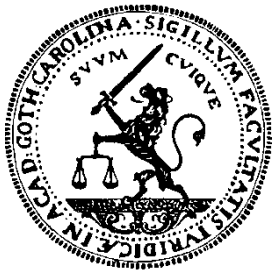

FACULTY OF LAW

LUND UNIVERSITY

Ida Markusson

Shielding kids and safeguarding secrets:

Examining the balance of children's right to protection and children's right to privacy

JURM02 Graduate thesis

Graduate thesis, Master of Laws program

30 higher education credits

Supervisor: Xavier Groussot

Semester: Spring 2023

Table of contents

Summary

This thesis starts from the premise that children's right to privacy is a part and parcel for children's right to participation online. Children's rights law inherently presents a dilemma relating to children's right to participation and protection, where a rights-based approached is considered the most effective way to address the dilemma. A rights-based approach is legal framework that can balance children's need for protection online with their capacity to maximize the opportunities and benefits from the digital sphere.

Firstly, this thesis provides an exposition of children's digital rights and their position in the digital sphere, aiming to provide an understanding of the landscape this thesis is going to navigate through. Children's rights and their translation into the digital environment by policies and legal doctrine are accounted for, as well as the EU's competence in relation to children.

Thereafter an examination of the EU legislator attempt to balance children's right to privacy and protection in the EU digital sphere is conducted. The analysis consists of reviewing secondary legislation in relation to a rights-based approach. This thesis concludes that when analyzing the balance between protecting privacy and protecting children, the latter is favored in legislative frameworks. The balance in the jurisprudence of the European Court of Justice and the European Court of Human Rights is also investigated. This thesis concludes that it is difficult to distinguish a balance, because of the best interest of the child principle is based on a case-by-case basis and there is insufficient case law concerning children's privacy in the digital sphere.

The controversies surrounding the European Commissions and the European Council proposal that directly affects both children's privacy and right to protection online are presented. In the last chapter, all the different examination is discussed together and the implication of the proposal on the balance are discussed.

Sammanfattning

Denna uppsats utgår från premissen att barns rätt till integritet är en del av barns rätt till deltagande online. Barnrättslagstiftning presenterar i sig ett dilemma som rör barns rätt till delaktighet och skydd, där en rättighetsbaserad strategi anses vara det mest effektiva sättet att ta itu med dilemmat. En rättighetsbaserad strategi förespråkar en balans mellan barns behov av skydd online och barns förmåga att maximera möjligheterna och fördelarna med den digitala sfären.

För det första ger uppsats en beskrivning av barns digitala rättigheter och deras position i den digitala sfären, i syfte att ge en förståelse för det landskap som uppsatsen kommer att navigera genom. Barns rättigheter och hur de översätts till den digitala miljön genom policyer och juridiska doktriner kommer redovisas, liksom EU:s kompetens i förhållande till barn.

Därefter genomförs en granskning av EU:s lagstiftares försök att balansera barns rätt till integritet och skydd i EU:s digitala sfär. Analysen består av att se över sekundärlagstiftningen i förhållande till ett rättighetsbaserat synsätt. Denna uppsats drar slutsatsen att det finns en övervikt av skyddsskäl i lagstiftningen, som ger uttryck för ett skyddande förhållningssätt. Avvägningen i EU-domstolens och Europadomstolens rättspraxis utreds också. Avhandlingen drar slutsatsen att det är svårt att urskilja en balans, eftersom principen om barnets bästa kommer uttryck i det specifika fallet och att det finns otillräcklig rättspraxis om barns integritet i den digitala sfären för att kunna dra några slutsatser.

Uppsatsen behandlar även kontroverserna kring EU-kommissionen och Europeiska rådets förslag som direkt påverkar både barns integritet och rätt till skydd online presenteras. I det sista kapitlet diskuteras alla olika delarna tillsammans och förslagets betydelse för balansen diskuteras.

Preface

Efter fem år i Lund är det nu dags för mig att sätta punkt på juristprogrammet och att ta mig an nya utmaningar. Det känns både spännande och vemodigt på samma gång. Tiden i Lund har gett mig vänner för livet och varit bland de mest minnesvärda åren jag upplevt. Jag vill tacka några av de personer som har gjort resan genom juristprogrammet särskilt speciell.

Först och främst vill jag tacka min handledare Xavier för värdefull handledning, peppning och flexibilitet. Ditt stöd har betytt mycket.

Tack till alla mina fina kollegor jag har haft möjlighet att få lära känna som studentmedarbetare på Juridiska Fakulteten. Repan och Nätis, min studietid hade inte varit lika rolig utan er. Tack för alla fredagsfikor, fester och skratt. Bland alla mina fantastiska kollegor vill jag vill rikta ett särskilt tack till Lärarlyftet. Ni är de bästa kollegorna man kan ha och jag kommer sakna er så mycket!

Tack till min familj. För all kärlek, hejarop och stöttning i allt jag åtar mig. Ni är mina största fans och min stora trygghet.

Tack till alla mina fina vänner som funnits där i både med- och motgångar. Jag ser fram emot att få fortsätta dela mitt liv med i framtiden också. Ni är underbara!

Lund i maj 2023,

Ida Markusson

Abbreviations

AFSJ	Area of Freedom, Security and Justice
CFR	European Union Charter of Fundamental Rights
CDSM	Copyright on the Digital Single Market Directive
CJEU	Court of Justice of the European Union
CSAM	Child sexual abuse material
CoE	Council of Europe
DSA	Digital Services Act
EU	European Union
EU Centre	EU Centre on Child Sexual Abuse
ECHR	European Convention on Human Rights
ECtHR	The European Court of Human rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
Interim Regulation	Regulation 2021/1232
LEA	Law enforcement authorities
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
UNCRC	Convention on the Rights of the Child

1 Introduction

1.1 Background

Over the last 30 years, constant technological innovation has placed communications and sociality onto new foundations. The transnational digital environment offers opportunities for children, but simultaneously presents various risks towards children. On the one hand, the digital spaces give children a place where they can effectively exercise their right to participate as an independent actor with their own agency. On the other hand, children are exposed to many risks and need protection in the digital environment.[1]

Because both children's opportunities online and risk associated with the online environment has increased, the full range of children's rights is affected and consequently becomes a natural part of the discourse on children's participation rights online. Materialising children's right in the digital environment is therefore acknowledged to be an essential part of the realisation of children's rights in general. A growing need is echoed to promote opportunities for children while simultaneously preventing children from risk presented in a digital environment.[2]

During the recent years, The European Union has increased momentum for legislative processes and strategies concerning children's digital presence.[3] For instance, by adopting the EU strategy on 'Better Internet for the Kids (BIK+)' which the EU proposal on prevent and combat child sexual abuse originates from.[4] The aim with the proposal is to protect children from the increasingly online child sexual abuse.[5]

The proposed regulation, known in the public debate as the *'Chat control regulation'*, has caused quite a stir in the European Union (EU).[6] On one hand, the draft regulation has been embraced by child rights organisations,

[1] Katharina Kaesling, 'Children's Digital Rights: Realizing the Potential of the CRC' in Ellen Marrus and Pamela Laufer-Ukeles (eds.) *Global Reflections on Children's Rights and the Law: 30 years after the Convention on the Rights of the Child* (1st edn Routledge 2021) 184.

[2] Muhammad Nawaila, Sezer Kanbul and Fezile Ozdamli,'A review on the Rights of Children in the Digital Age' (2018) 94 Children and Youth Services Review 390.

[3] Michael O'Flaherty and Snežana Samardžić-Marković**, '**Handbook on European law relating to the rights of the child' (Publication Office of the European Union 2022) 21.

[4] Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down rules to Prevent and Combat Child Sexual Abuse' COM (2022) 209 final, explanatory memorandum.

[5] COM (2022) 209 final, Recitals (4-5).

[6] For example, see Daniel Boffey, 'EU lawyers say plan to scan private messages for child abuse may be unlawful',*The Guardian* (8 May 2023) < https://www.theguardian.com/world/2023/may/08/eu-lawyers-plan-to-scan-private-messages-child-abuse-may-be-unlawful-chat-controls-regulation> Accessed 18 May 2023.

which have emphasised the need to protect children from sexual abuse online. For instance, over 90 child protection associations sent an open letter to the EU Commission supporting the draft regulation.[7]

On the other hand, industry associations and data protection supervisory authorities such as the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) which are independent privacy watchdogs in the EU), have released a joint opinion which criticises the proposal for being intrusive on privacy.[8] Some critics even argue that the proposal violates the right to privacy online which ultimately enables state parties to conduct mass surveillance.[9]

At the time of writing, the balance regarding the fundamental right to privacy (age generic) and children's right to protection from child sexual abuse is still controversial, and the proposal has still not been adopted. Whilst most of the criticism relates to individuals' privacy a such, I found it interesting to put the balance regarding children's right to privacy and protection under scrutiny and by that put legislative measures concerning children to a higher extent into the debate.

1.2 Purpose and research questions

The purpose of this thesis is therefore to examine the implications of the proposed EU regulation aimed at preventing and combatting child sexual abuse online on the balance between children's right to privacy and their right to protection online. To achieve this aim, this essay will firstly analyse the current state of this balance by reviewing existing policies, legal frameworks, and case law. Secondly, the proposed regulation is going to be analysed and an assessment of the potential consequences on children's privacy rights and protection rights is conducted. Conclusively, this essay will focus on the following research questions:

- What is the current state of balance between children's fundamental right to privacy and right to protection from sexual exploitation in EU digital spheres?

[7] Torn,'Open Letter: Thorn and 90+ Organizations Welcome the EU's Proposal to Prevent and Combat child Sexual Abuse' (31 May 2022) < https://www.thorn.org/blog/open-letter-thorn-and-50-organizations-welcome-the-eus-proposal-to-prevent-and-combat-child-sexual-abuse/> Accessed 18 may 2023.

[8] The European Data Protection Board and The European Data Protection Supervisor, 'Joint Opinion 04/2022 on the Proposal of the European Parliament and of the Council Laying down rules to prevent and combat child sexual abuse' (2022).

[9] James Vincet, 'New EU rules would require chat apps to scan private messages for child abuse: The proposal has been called unworkable and invasive by privacy experts' *The Verge* (11 May 2022) < https://www.theverge.com/2022/5/11/23066683/eu-child-abuse-grooming-scanning-messaging-apps-break-encryption-fears > Accessed 18 May 2023.

- How (to what extent) does the EU proposal to combat child sexual abuse online impact the balance between children's fundamental right to privacy and right to protection online in transnational digital spheres?

1.3 Methodology and material

1.3.1 Methodology

To fulfil the purpose in this thesis, legal sources (or elements in the legal norm hierarchy) are processed with the aim of systematizing and interpreting the existing law. The method applied can therefore be described as legal dogmatic. The main task of a legal dogmatic analysis can be understood as a reconstruction of legal principles and rules in a system, where the result of such procedure reflects the content of the applicable law and how it must be understood in a certain context (*de lege lata*). However, the legal dogmatic method is also considered to allow a critical analysis of the legal situation, which appears throughout the thesis and in the discussion.[10]

The legal dogmatic method used in this thesis is influenced by the legal methodology and interpretation methods used by the Court of Justice of the European Union (CJEU).[11] The most imperative task of the CJEU is to create a basis for a common interpretation of EU law within the entire Union.[12] Although the CJEU have different ways to interpretate union law, this thesis is going to use the method that the court practises the most, namely a teleological approach which is associated with the *modus operandi* of the CJEU.[13]

This approach is described as a free and strongly purpose-oriented method, where provisions are interpreted against contextual elements such as its purpose and background. Therefore, great emphasis is placed on the purpose of the legislation.[14] The teleological approach is based on interpretating the concrete legal rules based on its intended goal, while also considering the overarching goals set for the entire Union which are expressed through primary

[10] Jan Kleineman, 'legal dogmatic method' in Maria Nääv and others (eds.) *Legal methodology* (2nd edn Studentlitteratur AB 2018) 35.

[11] Jörgen Hettne and Ida Otken Eriksson, '*EU legal methodology: Theory and impact on Swedish law enforcement*' (2nd edn Norstedts Juridik 2011) 168.

[12] Consolidated version of the Treaty on European Union [2016] OJ C 202/1 (TEU), Article 19.

