: Law of the European Convention on Human Rights. 2nd edition. Oxford University Press, Oxford
Livingstone, Sonia and O´Neil Brian, ” Children´s Rights Online: Challenges , Dilemmas and Emerging Directions ” In: *Minding Minors Wandering the Web: Regulating Online Child Safety,* Simone van der Hof, Bibi Van den Berg and Bart Schermer (eds.), vol. 24, The Hague, 2014, pp. 19-38.

Schartum, Dag Wiese and **Bygrave** Lee A. *Utredning av behov for endringer I personopplysningsloven (2006)*

Schartum, Dag Wiese and **Bygrave** Lee A. *Utredning om fødselsnummer, fingeravtrykk og annen bruk av biometri i forbindelse med lov om behandling av personopplysninger § 12” (2008)* Available at: https://www.regjeringen.no/contentassets/daad3dbe61c74f5c9240d16478b088ba/g-0406.pdf. Accessed 15.08.2017

Smith, Lucy, ”Om barns personvern”, Tidsskrift for familerett, arverett og barnevernrettslige spørsmål 02 (2011) volume 9, pp 106-126

Thierer, Adam “ A framework for responding to online safety risks” In: *Minding Minors Wandering the Web: Regulating Online Child Safety,* Simone van der Hof, Bibi Van den Berg and Bart Schermer (eds.), vol. 24, The Hague, 2014, pp. 39-66

Tungendhat Michael QC, Sherborne David, and Barnes Jonathan, ”Data Protection and the Media” In: *The Law of Privacy and the Media,* Michael Tungendhat QC and Iain Christie (eds), Oxford 2002, pp. 153-191.

Van den Berg, Bibi ”Colouring Inside the Lines: Using Technology to Regulate Children´s Behaviour Online” In: *Minding Minors Wandering the Web: Regulating Online Child Safety,* Simone van der Hof, Bibi Van den Berg and Bart Schermer (eds.), vol. 24, The Hague, 2014, pp. 67-85.

Van der Hof, Simone., Van den Berg Bibi., and Schermer, Bart (eds.), *Minding Minors Wandering the Web: Regulating Online Child Safety,* vol. 24. The Hague, 2014

White RCA, **Ovey** C (2009) Jacobs, White and Ovey: the European Convention on Human Rights, Oxford University Press, Oxford.

6.5 Online sources

About the EEA Agreement: http://www.efta.int/eea/eea-agreement. Accessed 10.11.17.

http://www.sbs.com.au/news/dateline/story/norways-stolen-children. Accessed 26.07.16

https://www.youtube.com/watch?v=C-PzrwliUk4. Accessed 26.07.16

https://www.youtube.com/watch?v=owGTvlU9Nkw. Accessed 14.07.2016

List of consultative bodies that had comments to the consultative paper on implementation of the GDPR. Available at: https://www.regjeringen.no/no/dokumenter/horing-om-utkast-til-ny-personopplysningslov--gjennomforing-av-personvernforordningen-i-norsk-rett/id2564300/. Accessed 13.11.17.

The Norwegian DPA´s consultation response. Available at: https://www.regjeringen.no/no/dokumenter/horing-om-utkast-til-ny-personopplysningslov--gjennomforing-av-personvernforordningen-i-norsk-rett/id2564300/?uid=84c953f2-30a4-44ce-a03e-f5a0afbed298. Accessed 18.11.2017.

UNCHR guidelines on determining the best interests of the child. Available at http://www.unhcr.org/4566b16b2.pdf. Accessed 03.09.17.