[13] A few examples of other methods that the CJEU uses is for instance linguistic interpretation (focusing exclusively on the wording of the provisions), multilingual interpretation and autonomous interpretation, see Hettne and Otken Eriksson (n 10) 159.

[14] Hettne and Otken Eriksson (n 10) 168.

law (the treaties).[15] Additionally, the interpretation must also be made based on the context in which the rules exist.[16]

The purpose-oriented method is explained by the fact that EU's ability to act is bound by the competences the Member states have conferred to the Union by the treaties and the objectives set out therein. The treaties are usually described as framework treaties because they lack any trajectory of how the objectives should be achieved. In practise, the teleological approach has a subsidiary meaning and is often used when a provision is unclear, or the contextual elements are vague. This approach is frequently used because secondary legislation is often vague and unclear, resulting from the legislation process often is based on compromises from Member states.[17] <wording<?

The jurisprudence from the CJEU and general legal principles have a high normative value as a legal source in EU Law. The case law may constitute the predominantly applicable law in certain areas in the EU legal order. The case law is further also an important interpretive tool for the CJEU when interpretating EU law.The CJEU have had a great impact on the legal development concerning fundamental rights and the interpretation. At the same time, the CJEU have been widely criticized for 'judicial activism' when using general legal principles in relation to fundamental rights.[18] For example, criticism arose following certain judgements related to the domain of private life and data protection, which hold significant relevance in this thesis.[19]

General legal principles can be described as the 'spinal cord' of EU and are characterised by having an open and purpose-oriented character. The use and great importance of the principles are explained by the incomplete nature of EU law and the treaties character as 'framework'. The general principles have three functions: to fill out gaps in EU legal order, interpretate secondary law in a way that is in accordance with the principles, and to serve as a yardstick to test the validity of secondary law.[20] The CJEU considers the general rules as an expression of fundamental principles that can explain the content and place of the rules in the larger system. Consequently, the most important thing is not the wording of the provision, but the purpose in a wider context, i.e., general legal principles have a great importance.[21] General principles are described to complement the primary EU law.[22]

---

[15] Treaty on the Functioning of the European Union [2016] The Treaty on the Functioning of the European Union OJ 202/01 (TFEU) and TEU.

[16] Jane Reichel 'EU-legal dogmatic method' in Maria Nääv and others (eds.) *Legal methodology* (2nd edn Studentlitteratur AB 2018) 122.

[17] Ibid 122.

[18] Reichel (n 16) 125; Hettne and Otken Eriksson (n 10) 60.

[19] Reichel (n 16) 125.

[20] Reichel (n 16)125; Hettne and Otken Eriksson (n 10) 168.

[21]Hettne and Otken Eriksson (n 10) 62.

[22] Ibid 73.

This thesis concern children's fundamental rights, which makes it imperative to sort out the legal currency at EU level. Fundamental rights were firstly an aspect of the general principles of EU law: written and unwritten principles drawn from common constitutional traditions of Members states.[23] The CJEU has also established that international human rights treaties and conventions to which the Member states are signatories are likewise part of the fundamental rights landscape and, by implication, the EU general principles framework.[24] Today, fundamental human rights as general principles have also been set out in constitutional stone, for instance in the TEU. In the TEU, it is stated that the Charter of Fundamental Rights of the European Union (codification of CJEU's case law) have the same legal values as the treaties.[25] Furthermore, Article 6(3) TEU states that fundamental rights, as guaranteed by the European Convention on Human Rights (ECHR) and also as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law'.[26]

Three principle human rights instruments form the foundation of EU's children's rights: United Nations Convention on the Rights of the Child (UNCRC), ECHR and CFR.[27] According to Article 52(3) CFR, the rights in the CFR corresponds to the rights guaranteed by the ECHR and that the meaning and scope of those right are the same as those laid down by the ECHR. Moreover, it also states that Union law is not prevented from providing more extensive protection i.e., the ECHR lays down the minimum threshold for human rights in the CFR. The level of protection is determined in Article 53 CFR: no provision in CFR may be interpretated as restricting or infringing on fundamental rights recognised within the respective jurisdictions in Union law, international law and the international conventions to which the Union or all Member states are parties. Children are bearers of the same rights as adults, they are entitled the same rights as adult.[28]

This thesis also relies on an analysis of recitals in order to examine the efforts made by the EU legislator to strike a balance in safeguarding children's rights within the digital environment. Consequently, the normative value of recitals must be discussed. Both EU directives and EU regulations begins with a preamble, which are divided into considerations and reasons. The introductory text contains several reasons why the legal act was produced. These are not legally binding but have a significant value regarding how the subsequent articles are to be interpretated. This requires a connection between the article to be interpretated and the reasons in questions. The aim is subsequently to

[23] Helen Stalford, *Children and the European Union: rights, welfare and accountability*, (Hart publishing 2012) 30.

[24] Ibid 19.

[25] Charter of Fundamental Rights of the European Union [2016] OJ C 202/1 (CFR); 6.1 TEU.

[26] European Convention on Human Rights [1950].

[27] United Nations Convention on the Rights of the Child [1989].

[28] Stalford (n 23) 19.

analyse to what extent of a rights-based approach was considered by the EU legislator.[29]

1.3.2 Material

The material has been selected with consideration to the method, as well as the suitability of the material to achieve the purpose of this essay. For instance, this thesis accounts for several rulings from the CJEU and the ECtHR. A comprehensive search for relevant case law was conducted in the CJEU's database CURIA and in the ECtHR database HUDOC, utilizing various search terms such as 'privacy', 'children fundamental rights', 'protection' and 'best interest of the child'. The search was conducted between 23rd of February 2023 to 10th of May 2023 with no precise results. Therefore, a significant challenge in this regard was the absence of case law concerning children's rights in the digital sphere. The rulings are selected by relevance to the purpose of this thesis and are based on cases have been discussed in the legal doctrine that relates to children digital rights.

Another significant challenge in this thesis concerns the present state of the art regarding children's digital rights to online privacy and protection from sexual abuse. Although there is significant research on children's privacy in legislative frameworks, children's privacy in relation to parental control, online risks and reviews of policies concerning children in the digital sphere, this type of contribution of issues is missing. This thesis is therefore based on material that touch upon both adults' rights and children's rights, to the extent that it is covered in different sources.

This thesis is also based on presenting relevant legislation, legal proposals, their recitals, and policies. A core document to frame and to find relevant policies, legislation, and legislative proposals for this thesis is the 'Compendium of relevant (BIK+) legislation and policy' which the European Commission has put together a compilation of the existing EU formal texts that relates to children in the digital worlds.[30] The legal position of soft law within EU law (guidelines, policies etc.) is not in its nature a binding document, meaning that it cannot normally be subject to judicial review by the EU Court.[31]

Legal doctrine has also been used in this thesis. The purpose with the legal doctrine is to contextualise and to shed light on different interpretations as well as to deepen the discussion around the nature of the norm system.[32] The authority of the legal doctrine depends on the strength and logic of the

[29] Hettne and Otken Eriksson (n 10) 158.

[30] European Commission, 'New Better Internet for Kids' Strategy (BIK+): Compendium of EU Formal Texts Concerning Children in the Digital World' (2022)

[31] Reichel (n 16) 125.

[32] Kleineman (n 10) 36.

argument.[33] The legal doctrine used consists of many of jurisprudential articles but the *EU charter on fundamental rights: A commentary* edited by Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward has played a vital role as the foundation of this thesis.

1.3.3 Theoretical points of departure

This subchapter aims to account for the theoretical points of departure of this thesis. There is a dilemma inherently present in children's rights law, namely the empowerment vs protection dilemma. The dilemma is part of a larger fundamental conflict underlying the whole of children's rights law. The empowerment vs protection dilemma is a conflict inherent to the UNCRC due to the potential tensions between articles pertaining to protective rights and those relating to participatory rights.[34]

Article 24 CFR that sets out the rights of the child in union law, has partially embraced this dilemma. Scholars argue that Article 24 CFR is a 'curious mix of what might loosely be termed children's protection and empowerment rights', which are often found to be in conflict. CFR explicitly resonates the tension between the child's right to express his or her views freely, which should be taken into consideration in accordance with a child's age and maturity, and the right to protection, when decisions are taken on behalf of the child, in his or her best interests. The right to protection stems from children's vulnerability, dependence on adults and need for physical and psychological care and nurture. Participatory rights (emancipatory rights) include children's claims to decision-making rights.[35]

The dilemma also relates to the tensions among several principles on which the UNCRC is built upon, such as the best interests of the child and the evolving capacities, participation, and self-determination of the child. These values are also underpinning Article 24 CFR. Efforts to support the best interests of the child require participation from children, but there is an inherent contradiction between the two, namely children's roles as beneficiaries of interventions by adults and competent social agents in their own rights.[36]

What is of particular interest is the special relation between privacy, and participation and protection rights. As a result of the CFR does not refer to any underlying values in relation to privacy, there are many different understandings of what constitutes privacy. Hijelke gives examples of arguments surrounding privacy. For instance, that scholars argue that the right to privacy reflects a value, namely individuality or personal freedom and may even be

[33] Kleineman (n 10) 36.

[34] Milda Macenaite,'From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU general data protection regulation' (2017) 19(5) New media & Society 766.

[35] Ibid 767.

[36] Ibid 768.

opposed to societal needs. It it's also argued in the legal doctrine that privacy also reflects a value in itself, by doing things privately. Others argue that the right to privacy is also a representation of other core ethical values in society, particularly human dignity and autonomy. According to the preamble of the CFR, all rights are underpinned with human dignity, but particularly privacy. Autonomy in relation to privacy seeks to describe a right to personal autonomy, that implies that an individual must be in control of his/her own life.[37]

Scholars argue that the children's right to privacy in the digital environment has various dimensions. For instance, it's important to protect children's privacy online as children constitutes a specifically vulnerable group of online users, that lacks awareness and capacity to anticipate potential long-term privacy consequences. However, the right to privacy is also a vital participatory right, especially with regards to older minors insofar that it is 'part and parcel of individual autonomy which is a necessary part of the participation right'. In other words, privacy could be seen as a prism in which when lights being shed on, a spectrum of participatory rights appears. [38]

Soft law policies steaming from EU-bodies, legal doctrines and UNCRC guidelines have called for a right-based (holistic) approach concerning children in order for children to realise their rights. This means a legal framework that can balance children's need for protection online with their capacity to maximize the opportunities and benefits from the digital sphere.[39]

This essay therefore starts from the premise and theoretical approach that privacy is a faciliatory (part and parcel) of all children's participatory rights which creates room for a discussion relating to children's rights on a general basis. This makes the thesis more in line with the interrelated nature of the different groups of rights in the UNCRC.[40] Hence, it is interesting to investigate the balance between children's privacy rights (including participation dimensions) in relation to children's right to protection that currently is discussed in the public debate. This to shed light on how the European Union have balanced children's digital rights in its case law and how the children's rights dilemma has been considered in order to realise the full extent of children's rights.

---

[37] Hielke Hijmans, *The European Union as Guardian of Internet Privacy; The Story of Art 16 TFEU* (Springer 2016) 40.

[38] Eva Lievens and others, 'Children's Rights and Digital Technologies' in Ursula Kilkelly and Ton Liefaard (eds.) *International Human Rights of Children* (2019 Springer) 496.

[39] Katharina Kaesling 'A Rights-Based Approach to Children Digital Participation in the Multi-Level System of the European Union' in Nina Dethloff Katharina Kaesling and Louisa Specht- Riemenschneider (eds.) *Families and New Media* (2023 Springer) 110.

[40] Savitri Goonesekere 'The Interrelated and Interdependent Nature of Children's Rights' in Jonathan Todres and Shani M King (eds.) *The Oxford Handbook of Children's rights law* (2020 Oxford Handbooks) 98.

1.4 Delimitations

The focal point of this essay is to examine the balance between children's right to privacy in the online transnational digital sphere with the right to protection from sexual exploitation and sexual abuse online. Moreover, the focal point is also to discuss children's rights based on the general classification's 'protection' and 'participation' rights in a broader perspective (through the right to privacy as a part and parcel for the participation right), instead of a detailed analyse on the impact of all rights. Due to its narrow scope and the extensive case law concerning privacy aspects (age generic) and the various risk to harm online, this essay only intends to give a hint of the balance between children's digital rights. However, this still plays a vital role as a facilitator for discussion regarding children's rights. Moreover, this thesis does not intend to be completely comprehensive in any matter. Importantly, this thesis only focuses on the mere balancing between children's rights and does not put any value in the matter.

This thesis will not address several issues relating to child sexual abuse online. For instance, the debate regarding a right to internet for children, as this essay focuses on a debate where the primary condition is that they have access to internet. Furthermore, the legal proposal treated in this thesis has also been criticised for having a major impact of the freedom to conduct a business. This is only mentioned in this subchapter but not further developed as there is no need to when considering the research questions. Children's right to privacy exists only within a framework that also respects parental authority, although there are questions regarding the parental involvement of children's online participation. These issues fall outside of the scope of this thesis, as it seeks to address issue that relates outside the domestic sphere.

Although the national courts could be considered as 'powerhouses' in the EU because they apply EU law, this thesis has been limited to not consider national case law.[41] The limitation is primary because of scope managing and simplification; EU law is a complex field pertaining several layers. The limitation creates a more straightforward approach in line with the thesis research questions and focus. Technical aspects will be short.

1.5 Outline

After the initial chapter follows an exposition of children digital rights to contextualize and to create an understanding of the landscape this thesis is going to navigate through. This by accounting for the rights that children are entitled to and how they are translated into the digital environment by soft law policies

[41] cf Hettne and Otken Eriksson (n 10) 28.

and legal doctrine and explaining EU's competence in relation to children's rights.

The third chapter examines the EU legislator attempts to balance children's right to privacy and protection through reviewing and analyzing secondary legislation in relation to a holistic approach. The fourth chapter aims to account for how fundamental human rights in EU law can be limited and derogation from and analyses case law from the CJEU and ECtHR in relation to privacy, children's protection online, and the best interest of the child. The fifth chapter accounts for the controversies surrounding the EU proposal regarding online sexual abuse on children. Finally, this thesis ends with a discussion with the research questions in consideration.

2 Children's digital rights

2.1 Translating children's rights to 'digital rights'

This chapter aims to provide a background on children digital rights and to create an understanding of how child online sexual exploitation and children's privacy takes form in the EU digital sphere.

One out of three users online today are estimated to be children. Their digital playground includes digital (social) media, mobile apps, and the internet of toys. A new comradeship has emerged online that children on a general note have a right to be a part of.[42] In fact, the use of digital technologies is today considered essential to exercising rights that relates to the exchange of communication. Consequently, the situation raises questions of the existence of new rights, accessory to the previous ones that are fundamentally related to the digital age, namely digital rights. Simultaneously, digital technology also increases the risks of fundamental rights infringements.[43]

The concept of 'children digital rights' may be considered as the legal protections and entitlements that are designed to ensure that children can safely and fully participate in digital society.[44] The digital era has not brought new rights to children but imposes an obligation on states to adapt the framework of existing right to the digital environment.[45]

Children's rights, as established in the EU charter, the ECHR and the UNCRC are often divided into two generalised categories: protection rights, and participatory rights, where privacy works as 'part and parcel' for the latter right.[46] Nevertheless, these protection and participation rights covers a range of areas, including privacy, data protection, freedom of expression, access to information, and protection from harmful content. Moreover, there are four overarching principles: non-discrimination, best interest of the child, the right to survival and development and the views of the child.[47]

Soft law policies steaming from EU-bodies, legal doctrines and UNCRC guidelines have called for a right-based (holistic) approach concerning children for children to realise their rights. This means a legal framework that can

[42] Katharina Kaesling, 'Children's digital rights: realizing the potential of the CRC' (n 1) 183.

[43] Eduardo Celeste, *Digital Constitutionalism; The Role of Internet Bills of Rights* (Routledge 2023) 16.

[44] Lievens and others (n 39) 489.

[45] Matko Gustin, 'Challenges of Protecting Children's Rights in the Digital Environment' (2022) 6 ECLIC 453.

[46] Helen Stalford (n 23) 32; See chapter 1.3.2 for the theoretical departure concerning privacy.

[47] Katharina Kaesling, 'A Rights-Based Approach to Children Digital Participation in the Multi-Level System of the European Union' (n 40) 81.

balance children's need for protection online with their capacity to maximize the opportunities and benefits from the digital sphere. Kaesling emphasises that a rights-based approach to children's participation online underscores vital point for their digital participation in the multi-level system of the European Union.[48]

2.2 The principle of the best interest of the child

The balancing of children's protective and participative rights is directly linked to the implementation of the core principle of the best interests of the child. The principle is encapsulated under Article 24(2) CFR, case law of the ECtHR and Article 3 UNCRC.[49]

In the legal doctrine, the best interest of the child is described as a core principle that contains a fundamental interpretative legal principle, a substantive right, and a rule of procedure.[50] Moreover, the principle of the best interests of the child influences the interpretation of legal norms. If one legal provision is open to more than one interpretation, the interpretation that most effectively completes the child's best interest should be chosen.[51]

Concerning the best interest of the child as a substantive right, children have a right to have their best interests assessed and considered as a primary consideration. This in relation to both decisions concerning a child as an individual but also decisions concerning children as a group.[52]

In case of a conflicting rights issue, the General comment states:

> 'If harmonization is not possible, authorities and decision-makers will have to analyses and weigh the rights of all those concerned, bearing in mind that the right of the child to have his or her best interests taken as a primary consideration means that the child's interests have high priority and are not just one of several considerations'.[53]

The General Comments also withholds that the best interest of the child does not attempt to prescribe what is best for the child in any given situation at any point of time. Rather, the comment states that the best interest of the child

[48] Katharina Kaesling, 'A Rights-Based Approach to Children Digital Participation in the Multi-Level System of the European Union' (n 40) 100.

[49] Ibid 77 ff.

[50] Ibid 83.

[51] United Nations Committee on the Rights of the Child, 'General Comment nr 14 [2013] on the Right of the Child to have his or her Best Interests taken as a Primary Consideration (General Comment nr 14)' (adopted on 29 May 2013, CRC/C/GC/14) 3.

[52] Katharina Kaesling 'A Rights-Based Approach to Children Digital Participation in the Multi-Level System of the European Union' (n 40) 84.

[53] General Comment nr 14 (n 52) 10.

principle is a dynamic concept that encompasses numerous issues which are continuously evolving.[54]

Furthermore, scholars suggests that the best interest of a child is flexible and is a mean for accounting the different socio-cultural context in which it is to be applied. In other words, the best interest of the child is culturally and socially determined. This is often considered to be based on what is empirically the most common form of life for children in general, arguing that the digital sphere and is a new context and should be a part of its presumed content. [55]

As a *rule of procedure,* the best interest of the child includes the evaluation of the impact a decision on the children concerned. Furthermore, the justification of a decision must show that the right has been explicitly considered by explaining what that has been in the child's best interests, based on which criteria and how the child's interests have been weighted against other considerations. This is applicable in both broad issues of policy and individual cases.[56]

To satisfy the requirements of the rule of procedure, trans-sectorial analysis may be necessary, regulatory measures from different legal areas may be considered collectively to properly understand the impact of the legal situation on children. This may also include measures that do not target children specifically, but that might affect children differently than adults.[57]

2.3 Children's digital right to protection from sexual exploitation

Evidence suggests that CSAM is more available and in larger amounts than it ever has been in human history, enhanced by new digital technologies. Widespread availability of technologies including the internet, dark webs, social media, mobile phones, video cameras and instant messaging have significantly changed the ways in which CSAM is produced and spread. These digital developments have allowed perpetrators to connect with children and document abuse by using portable devices and have therefore changed the dynamics of dissemination and detection avoidance. Today, perpetrators may easily connect with each other and share large capacities of CSAM when using the Dark Web. Child victims of sexual abuse often suffer innumerable physical, psychological, and social harms.[58]

[54] General Comment nr 14 (n 52) 5.

[55] Natasha Kravchuk 'Privacy as a New Component of "The best interest of the Child"' (2021) 29 (1) The international Journal of Children's Rights 121.

[56] Katharina Kaesling, 'A Rights-Based Approach to Children Digital Participation in the Multi-Level System of the European Union' (n 40) 84.

[57] Ibid 84.

[58] Francis Maxwell 'Children's Rights, The Optional Protocol and Child Sexual Abuse Material in the Digital Age' (2022) 31(1) The International Journal of Children's Rights 62.

The commitment to protect children in the EU is strong. Through various human rights instruments, practice guides, general comments, protocols and recommendations, several areas related to child ill-treatment are targeted.[59] For instance, almost every provision in the UNCRC contains some provision that supplements Article 19 UNCRC which sets out the general framework for state parties to protect children. Detailed provisions concerning economic and sexual exploitation are found in Articles 32-39 UNCRC. Additionally, the best interest of the child is found in Article 24 CFR, which provides a general commitment to protect children. The protection of children in the ECHR have been interpreted by the ECtHR to fall under Article 3 and 8 ECHR.[60]

The UNCRC general comment nr 25 on children's rights in relation to the digital environment emphasises measures to 'prevent exploitative use of children in pornography'. Furthermore, it is stated that parties should require a high standard of cybersecurity, privacy by design and safety by designed. Moreover, The general comment instructs that state parties should take legislative and administrative measures to protect children and implement safety and protective measures in accordance with children's evolving capacities.[61]

Maxell argues that by taking children's rights framework under the UNCRC, the most effective way to holistically achieve children's rights are prevention. Maxell argues to reduce the vulnerability of potential victims, it is important to focus on prevention distinguished from criminalization. Maxwell highlights that preventative measures for instance could be targeted against potential offenders from acting on pedophilic desires, equip children with knowledge and shaping the place of offending and consequently reducing the risk for children in the digital spheres.[62]

Moreover, Maxell argues that there are reasons to doubt the assumption that methods of criminalization for prevention is insufficient in relation to children's rights. For instance, many children victims of online sexual abuse do not report the exploitation. The understanding that children's own abuse will be watched by many others compounds shame and self-blame. Instead of reacting after the exploitation (criminalization) Maxell argues that a reduce burden on children to report better realizes children's rights, when taking into account all of the UNCRC overarching principles. [63]

[59] Helen Stalford (n 23) 168.

[60] Conor O'Mahoney, 'Child Protection and the ECHR: Making sense of Positive and Procedural obligations' in The International Journal of Children's Rights (2019) 27(4) 660.

[61] United Nations Committee on the Rights of the Child, 'General Comment nr 25 [2021] on Children's rights in relation to the Digital Environment (General comment nr 25)' (adopted on 2 March 2021, CRC/C/GC/25) 19.

[62] Francis Maxwell (n 59) 64.

[63] Francis Maxwell (n 59) 65 f.

2.4 Children's right to online privacy

In contrast to children's right to protection, privacy as a participation right is often mentioned briefly in legal and policy documents, but not in a longer explanatory way. Furthermore, children's privacy is often concentrated to data protection when it comes to the digital environment. Thus, privacy is a much broader and more complex concept.[64] Privacy for everyone has been recognised for a long time and that 'everyone' has without further thought assumed to be an adult, while the idea that minors merit the same, if not increased protection is not noticeable or lobbied for during law-making processes.[65]

Nonetheless, there are scholars that argue that privacy for children has gained more attraction during recent years, particularly in relation to parents' involvement in children's presence on the digital sphere.[66] For instance, Hijelke argues that children merit extra protection as a group of vulnerable people.[67]

The right to privacy (age generic) is not easy to describe. Although there are substantial provisions that relates to privacy, there are many different conceptualisations and interpretation of the concept privacy and data-protection. In short, privacy is a broad concept that relates to various aspects of one's individual and personal sphere of life, meanwhile data protection is more linked to processing of personal data and can be considered as a subset to the right to privacy. Personal data relates to information concerning an identified or identifiable individual and the capacity to control personal data about the individual.[68] Relevant provisions concerning children's privacy online are 16 UNCRC and Article 7 CFR that states that everyone has the right to respect for his or her private and family life, home, and communications. The article has a general application to any field of EU law where intersecting elements of the right may be affected.[69] In the EU digital sphere, privacy matters are often connected with Article 8 CFR (the right to protection of personal data).[70]

The rights of the child to privacy and right to protection of personal data are especially under pressure in the digital realm. Throughout childhood, children share media with friends, family or even sometimes strangers online. What is

[64] Lievens and others, (n 39) 496.

[65] Milkaite and Lievens 'Children's rights to Privacy and Data Protection Around the world: Challenges in the Digital Realm'10(1) 2019 European Journal of Law and Technology < https://ejlt.org/index.php/ejlt/article/view/674> Accessed 16 May.

[66] Kravchuk (n 56) 105.

[67] Hijmans (n 38) 42.

[68] Milkaite and Lievens (n 66).

[69] David Mangan 'Article 7 (Private Life, Home and Communications)' in Steve Peers and others (eds.) *The EU Charter of Fundamental rights: A commentary* (2021 Hart publishing) 152.

[70] This connection is further discussed in chapter 5.

disclosed is sometimes of a private or even intimate nature.[71] It has by now bee established in both literature and at a policy level that the engagement of minors in the practise of sexting is a legitimate form of sexual exploration . According to literature and international case law, intimate decisions, primarily of a sexual nature, as well as activities that occur in both public and private spaces and encompass sensitive issues as sexual preferences falls within the rather elusive concept of privacy. Sharing intimate imagery or texts of a sexual nature remains vital for an individual's self-development and self-determination and that intermediaries' users maintain the right to protect personal information from being monitored. Consequently, boundaries between the legal and illegal nature of sexual imagery depicting children are increasingly blurred. It follows that sexual or sexually suggestive imagery is not always the result of coercion or harassment as research shows that sexual images of children may be the result of coercion or harassment. Instead, research shows that sexual images of children may be exchanged among children on a consensual basis within intime relationships or as a form of exploration of sexuality.[72]

Moreover, research has revealed that children generally consider themselves to have a right to privacy online from their parents or friends, but have a limited understanding that their privacy may be infringed upon by states or commercial actors. According to Milkaite and Lievens, it is a well-established fact that, when children navigate the internet, and use mobile apps and connected devices, data about them is collected by both public actors, governments, and private actors as businesses. Moreover, the collection of personal data sets may lead to unprecedented consequences in the long term.[73]

Dataveillance is a term for automated, continuous, and unspecified collection, retention, and analysis of digital traces by state and corporate actors. There is evidence that individual's sense of being subject to digital dataveillance can cause them to restrict their digital communication behaviour, leading to a chilling effect as a self-inhibition and risk to undermine individual autonomy, well-being and democratic participation.[74]

Privacy in digital contexts is elaborated in the General comment.[75] For instance, it is highlighted that privacy is vital to children's agency, dignity, and

[71] Milkaite and Lievens (n 66).

[72] Argyro Chatzinikolaou 'Sexual images depicting children: The EU legal framework and online platforms' policies' 11(1) 2020 European Journal of Law and Technology < https://ejlt.org/index.php/ejlt/article/view/740> Accessed 7 May.

[73] Milkaite and Lievens (n 66).

[74] Moritz Büchi Noemi Festic and Michael Latzer 'The Chilling Effects of Digital Dataveillance:Theoretical Model and an Empirical Research Agenda' (2022) Big Data & Society 1,14. < https://journals.sagepub.com/doi/full/10.1177/20539517211065368> Accessed 10 May.

[75] United Nations Committee on the Rights of the Child, 'General Comment nr 25 [2021] on Children's rights in relation to the Digital Environment (General comment nr 25)' (adopted on 2 March 2021, CRC/C/GC/25) 11.

safety and for their exercise of their rights. Threats to children's privacy is for instance data collection and processing by public institutions, legal entities, organisations, criminal activities, activities from family members but also children's own conduct. Moreover, data is defined as a broad concept, including information about children's identities, activities, locations, communication, emotions health and relationships. Combinations of personal data may identify children, for instance the use of biometric data. In addition, digital practises may lead to arbitrary or unlawful interference with children's right to privacy and may have adverse consequences on children. Such digital practices are automated data processing, profiling, behavioural targeting, mandatory identity verification, information filtering and mass surveillance. Additionally, Interference with a child's privacy is only permissible if it is neither arbitrary nor lawful. The interference should be provided for by law and intended to serve a legitimate purpose while also uphold the principle of data minimization. Furthermore, the interference must also be proportionate and designed to observe the best interest of the child and must not conflict with the aims, objectives, and provisions of the UNCRC.[76]

2.5 EU's competence to regulate children right's issues

In order to understand the scope of children's right in EU, it is important to understand competence in EU to promote children's rights. The EU legislator have limited competence over the 'general promotion' of children's rights. The EU legislator only have competence in the areas conferred upon it by the Member states, which are found in the treaties. The treaties have only a few direct references relating to the rights of the child. For instance, Article 3(3) TEU states 'protection of the rights of the child' and Article 3(5) TEU states that EU aims to protect human rights, particularly the rights of the child.[77] In the TFEU, children are recognized in the 'area of freedom, security and Justice'(AFSJ), specifically in the context of asylum and immigration and cross-border criminal law. The clearest impact on children's rights have occurred in AFSJ. For illustration purposes, the most extensive nature of the provisions in the CSAM Directive are conferred to Article 82(2) and 83(1) TFEU. The articles provide competence to adopt measures on serious crimes with a cross border dimension including the trafficking and sexual exploitation of women and children.[78]

The few references to children in the treaties is not indicative that the EU does not have the competence to enact child-related measures. Firstly, because the EU has the authority to act in relation to any matter that crosses with an issue prescribed in the treaties, even if the link is relatively tenuous. For instance,

[76] Ibid 11.

[77] Ruth Lamont 'Article 24' in Steve Peers and others (eds.) *The EU Charter of Fundamental rights: A commentary* (2021 Hart publishing) 694.

[78] Ibid 700.

the EU legislator could be relatively inventively when referring to a broad treaty reference. The ultimate limit is the proportionality and subsidiary principles in EU law. Secondly, Article 24 CFR and the principle of the best interest of the child reflects the impact that EU law have on children and have a possibility to have a major impact of a wide range of measures.[79]

The European Union have sought to influence areas concerning children through different measures. For example, activities aimed at preventing online exploitation and the creation of a 'safer internet' by raising public knowledge and education. The goal aimed at making EU more relevant for children and important and promoting engagement with children across the state.[80]

[79] Ibid 694.
[80] Ibid 703.

3 The balance on children's digital right to privacy (participation) and protection from child sexual abuse in the legislative framework

3.1 Introduction

This chapter aims to account for the historical development, nature and scope of EU intervention concerning the legal framework of child protection and privacy online in EU law. Therefore, relevant legislative measures in transnational digital spaces are mapped out to examine how the user's privacy (including children) and the protection from sexual exploitation and abuse of children have been balanced throughout the history in digital spheres.

However, it's important to recognise that children's right to protection covers an array of issues.[81] Issues and risks that are related to the online environment is for instance online bullying, harmful content, exposure to sexual predators and privacy matters.[82] It's the issues sexual exploitation and privacy matters that will inform the discussion in this chapter.

3.2 The balance in secondary legislation: Then and now

3.2.1 Inserting a special liability regime

To get a proper understanding of the development and trajectory of the development it is important to start from the beginning of regulating the online environment. The Directive 2000/31 (e-Commerce Directive) was first of its kind and established a special liability regime for shared and disseminated online content.[83] The directive introduced into the EU legal model the opportunity for digital service providers to avoid liability if they are not aware of illegal content stored or uploaded by their users.[84] The aim with the The e-commerce Directive was to remove obstacles for cross-border online services, rather than protecting (children's) privacy or children from harm. Thus, this

[81] Stalford (n 23) 168.

[82] Kaesling, 'Children's digital rights: realizing the potential of the CRC' (n 1) 196.

[83] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) [2000] OJ L 178/1 (e-Commerce Directive).

[84] Marcin Rojszczak, 'Online content filtering in EU law- A coherent framework or jigsaw puzzle?' (2022) 47 Computer Law & Security Review < https://www.sciencedirect.com/science/article/pii/S0267364922000826> Accessed 30 April.

regulation still plays a vital role to understand the regulation that target those aforementioned areas.[85]

Children and privacy issues are mentioned in the recitals. Children are mentioned in the recitals '(…) the directive must ensure a high level of protection of objectives of general interests, in particular the protection of minors and human dignity, consumer protection and protection of public health'.[86] With regard to privacy it is stated that Member states are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature but that this only applies for monitoring obligations in a specific case.[87] Besides, the Member states must prohibit any kind of interception or surveillance of communications by others than the sender and recipient, except when legally authorised.[88]

The e-Commerce Directive, as previously mentioned, implemented a special liability regime, namely the *'notice and take down*' model in relation to internet service providers. This model defines the requirements under which a service provider may be exempted from liability for content stored at the request of users.[89] Firstly, the services provider must lack knowledge about the illegal nature of the content. Secondly, the service provider must conduct immediate action (blocking or removal of the information) if reliable information indicating its illegal nature. How the knowledge of the illegal nature of the content was gained is irrelevant. In other words, it doesn't matter whether it is by the service provider itself, the victim, or a third-party user. Simultaneously, the liability regime does not expressly include an obligation to remove other content that is identical to the challenged or to ensure that the similar content is also removed in the future.[90] Moreover, Member states are forbidden from imposing a general obligation to monitor information or 'actively seek facts or circumstances indicating illegal activity'.[91] This prohibition only concerns the implementing of a general oversight obligation on service providers, without affecting the possibility of establishing specific content control requirements.[92]

The EU legislator has throughout the years adopted legislation *lex specialis* which have supplemented the '*notice and take-down model'* in the e-Commerce Directive in various ways. For instance, there have been supplements concerning private interests but also in the field of criminal law with the view

[85] Ibid.
[86] Recital 10 e-Commerce Directive.
[87] Recital 47 e-Commerce Directive.
[88] Recital 15 e-Commerce Directive.
[89] Article 14(1) e-Commerce Directive.
[90] Rojszczak (n 85).
[91] Article 15(1) e-Commerce Directive.
[92] Rojszczak (n 85).

to facilitating the fight against serious crime.[93] A great distinction between the two different field is the role of the public authorities in deciding the scope of information that should be blocked or removed from cyberspace. In the field of criminal law, the legislation concerns the fight against child sexual abuse, child pornography and removing or preventing access to terrorist content.[94]

The commission recognised the need to reform the e-Commerce Directive and adopted the Digital Services Acts (DSA) in 2022.[95] The DSA aims to provide an updated regulatory framework for the operations of digital services while at the same time maintaining the 'core principles of the liability regime and the prohibition of general monitoring'. Moreover, in the explanatory memorandum is it stated that the prohibition of general monitoring obligations is 'crucial to the required fair balance of fundamental rights in the online world'. Secondly, the application will not affect the Child sexual abuse Directive (CSAM Directive) other directives regarding monitoring obligations.[96]

3.2.2 Protective and preventative legislation concerning child sexual abuse

Out of a historical perspective the CSAM Directive, replacing the Framework Decision 2004/68/JHA, was the first regulation to allow and define an obligation to apply online content filtering measures.[97] The purpose with the directive is to improve the protection of children from sexual abuse and exploitation by adopting prevention measures, protecting child victims and investigate and prosecute offenders.[98]

The recitals mentions both participatory rights and protection rights. Children's right to protection from child sexual abuse and that the child's best interest must be the primary consideration is highlighted several times in the recitals.[99] It is also emphasised that it vital to considering an assessment of children's needs.[100] The CSAM Directive excludes personal face-to-face

[93] For example: responding to hate speech and defamation and copyright protection, see Rojszczak (n 85).

[94] For instance, Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography (CSAM-Directive) [2011] OJ L 335/1; Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA [2017] OJ L 88/6.

[95] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277/1.

[96] Recital 10 CSAM Directive.

[97] Rojszczak (n 85).

[98] Recital 4 CSAM Directive.

[99] Recital 2, 6, 30 CSAM Directive.

[100] Recital 30 CSAM Directive.

communication between consenting peers, as well as children over the age of sexual consent and their partners from the definition. Moreover, the directive does not govern Member parties' policies regarding consensual sexual activities in which children may be involved and which can be regarded as the normal discovery of sexuality during human development. The directive is taking account of the different cultural and legal traditions and of new forms of establishing and maintain relations among children and adolescent, including through information and communication technologies. These issues fall outside of the scope of the CSAM Directive. It is stated that effective investigatory tools should be made available. Those tools could include interception of communications, covert surveillance including electronic surveillance (…) taking into account, amongst other, the principle of proportionality and the nature and seriousness of the offences under investigation.[101]

The CSAM Directive set out obligations for Member parties to establish national measures to make certain the removal of child pornography content distributed from servers located within their respective territory.[102] Furthermore, the Directive also provided for a possibility to voluntary implementation of blocking measures regarding sites containing child pornography located on foreign services.[103]

The directive does not lay out detailed provisions regarding the removing and blocking of contested content. Nor does it lay out a maximum time limit for removing or blocking the contested content. Furthermore, the directive does not contain any proactive obligation for service providers to identify paedophile content, and no sanctions for non-compliance. To meet their obligations, Members states have in general chosen to meet their obligations in two different ways; by relying on the *'notice and takedown'* mechanisms set out in the e-Commerce Directive or implementing measures under national criminal law. In some countries which choose to rely on the notice and takedown mechanisms have also set up hotlines for monitoring paedophile content and report identified cases to services providers. Subsequently, that information in Member states also have been shared to law enforcement authorities. This practice, informing Law enforcement authorities (LEA), is also used when infringing content is found on servers in other countries.[104]

In relation to the voluntary implementation of blocking measures, only half of the Member states have chosen to introduce such national legislation. In those cases, the blocking is either based on a court order or is completely voluntary. It is also common that public services create a list of 'black sites' which is shared with service providers. In the same way here as regarding the removal and blocking of contesting content, the directive does not set out any

[101] Recital 27 CSAM Directive.
[102] Recital 2 CSAM Directive.
[103] Rojszczak (n 85).
[104] Ibid.

detailed provisions. For example, there are no formal obstacles to the establishment of a blocking mechanism implemented concerning providers of mobile devices, in comparison with ISPs.[105]

The Victims' Rights Directive aim is to establishing minimum standards on the rights, support, and protection of victims of crime, for instance child sexual abuse, sexual exploitation, and child pornography.[106] The directive contains provisions that states the right to protection of privacy for all people under criminal proceedings.[107] The directive emphasises that an individual assessment should take into account the personal characteristics of the victim such as for instance his or her age.[108] Concerning children is it stated that the best interests of the child must be a primary consideration in accordance with CFR and UNCRC. Child victims should also be considered and treated as the full bearers of rights set out in the Victims' Rights Directive and should be entitled to exercise those rights in a manner that considers their capacity to form their own views.[109]

The Audiovisual Media Services Directive (AVMSD Directive), revised in 2018 to consider newly developments, contains measures to protect minors from harmful content on video sharing platforms.[110] The AVMSD Directive also contains cross-references to the prohibition of general monitoring set out in the E-commerce Directive.[111] For instance, there are rules to protect children from seeing illegal or harmful content, in appropriate advertising, product placements. Video-sharing platforms also have obligations to protect all users from certain illegal content, for example child pornography set out in accordance with the CSAM-directive.[112]

To protect children, the platforms are required to offer easy ways for users to rate, flag and report illegal/harmful content. Moreover, implement parental controls and age verification systems.[113] Consequently, great emphasise on protection children is in the directive whereas platforms must protect children from audio-visual content that 'impair their physical, mental or moral

[105] Ibid.

[106] Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA, [2012] OJ L 315/57; Recital 7 Victims' Rights Directive.

[107] Article 21 Victims' Rights Directive.

[108] Recital 55 Victims' Rights Directive.

[109] Recital 14 Victims' Rights Directive.

[110] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (codified version) (Text with EEA relevance), [2010] OJ L 95/1; Recital 4 Victims' Rights Directive.

[111] Article 28(a) AVMSD Directive.

[112] Article 28(b) AVMSD Directive.

[113] Article 28 (f), 28(i) AVMSD Directive.

development'.[114] Additionally, it is recognises that children merit specific protection about the processing of their personal data.[115]

While the specific risks on children encounter on such platforms are mentioned, there is no reference to benefits children encounter due to their participation.[116] In comparison, those with impairments and elderly people are seen to be further integrated in the social and cultural life of the EU.[117] Consequently, there is no participatory rights for children mentioned *per se* in the recitals although the directive is shaping the limits of restrictions on children's participation in the transnational digital sphere.[118] Albeit, there are some recitals concerning individuals and the purpose of audio-visual media services of shaping public opinion, empower viewers (including minors) by providing sufficient information, and how important it is to promote media literacy.[119]

3.2.3 Privacy legislation and its relation to CSAM

The general data protection regulation (GDPR), with the purpose to harmonise privacy laws and providing greater protection and rights to individuals, contains numerous provisions concerning the processing of children's data.[120] The regulation contains many innovative *empowerment rights* such as the right to be forgotten, the right to data portability, protection by design and data protection by default and provision concerning transparent information and awareness.[121] Simultaneously, GDPR contains two protective provisions for children as data subjects whose personal data is collected, held, or processed. Firstly, there is a protective provision that impose obligations on external parties to abstain from certain data collection practices. Secondly, positive obligations on parents to engage in activities to secure the effective enjoyment of their child's fundamental rights.[122]

Despite the overweight of empowering rights, GDPR is still considered to fail on empowerment rights as a paternalistic protection is favoured over empowerment of children. Scholars highlights that the regulation justifies protective measures exclusively in the light of children's inadequacies by stating that

[114] Article 6(a), Recital 19 and 47 AVMSD Directive.

[115] Recital 21 AVMSD Directive.

[116] See for instance recital 4, 20, 21,28,30 and 47 AVMSD Directive.

[117] Recital 22 AVMSD Directive.

[118] Katharina Kaesling 'A Rights-Based Approach to Children Digital Participation in the Multi-Level System of the European Union' (n 40) 110.

[119] Recital 19,54 and 59 AVMSD Directive.

[120] 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, GDPR) [2016] OJ L 119/1.

[121] For a longer discussion regarding children's or individuals empowering rights in GDPR see Macenaite, (n 34) 768.

[122] Parental obligations are not going to be further discussed as they fall outside the scope of this thesis.

children merit specific protect due to their lower awareness of risks, consequences, safeguards, and rights relating to the processing of their personal data. In relation, all the empowering rights concerns individuals as such.[123] Scholars argue that GDPR sets the overall tone for the treatment of a child's personal data when it says that children merit specific protection about their personal data, as they may be less aware of the risks, consequences safeguards and their rights in relation to the processing of personal data.[124]

In GDPR it is stated the right to protection of personal data is not an absolute right. The protection of personal data must be considered in relation to its function in society and balanced against other fundamental rights, in accordance with the principle of proportionality. In addition, that GDPR respects *all fundamental rights* and observes the freedoms and principles recognised in the Charter, *in particular* the respect for private life, home and communications, the protection of data (..). The recital does not mention Article 24 CFR, the rights of the child, although there are provisions concerning children directly and indirectly.[125] GDPR has also played a vital role concerning the processing of personal data by providers of number-independent interpersonal communication services by means of *voluntary measures* for the purpose of detecting, reporting, and removing CSAM up until 20 December 2020.[126]

The e-Privacy directive makes sure that all users, including children, can use electronical communications in a confidential way and that their devices are protected.[127] The e-Privacy Directive ensures the protection of fundamental rights and freedoms, in particular the respect for private life, confidentiality of communications and the protection of personal data in the electronic communication sector.[128] The commission has proposed a new regulation on e-Privacy to modernise the current Directive and provide more legal certainty for all users.[129] Children is not mentioned in the recitals of the directives nor in the proposal.[130]

In 2021 a regulation concerning a *temporary derogation* from the e-Privacy Directive was adopted. This temporary derogation (Interim Regulation) from the provisions 5(1) and 6(1) e-Privacy Directive allows online

[123] Macenaite (n 34) 775.

[124] Recital 38 GDPR.

[125] Recital 4 GDPR.

[126] Rojszczak (n 85).

[127] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, e-Privacy Directive) [2002] OJ L 201/37.

[128] Recital 1 e-Privacy Direcive.

[129] Commission, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications, Proposal for a Regulation on e-Privacy)' COM (2017) 010 final.

[130] See e-Privacy Directive and the proposal for a Regulation on e-Privacy.

communication services to voluntarily detect, report and remove child sexual abuse material online (to fight serious crime) until august 2024.[131] Like the CSAM Directive, this regulation deals with preventing access to and distribution of paedophile content. In contrast to the CSAM Directive the purpose of this regulation is to allow providers of certain electronic communications services to use modern data processing measures to identify cases of CSAM.[132]

The directive underlines that Article 24(2) CFR and that the child's best interests must be primary consideration and that 'digitalisation has brought about many benefits for society and the economy, but also challenges such as child sexual abuse'. There is also a direct reference to the UNCRC.[133] The protection of children online is one of the Unions priorities.[134]

This regulation also introduces a legal basis for the usage of automated mechanisms for analysing traffic and content data exchanged between users of communication systems and reporting them to authorised authorities in the event of suspected paedophilic content. Therefore, an exception was introduced to the application of the GDPR and the e-privacy Directive by increasing the permissible scope of use of data by providers of the number-independent interpersonal services (such as operators of instant messaging services like Skype or Viber).[135]

The provisions regarding the service providers obligations are rather detailed, for example by indicating a data retention period and by strictly limiting the scope of permissible processing. Thus, the regulation does not in principle exclude any technical means used to identify illegal material. Scholars argue that the regulation rather establishes a framework for service providers to develop and use new ways of user surveillance that would be more effective in detecting infringements.[136] The directive emphasis limitations interfere with the right to confidentiality if they involve a general and indiscriminate monitoring and analysis of the communications of all users.[137]

Scholars withholds that if the outcome of the Interim Regulation leads to a possibility of a permanent and generalised monitoring and analysis of all user's communications is going to be accepted, same reasoning and arguments that the regulations is based on may transfer to other crimes labelled as

[131] Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse (interim Regulation) [2021] OJ L 278/69.

[132] Rojszczak (n 85).

[133] Recital 4 Interim Regulation.

[134] Recital 3 and 4 Interim Regulation.

[135] Rojszczak (n 85).

[136] Ibid.

[137] Recital 8 Interim Regulation.

serious.[138] This discussion has further exacerbated in relation to the EU proposal regarding child sexual abuse which aims to replace the temporary derogation. This proposal will be further discussed under chapter 6.

3.3 Discussion

The purpose with this subchapter was threefold. Starting out with the first, the historical development regarding intermediaries' obligations and the impact of user's privacy rights started off with the '*notice and take down'* regime. Gradually, intermediaries were imposed different obligations. Firstly, the sexual abuse directive that adopted which imposed the first filtering obligations, although without detailed provisions. Many of the Member states choose to rely on the notice and take down system. Secondly, the AVSVD Directive regulated the audio-visual media online - not through filtering obligations, rather by implementing an effective reporting system. The AVSVD Directive also contains references to the e-Commerce Directive and the prohibition of general monitoring. The Interim Regulation on the other hand opens new ways to monitor because it provides a legal basis for automated mechanism to analyses traffic and location data. It seems that the spectator becomes the monitor for their users (illegitimate) actions on their platforms.

In relation to monitoring, some of the legislations have echoed prohibition on general monitoring and prohibition of unlawful interference (e-Commerce Directive) throughout the history, which today is one of the aims of DSA; to maintain the core principle of the liability regime and the prohibition of general monitoring. In the event of combating crime under the CSAM Directive, it echoed that electronic surveillance must be proportionate to the nature and seriousness of the measures conducted. Interestingly, there are no recitals in the Interim Regulation that emphasizes the importance of not conducting surveillance (compare with CSAM Directive) although according to critics the Interim Regulation opens for such possibilities. Thus, the Interim Regulation contains statements regarding general and indiscriminate monitoring.

Concerning the nature of the EU intervention there are arguments for a protectionist approach still overweight's a holistic approach.[139] Their argument that are in favor for a holistic approach, such as for instance under the victims' Rights Directive where children are considered as bearer of rights and that they are entitled to exercise those rights in a manner that considers their capacity to form their own views. Moreover, in the CSAM Directive, personal face-to-face communication between consenting peers was excluded from the scope, as well as children over the age of sexual consent and their partners from the definition.

[138] Rojszczak (n 85).
[139] See chapter 1.3.2

At the same time, there are many arguments that are in favor for a protectionist approach. One a general note, children tend to be considered in a group of 'vulnerable persons' concerning risks, meanwhile the benefits from the digital environment are applicable of all people. Consequently, there is no participatory rights for children mentioned *per se* in the recitals although the legislation is shaping the limits of restrictions on children's participation in the transnational digital sphere, or there is no participatory right mentioned at all. This is particularly visible under the AVSVD Directive, where those with impairments and elderly people are further integrated in the social and cultural life. Moreover, it is consistently repeated in the GPDR children merit extra protection, but their rights aren't mentioned in the recitals, nor the best interest of the child.

4 Balancing children's digital rights to privacy (participation) and protection from child sexual abuse

4.1 The issue of insufficient case law

This chapter aims to account for the limitations and derogations of children's right to privacy and right to protection in the transnational digital sphere, and how these rights have been interpreted in the case law derived from the CJEU and ECtHR.

Child protection is a complex matter, pertaining measures through legislation, policies and by Member states on their own.[140] Many of the substantive rights in the CFR are applicable to child protection, meanwhile Article 24 CFR acknowledges more generally children's inherent vulnerability and need for protection.[141] Substantive EU measures concerning child sexual exploitation have been previously discussed in chapter 3, where legally binding EU child protection measures that has been developed concerning with an aim to protect children is the CSAM Directive, AVSVD Directive, and the Interim Regulation. Therefore, these regulations must be used as a benchmark when interpretating the right to protection from sexual exploitation and its balancing, where references to Article 24(2) CFR best interest of the child and UNCRC as instrument is mostly prevalent. The Courts interpretation of Article 24(2) CFR is therefore of relevance in relation to the right to protection from sexual abuse.

Obtaining case law that directly pertains to the specific legislative framework and addresses children's right to protection and privacy in a digital sphere as a 'conflicting rights dilemma' proves to be challenging. To the best of this authors knowledge, as of the present date, there is an absence of case law that addresses this situation. Due to aforementioned reasons, this chapter will focus on the interpretation of children's rights in relation to existing case law and legal analysis. When case law concerning children is insufficient, the interpretation of adult's (human) rights is analysed to provide guidance.

[140] Helen Stalford (n 23) 167.

[141] For instance, Article 3 (right to the integrity of the person), Article 4 (prohibition of torture and inhumane degrading treatment and punishment), Article 5 (prohibition of slavery and forced labour), Article 18 (right to asylum), Article 19 (protection in the event of removal, expulsion, or extradition) and Article 32 (prohibition of child labour and protection of young people) in CFR.

4.2 Best interest of the child

4.2.1 The inherent limitations on best interests of the child

Article 24 CFR does not contain any specific derogations, although the terms of Article 24(1) and 24(3) CFR permits their non-application in defined circumstances. Article 24 (2) CFR obliges Member states to make the child's best interests a primary consideration in their decision-making when implementing EU law. The article further state that all decisions by a public authority, including courts, must have the child's best interests as a primary consideration. Article 24(2) CFR is inherent limited in its application in a two folded way.[142]

Firstly, by the status of the best interest's principle, as a 'primary consideration'. The child's best interests can be overridden by other factors in the decision-making because the best interest of the child is one of several 'primary factors' amongst other legitimate factors. If the child's best interests are the paramount consideration in a decision, the best interests factor dictates the decision-making process. Accordingly, this limits the role of the child best interests in decision-making as one important factor, rather than the most important factor. Secondly, Article 24(2) CFR is limited in relation to the bodies applying the principle in their decision-making. The bodies that should consider the best interest of the child principle are public authorities and private institutions. Consequently, children's rights are limited because of the circumstances in which children's bests interests will be considered.[143]

4.2.2 The interpretation of best interest of a child

4.2.2.1 The European Court of Justice

The rights of the child as protected by Article 24 CFR have had considerable impact on the ECJ case law, especially in relation to migration and asylum issues. Beyond that, also vis-à-vis cross boarder-family law and child abduction matters. The principle has also worked as guidance for the interpretation of secondary legislation on family reunification and for the guidance on the interpretation of the right to *family life* under Article 7 CFR. Despite the fact that Article 7 CFR encompasses both *family life* and *private life,* with the possibility of these two values intersecting, there is notable absence of case law from the CJEU regarding the best interest of the child in relation to the right to *communication* and *private life*.[144]

Scholars are today under the notion that there is no substantive content in the best interests of the child as a norm. In EU law, it has come to be defined as

[142] Lamont (n 78) 720.

[143] Ibid 720.

[144] Cf O'Flaherty and Samardžić-Marković (n 3). There is no notion of private life as such, and that search on CURIA does not give any guidance nor any scholarly articles.

casuistically by the CJEU. To achieve what can be considered best interest of the child in decision-making, the court must take discretionary account of the child's interests and wishes. The CFR is silent regarding possible conflicts between the best interests of the child and other interests, and the CJEU has been reserved in its reasoning on such rulings.[145]

The meaning of the child-specific protection of rights in Article 24 of the EU Charter appears to be above all a matter of there being protection for the children's needs and a consideration of the child's best interests, where its precise meaning depends on the concrete circumstances in the case. The application may require flexible approach to measures and including considering alternatives most favourable to the child's welfare. Additionally, the application may require decisions-makings with rapidity, and providing for procedures that guarantee that children can freely express their views in accordance with their age and maturity.[146] Moreover, scholars are under the impression that Article 24(2) CFR have been interpreted as confirming and supporting interpretation of the existing law, rather than disruptive the EU legal framework in the interests of the child.[147]

The legal nature of the concept *'best interests of the child'* is unclear. Lang argues that there are three formal arguments and a number of substantive one in favour for considering the concept of best interests of the child as a general principle of EU law, or a consistent part of the right to family life and of the rights of the child (that in themselves could be considered general principles of EU law).[148] The three formal arguments in conjunction with each other favours the interpretation of a general principle of EU Law. The first formal argument derives from the fact that Article 6(3) TEU declares that 'fundamental rights, as guaranteed by the ECHR and as they result from the constitutional traditions common to the Member states, shall constitute general principles of EU law'. The second formal argument is based upon the numerous rulings in which the ECHR has stated that the States Parties have a duty to protect the best interest of the child, which consistently affirms the best interests of the child principle in Article 8 ECHR. Moreover, that the EU Charter explicitly lists the rights of the child in Article 24 CFR is also in favour for the interpretation and that the wording derives from a principle of international law.[149] Lastly, the fact that several EU instruments invoke the

[145] Carl Lebeck, *EU-charter on Fundamental rights* (2nd edn 2016 Studentlitteratur AB) 565; Kravchuk (n 56) 102.

[146] Steven Greer Janneke Gerards and Rose Slowe (eds.), 'The fundamental Rights Jurisprudence of the European Court of Justice' in *Human Rights in the Council of Europe and the European Union: Achievements, Trends and challenges* (Cambridge University Press 2018) 348.

[147] Lamont (n 78) 723.

[148] Iris Goldner Lang 'The Child's Best Interest as a Gap Filler and Expander of EU Law in Internal Situations' in Katja S. Ziegler and others (eds.) *Research Handbook on General Principles of EU Law* (2019 Edward Elgar Publishing) 564.

[149] Previously discussed in chapter 2.2

UNCRC, implies that they embrace not only the concept itself, but also its function in the legal nature as interpretated by the UN Committee.[150]

Some substantive arguments favouring the idea of a general principle of EU law is that the rights of the child in general and the principle of the child's best interests express core values of the EU legal system. They are intrinsic to EU's social values and convictions, which is associated with the functioning of a democratic civilised society. The rights of the child and the child's best interests suggest the underlying rationale in rulings concerning children, by guiding the court to rulings that will accommodate the child's best interests in the given circumstances. In other words, it differs from an ordinary rule. Besides, the child's interests contain a certain level of generality and abstraction, which has a threefold manifestation. Firstly, they are applicable to any situations involving children and consequently underlies the whole EU system. Secondly, the level of abstraction makes the principle adaptable to the situation of each child and their development.[151] Thirdly, the rights of the child and the child best interests are recognised across all Member states.[152] The last substantive argument is related to the notion of that the child best interests also serve a three-layered function attributable to general principles of EU law. Lang argues that the concept of the child's best interests has an interpretative and gap-filling function, which enables the evolution of EU law and its expansion to a new category of situations concerning children that previously fell outside the scope of EU Law.[153]

4.2.2.2 European Court of Human Rights

The case law from the ECtHR concerning the principle of best interest of the child has attracted criticism for various reasons. Firstly because of children not being adequately protected because there is no guarantee of the child's right to be heard, or that the child's welfare is of primary our paramount importance. Additionally, the lack of participatory rights means that the protection of children's welfare has a much greater stake in ECHR than their right to autonomy.

Secondly, the approach taken by the ECtHR concerning children in its ruling have been criticised for 1) failing to fully articulate a conception of 'best interests of the child', leaving state parties with a great margin of appreciation and 2) in for being inconsistent in its own case law.[154] Although the court have pointed out that 'there currently a broad consensus – including in international law – in support of the idea that in all decisions concerning children,

[150] Lang (n 149) 165.

[151] The level of abstraction has also been criticised for being unclear. See Kravchuk (n 56) 103.

[152] This argument is derived from the authors own analysis of case law concerning family reunification in Lang (n 149) 565.

[153] Ibid 567.

[154] Lamont (n 78) 705.

their best interests must be *paramount*', the case law from the ECtHR appears to be ambivalent because of the use of 'primary consideration' and 'paramount consideration' without a sufficient clear distinguishing criterion.[155] Thus, there are evidence of an emerging child-centred approach because of the greater extent of references to UNCRC.[156]

Nevertheless, the ECtHR has repeatedly stated that it has not set out an exhaustive list of factors to consider, because the factors may vary depending on the circumstances of the case in question. However, scholars argue that the ECtHR jurisprudence shows that there are certain presumed interests, for instance child's health and development.[157]

In the ECtHR's case law child protection has primarily been grounded in Article 3, 2 and 8 ECHR but the principle 'children should be protected from ill-treatment' remains the same. In cases of ill-treatment which may not reach the Article 3 ECHR threshold, there is a separate obligation deriving from Article 8 ECHR to enact effective laws to protect children from abusive conduct.[158] Most of the child abuse and neglect occurs at the hand of private actors, which makes the case law more complex. This because the case law establishes a line of responsibility to the state. The ECHR has been interpretated by the ECtHR in a way that imposes demanding obligations on State Parties that are increasingly influenced by the UNCRC. The obligations include *procedural* obligations to investigate complaints of ill-treatment, obligations to protect children before it occurs, responding to ill-treatment and effective remedy, obligations that also have been reaffirmed in rulings from the CJEU.[159]

In relation to ill-treatment, the ECtHR addressed online safety issues in *K.U V Finland.* The court stated that a posting of advertisements of a sexual nature concerning a 12-year-old boy was a criminal act that resulted in a child becoming target for paedophiles. The court called for a criminal law response that included appropriate investigation and prosecution measures. The court noted that new forms of communications required even greater carefulness when the information related to child privacy concerns. States have a positive obligation to establish a legislative framework to protect a child from grave interreference with his/her privacy in appropriate manner.[160]

---

[155] Kravchuk (n 56) 104.

[156] Anette Faye Jacobsen 'Children's rights in the European Court of Human rights – An emerging Power Structure' in The International Journal of Children's Rights (2016) 24 (3) 548 ff.

[157] Kravchuk (n 56) 104.

[158] How the articles interrelate are further discussed in O'Mahoney (n 61) 663.

[159] For instance, see para. 126 – 128 *Case 511/18 La quadrature du net and Others* (2020) ECLI:EU:C: 2020:791.

[160] Kravchuk (n 56) 106; *K.U. v. Finland* [2008] (App no. 2872/02).

4.3 Privacy in a digital context

4.3.1 The interconnectivity between CFR and ECHR

Case law concerning information technology from the CJEU has grown during the recent years. In these cases, Article 7 and 8 CFR has often been considered in conjunction.[161] Before going into the possible limitations on privacy, this relationship will be discussed.

Article 7 and 8 CFR are interconnected with Article 8 of the ECHR. The rights set out in Article 7 CFR concerning the right to privacy correspond to those in Article 8 ECHR.[162] In accordance with Article 52 (3) CFR, the meaning and scope of this right are the same as those of the corresponding articles of the ECHR.[163] By this follows that the limitations that may legitimately be imposed on this right are identical to those allowed by Article 8 ECHR. Meanwhile Article 8 CFR that states the protection of personal data contains several sources. The article is 'based upon' Article 8 ECHR, on the Council of Europe Convention 108 and Directive 95/46/EC.[164] The ECHR is not formally incorporated into EU law, although it forms a general principle of EU law. Consequently, the assessment of EU law is assessed against the CFR.[165]

Although Article 8 CFR is closely connected with the right to respect of private life express in Article 7 CFR their correlation has various dimensions. The rights may under certain circumstances be understood as intermingling; 'it should be borne in mind that the right to respect for private life with regard to the processing of personal data concerns any information relating to an identified or identifiable individual'. But at the same time, the rights can intersect because of protection of personal data can affect private life. When they intersect, Article 7 CFR forms a broader protection of a right to respect to private life, home, and communications meanwhile Article 8 CFR seems to be a particularised subset of privacy, focusing upon personal data.[166]

---

[161] Mangan (n 70) 179.

[162] Other sources of Article 7 CFR are Article 12 in the Universal Declaration of Human rights and Article 17 of the International Covenant on Civil and political rights.

[163] Article 52 (3) CFR states that 'In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention'.

[164] 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 [1995] OJ L 281/31; Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) [1981] CETS No. 108.

[165] Mangan (n 70) 179.

[166] Ibid 193.

Article 7 CFR includes many different aspects of private life. The precis meaning of private life is hard to distinguish. The concept of private life has a separate meaning as an autonomous concept both under ECHR and CFR. Private life is an overarching concept in relation to the other rights element under Article 8 ECHR and Article 7 CFR. Under Article 8 ECHR the concept of private life can be characterised as encompassing the physical, psychological, and moral aspects of the personal integrity, identity, and autonomy of individuals. Article 8 EHCR have an expansive interpretation that under the CFR finds its expression in several articles, such as Article 3 CFR (right to the integrity of the person), Article 8 CFR (right to protection of personal data) and Article 24 CFR (rights of the child).[167]

The express right to respect for communications in Article 7 CFR can be seen as a supplement to the protection of private life (and home). This right often overlaps with the right to respect for private life. Communications has today become an important tool for private life. These communication tools create data as a by-product, which individually or in the aggregate data collected can reveal details about an individual's private life. Furthermore, the protection extends to whether the communication is still being processed or has already been received and stored by the addressee. The protection extends not only to correspondence of a personal character (intimately private nature) but also correspondence with professional and commercial content.[168]

Information technologies convey data along with individuals' communications, where protection of personal data as an aspect of the right to respect for private life (including communications) remains a developing area within the spectrum of EU fundamental rights. The CJEU has released several decisions dealing with these issues. Although these articles combined importance has been recognized, further elaboration of each articles remit has been sparing. Importantly, these cases have concerned information technology and the capacity therein to from a repository of a wide range of information.[169]

The CJEU has demonstrated that, as a matter of principle, the need to interpret Article 8 CFR on data protection in accordance with the general right to respect for private life under Article 7 CFR by way of the combinate applications of both provisions. However, in other parts of the case law concerning data protection the CJEU has based its rulings on Article 8 CFR alone.[170]

4.3.2 Limitations on online privacy

The CJEU often consider Article 7 and 8 CFR together and does not apply a consistent approach to the distinction between the two articles. Regarding interferences, the court tend to formulate itself more extensively in relation to

[167] Ibid 153.
[168] Ibid 161.
[169] Ibid 179.
[170] Ibid 156.

privacy rather than limit itself to state that is also an interference with the right to data protection because the measure at issue 'constitute processing of personal data'.[171]

The explanatory note to the CFR articulates that Article 7 CFR is a qualified right, meaning that any interference with the protected rights will be prohibited unless it falls within the limitations permitted by Article 52 CFR.[172] Article 52(1) CFR sets out rules regarding any limitations on the exercise of the rights and freedoms recognised by the charter. The Article states that any limitation must be provided for by law and respect the essence of those rights and freedoms. This limitation is also subject to the principle of proportionality, meaning that the limitation must be necessary and genuinely meet the objectives of general interests recognised by the Union or the need to protect the rights and freedoms of others. It is important to note that Article 52 (1) CFR refers to two categories of justifications: the objectives of general interests recognised by the union and the need to protect the rights and freedoms of others. In principle these two grounds can overlap – since the Union's objective could include the protection of others' rights and freedom, for instance the rights of the child in 3(3) TEU.[173]

The CJEU may have the possibility to adapt a more flexible concerning the limitations on Article 7 CFR than what follows from 52(1) CFR. This because of the interpretation and application of Article 8 ECHR established by the ECtHR, has implications for the meaning and the scope of the rights under Article 7 CFR, as set out in Article 52 (3) CFR. The limitations laid down by Article 8(2) ECHR concerning the legal basis for interference requires accessibility, precision, legitimate aim, and proportionality.[174]

The CJEU have several times touched upon limitations of the right to privacy in relation to information technologies. The CJEU sets out its interpretative approach in relation to limitations that might be imposed on the existence of Article 7 and 8 CFR in *Volker und Markus Schecke.*[175] The case concerned the validity of secondary EU law provisions. The approach consisted of an assess whether the *"essence"* of the right has been respected by the limitations set out in the challenged law. The analysis then turns to proportionality, whether the measures taken meet genuine objectives of general interests and whether the measures taken are limited to those which are strictly necessary.[176] The necessity of the step taken was examined against the publication

[171] Herke Kranenborg 'Article 8' in Steve Peers and others (eds.) *The EU Charter of Fundamental rights: A commentary* (2021 Hart publishing) 282.

[172] Mangan (n 70) 157.

[173] Steve Peers and Sacha Prechal 'Article 52' in Steve Peers and others (eds.) *The EU Charter of Fundamental rights: A commentary* (2021 Hart publishing) 1625.

[174]Mangan (n 70) 157.

[175] Joined Cases C-92/09 and C-93/09 *Volker Und Markus Schecke GbR and Harmut Eifert V Land Hessen* [2010] ECR I-11063.

[176] Mangan (n 70) 194.

of details about the amount of EU subsidies farmers received. The CJEU stated that the interest pursued by the data processing should be balanced against the interreference with the right to privacy and the protection of personal data of the person concerned. Furthermore, they stated that derogations and limitations must apply in so far as it is strictly necessary, and based the assessment on whether the intended objective could be pursued by measures which interfere less with the right of the data subject concerned. Regarding the necessity of a measure, the court held that The Council and Commission could have taken less intrusive means into consideration and declared the provisions imposing the measures invalid.[177]

In *Digital rights* the validity of EU secondary law was challenged (the Data Retention Directive).[178] The objective of the Data Retention Directive was to have data available for the purpose of prevention, investigation, detection, and prosecution of serious crime, including organised crime and terrorism. The CJEU set out 1) that the threshold for interference with Article 7 CFR is not tied to incurring some form of harm, where demonstrating interference is sufficient and 2) that a further infringement would arise when authorities accessed this retained data.[179]

The *essence of privacy* was not affected in this case because the Data Retention Directive obliged Member states to ensure appropriate technical and organisational measures was adopted against accidental or unlawful destruction, accidental loss, or alternation of the data. The interest concerning public security justified the retention of the identified data. Instead, the directive failed on the proportionality analysis because the retained data was not limited to what was strictly necessary.[180] The CJEU concluded that the Data Retention Directive did not lay down clear and precise rules governing the extent of interreference in order to ensure that it was limited to what was strictly necessary.[181] The directive required retention for a period of between six and 24 months, of traffic data which affected the rights of practically the entire European population.[182] CJEU pointed to the likelihood that these activities would 'generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance'. [183]

In *Tele 2*, national Member state law that required the retention of data by telecom operators for law enforcement purposes was challenged.[184] Similarly,

[177] Kranenborg (n 172) 284.

[178] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd V. Minister for Communications (Digital Rights).*

[179] Mangan (n 70) 162.

[180] Ibid 174.

[181] Kranenborg (n 172) 285.

[182] Mangan (n 70) 194.

[183] *Digital rights,* para 37.

[184] Joined Cases C-203/15 and C-698/15 *Tele 2 Sweden and Watson (Tele 2)* ECLI:EU:C:2016:970.

to *digital rights,* the CJEU found that the essence of privacy was not compromised. The court turned to the proportionality test which the national law failed because the measures exceed what was strictly necessary to serve the objectives of crime detection and prevention.[185] The CJEU further stated, 'The legislation is comprehensive in that it affects all persons using electronic communications services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings.'[186] Regarding the seriousness of interference, the court concluded that the access to data which allowed precis conclusions to be drawn concerning the private lives of the persons concerning in the area of law enforcement, the only objective of fighting serious crimes was capable of justifying such access. Moreover, the CJEU set out substantive and procedural conditions that should be in place for the retention of the data and the subsequent access to it by LEA. The court considered that, among others, the retention as a preventative measure should be targeted, based on an objective criterion that establish a connection between the data retained and the objective pursued. Additionally, there should be security measures in place which protects the data against the risk of misuse and against unlawful access.[187]

Ministerio fiscal was a follow up to *Tele 2,* which also concerned national legislation requiring retention of data by telecoms operators for law enforcement purposes. The CJEU concluded that the objective pursued by a measure must be proportionate to the seriousness of interference with the fundamental rights in question. The data the LEA accessed was only aimed at identifying the owner of a sim card and not the communication as such. In relation to these circumstances, the CJEU considered that the interference by such access was not serious and that such access was capable of being justified by the objective of preventing, investigating, detecting, and prosecuting criminal offences generally.[188]

In *privacy international* and *La quadrature du net ao* the CJEU was asked to clarify its ruling in *Tele 2.*[189] Many Member states wanted that the CJEU should adjust its case law, particularly the parts concerning data retention. Despite this, the court confirmed its position in *Tele 2,* by insist on a targeted nature of a preventative retention measure.[190] The CJEU found that generalised and indiscriminate retention of telecommunications meta data for a limited period of time, when there are sufficiently solid grounds for considering that a Member states are confronted with serious threat to national security that proves to be genuine and present or foreseeable.

---

[185] Mangan (n 70) 162.

[186] *Tele 2*, para 45.

[187] Kranenborg (n 172) 285.

[188] *Case C-207/16, Ministerio Fiscal* [2018] ECLI:EU:C:2018:335.

[189] Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net ao* [2020] ECLI:EU:C:2020:790.

[190] C-623/17 *Privacy international* ECLI:EU:C: 2020:790.

The court considered that generalised and indiscriminate retention of only IP addresses assigned to the source of communication for a limited period was acceptable, and generalised and indiscriminate retention of data relating to the civil identity of users. The court did not exclude measures that allow recourse to the expedited retention of metadata 'quick freeze' already lawful kept by providers in order to shed light on serious criminal offences or attacks on national security where such offences or attacks have already been established or their existence may reasonably be suspected. The CJEU also states that it must strike a fair balance between the different positive obligations to combat criminal offences against, among others, minors and other vulnerable persons and the various interests and rights at issue. These positive obligations stem from case law from the ECtHR and Articles 3,4,7 CFR.[191]

In the three cases *SpaceNet, Dwyer* and *VD and SR* the CJEU mainly reiterated its own applicable case law on the retention of and access to traffic and location data.[192] In both the *Graham Dwyer* and *SpaceNe*t the CJEU found that in *La quadrature du Net* a hierarchy was clearly settled amongst objectives of public interest which may justify a measure taken pursuant to Article 15 (1) of the e-Privacy Directive. This hierarchy points out that fighting against serious crime is of a lesser importance than safeguarding national security. Additionally, the CJEU found that 'the general and indiscriminate retention of traffic and location data for the purposes of combating serious crimes exceeds the limits of what is strictly necessary'.[193]

In *SpaceNet* actions was brought to the CJEU challenging the obligation imposed of national law on telecommunications to retain traffic and location data relating to their customers telecommunications, in particularly regarding the fact that the retention was shorter (4-10 weeks) and concerned fewer data than the CJEU's previously judgements. The CJEU confirmed its previous case law that EU law prevents national legislation which provides, on a preventative basis, for the purposes of fighting serious crime and preventing threats to public security, for the general and indiscriminate retention of traffic and location data. The court found that the set of traffic and location data retained may allow very precise conclusions to be drawn concerning the private lives of the persons whose data are retained. For instance, behaviours of everyday life, permanent or temporary places of house, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them and enable a profile of those persons to be established.[194]

[191] *La quadrature du net,* para 78.

[192] Joined Cases C-793/19 and C-794/19 SpaceNet [2022] ECLI:EU:C:2022:123; Case C-140/20 *Graham Dwyer V Commissioner of AN Garda Síochána and ors* [2022] ECLI:EU:C:2022:456; joined Cases C-339/20 and C-397/20 *VD and SR* [2022] ECLI:EU:C:2022:789.

[193] *La quadrature du net*, para 117.

[194] *Spacenet* para 117.

The safeguards provided for by the national law intended to protect the retained data against the risks of abuse and against any unlawful access, the court point out that the retention of an access to those data constitute separate interreference with the fundamental rights of people concerned, requiring a separated justification. It follows that national legislation ensuring full respect for the conditions established by case law as regards access to retained data cannot, by its very nature, be capable of either limiting or even remedying the serious interference with the rights of the persons concerned which results from the general retention of those data.[195]

In *Dwyer* the validity of national legislation was challenged that required mobile phone data to be retained and disclosed to the police on request. The court stated that "The objective of combating serious crime, as fundamental as it may be, does not, in itself, justify a measure providing for the general and indiscriminate retention of all traffic and location data" and also recalled that authorities have positive obligations to 'protect private and family life, home and communications, and also the protection of the individual's physical and mental integrity, and the prohibition of torture and inhuman and degrading treatment'. In this case, the CJEU gave conditions set out in its judgement that are enacted to combat serious crimes/and or prevent serious threats to public security related to measures providing for targeted retention, expedited retention or retention of IP addresses. For instance, a geographical criterion in places that highly receive a very high volume of visitors but also the average crime rate in a geographical area.[196]

In *Opinion 1/15* (*EU-Canda PNR agreement*) confronted the type of wide-ranging collection, retention and sharing of data seen in the *Digital rights* and *Schrems* decisions (Although predating *Schrems*). The circumstances related to data transferred from EU to Canadian authorities. In this decision, the essence of privacy was not interference with because to ensure public security, the measure revealed limited information concerning the individual's private life and this data was restricted to air travel between the EU and Canada. However, the agreement went beyond what was strictly necessary as the articulation of data lacked precision; numerous reasons pertaining to the collection, retention, and disclosure of data.[197]

In *Schrems (Safe harbour agreement) an* agreement between the EU and US regarding third-country transfers (from the EU to US) was deemed to be invalided. [198] In comparison *digital rights* and *Tele 2,* the CJEU found that the essence of privacy was compromised and did not move on to a proportionality

[195] Xavier Tracol, 'The joined cases of Dwyer, SpaceNet and VD and SR before the European Court of Justice: The Judgements of the Grand Chamber about data retention continue falling on deaf ears in Member states' (2023) 48 Computer Law and Security Review 7.

[196] Ibid 4.

[197] Mangan (n 70) 188.

[198] C-362/15 *Maximilian Schrems v Data protection Commissioner (schrems)* [2015] ECLI:EU:C:2015:650.

analysis and put great emphasis on Article 7 CFR. The CJEU based its arguments on that the legislation allowed public authorities to have access on a general basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life. Additionally, the agreement failed to establish any possibility for an individual to pursue legal remedies to have access to personal data relating to him, or to obtain the rectification or reassure of such data or the absence of any legislation providing for a remedy does not respect the right to effective judicial protection as enshrined in Article 47 CFR.[199]

In the *Privacy shield decision (Schrems II),* the successor agreement to Safe harbour was also declared invalid.[200] The decision focused on the lack of safeguards, including the absence of limitations on the power to implement surveillance or guarantees for persons target by these programmes, the lack of actionable rights in courts before US authorities for data subjects and the failure to delimit in a sufficient clear and precise way the scope of such bulk collection of personal data. Scholars argue that these reasons tied together Article 7,8 and 47 CFR.[201]

Writing extra-judicially, President Lenaert argued that the CJEU's decision regarding information technology deploys a particular approach regarding the essence of the right, (which cannot be eliminated) followed by a proportionality analysis. Thus, the essence of which right may shift (*compare Shrems* and *Privacy Shield*) depending upon the circumstances before the CJEU.[202]

Wilman argues that EU general legal rules on the internet appears to be emerging concerning that online service providers may in principle not be made subject to an obligation of generalised and indiscriminate retention. Wilman argues that the rule is founded in EU secondary law but have to a large extent been constructed by the CJEU in rather extensive and controversial lines of case law, in the light of the CFR. Wilman bases his argument on the cases concerning *digital rights, tele2 and la quadrature du net aoe.* Due to Article 7's fundamental nature, the rules could be seen as an emerging general principle of EU internet law. Wilman argues that it's clear from the CJEU's case law that 'not everybody using online services can be treated as if he or she were a suspect'. However, Wilman continues that the CJEU accepts *"collateral damage"* in such ways that the fundamental rights of great amount of individuals may be interference with to some extent when it's necessary, for instance targeted retention that is based on the geographic criteria. But at the same time, linked in direct or a remote one is needed. Wilman

[199] Mangan (n 70) 187.

[200] C-311/18 Data Protection Commissioner V Facebook Ireland Ltd and Maximillian *Schrems (Schrems II)* [2020] QBECLI:EU:C: 2020:559.

[201] Mangan (n 70) 186.

[202] Koen Lenaerts, 'Limits on Limitations: The essence of Fundamental Rights in the EU' (2019) 20 German Law Journal 782.

emphasises that the prohibition is all about striking a fair balance, which requires a degree of give and take on both sides of the equation. [203]

4.3.3 Special protection for children?

Nevertheless, scholars are of the impression that the ECtHR and CJEU in the nearest future are going to see more cases relating to child privacy issues in the future. Except from *K.U V Finland*, the jurisprudence from the courts concerning children's privacy have been few, especially concerning the digital environment.[204] The ECtHR has not so far considered any data-processing cases where violations of a children's privacy are at issue.[205] Although there are some cases concerning *information disclosure,* which resembles with data processing.

In *Avilkina and others V.Russia,* confidential medical information about the applicants including a minor was disclosed by a medical facility following a request by the prosecutor's office. The court stated that the protection of personal data, including medical information, is of fundamental importance to a person's enjoyment of their right to respect for his/her private and family life, guaranteed by Article 8 ECHR. Furthermore, the court also stated that the disclosure of such data may seriously affect a individuals enjoyment of their private and family life, as well as their social employment situations by exposing them to opprobrium and the risk of ostracism.[206] The court also stated that the interest of a patient and the community as a whole in protecting the confidentiality of medical data may be outweighed by the interest of investigation and prosecuting crime and in the publicity of court proceedings, where such interest are shown to be of even greater importance.[207]

The issue of a child's reputation in the context of information disclosure was considered in *Aleksey Ovichinnikov v. Russia.* The court stated that in certain circumstances a restriction on reproducing information that has already entered the public domain may be justified. The case has been viewed as important by scholars because it confirms that a child's privacy must be protected, not only in cases of a potential safety threat, but also with the aim of respecting his/her reputation. Scholars argue that this is in line with Article 16 of the UNRC.[208]

Hiljke argues that special protection of privacy is given to children in the broad and dynamic sphere, supporting the claim with two cases. Firstly, in *K.U v. Finland* the applicant was the subject of an advertisement of a sexual

[203] FG Wilman 'Two Emerging Principles of EU Internet Law: a Comparative Analysis of the Prohibitions of General Data Retention and General Monitioring Obligations' (2022) 46 Computer Law & Security review 9.

[204] Also discussed in chapter 4.2.2.2.

[205] Kravchuk (n 56) 106.

[206] Ibid 107.

[207] *Avilkina and others v. Russia* (2013) (App no. 1585/09).

[208] Kravchuk (n 56) 107; *Aleksey Ovichinnikov v. Russia* [2010] (App no. 24061/04).

nature on an internet dating site when the child only was 12 years old. In *S. and Marper v. UK* was protection given children as a vulnerable group; retention of biometric data was especially harmful in the case of minors.[209]

4.4 Discussion

This chapter started with account the best interest of the child's principle. Under what circumstances the child's best interests should be a paramount or 'one of many' primary considerations remain unclear in relation to the case law from the CJEU and ECtHR. This issue is further enhanced by the lack of case law creating a substantive 'norms' that may guide the decision-making in different fields of legal situations.

The practical outcome whether the best principle of a child should be understood as a paramount or 'one of many' primary considerations might play a vital outcome for the decision-making, especially since the CFR and the case law is silent regarding conflicting rights dilemmas in where (children's) rights are at stake. However, the best interest of a child principle might also be described as an EU general legal principle; that is interpretative, gap-filling that and enables the development of EU law, which might in certain cases speak for a disruptive outcome in favor for children's right. Moreover, the caustic approach by the CJEU have its benefits, for instance that it contains a level of generality and abstraction, making it flexible for consider all children and their differently maturity and development. Although other scholars are unhave put forward those arguments regarding children's rights rarely is disruptive, rather confirming and supporting the application of existing law.

If a case relating to the privacy of children and protection from sexual exploitation (harm) was brought up to the CJEU, its difficult (due to lack of insufficient case law and the character of the principle of best interest of the child) to assess how the balance would play out. At the one hand, children have a strong protection from ill-harm accordingly to the ECtHR case law and potentially as an EU legal general principle. Their protection has also put positive obligations on states, which is also reaffirmed in case law from the CJEU.

At the other hand, many cases regarding privacy and information technologies have been brought up to CJEU, in where they have played as strong defenders of privacy and data protection. The CJEU have even been so strong defenders that discussions about an emerging EU legal principle have been brought up to the table.

Notably, the case law does not prohibit data retention as such, or even mass collection of data. The case law rather shows that the essence of privacy has

[209] Hijmans (n 38) 47; *Marper v. UK* [2008] (App no 30562/04 and 30566/04); *K.U. v. Finland* [2008] (App no. 2872/02).

not been interfered with and the objectives brought up to the court have been justified, although the measures concerned have failed to comply with the CJEU proportionality analysis. The proportionality test has deemed factors such as long retention time, traffic and location data, insufficient safeguards and the lack of an effective remedy as exceeding over what is considered necessary (and proportionally). Importantly, it follows that under 'right' circumstances or what Willman argues as 'collateral damage' crime prevention online may occur, although the hierarchy set out in La quadrature concerning justified targeted data retention (in a digital context) for crime preventative purposes may be difficult to transform into the digital environment because the character of the internet is fluid.

Concerning the analogy of the ECtHR's Case law, *Avilkina and Others V. Russia* recognises the value of undisclosed information concerning private life in relation to children but that it under certain circumstances also may be outweighed in relation inter alia, crime prevention. This analogy supports the idea of child privacy being outweighed by crime prevention interests but are also in line with the criticism of overweight of protection incitements under the ECtHR. Meanwhile *Aleksey Ovichinnikiova V.Russia* shows a 'child-friendly' approach to privacy and children's own *autonomy* and the connection to the UNCRC Article 16 (despite the criticism of ECtHR lacking participatory rights). However, both cases support the idea of child privacy.

5 The EU proposal to combat child sexual abuse

5.1 General overview

The objectives of this chapter are twofold: firstly, to provide a general overview of the proposal, and secondly to examine the criticisms raised by scholars and rights organisations against the proposal. The critique revolves around arguments concerning human rights to privacy in general, rather than specifically focusing on children's right to privacy.[210] Nevertheless, these arguments can be used as a valuable foundation for initiating discussions pertaining to children's rights. Relevant case law from the CJEU is to be assessed in relation to the draft regulation to develop and nuance scholarly arguments. The chapter ends with some suggestions of improvement that scholars have suggested concerning the proposal specifically.

On the 11 May 2022 the European Commission issued a Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat the serious crime of child sexual abuse.[211] This proposal seeks to permanently replace the temporary Interim Regulation and regulates issues that are on the crossroad of several existing instrument concerning privacy: GDPR, e-Privacy Directive and the DSA.[212]

The proposal seeks to protect the rights of children, concerning their fundamental right to human dignity, to the integrity of the person, the prohibition of inhuman or degrading treatment and the rights of the child.[213] The explanatory memorandum of the proposal it acknowledges earlier legislation prohibits general monitoring obligations on intermediaries. The proposal acknowledges that information society services have become very important for many aspects of present-day life, including children but also for perpetrators of child sexual abuses**.** The proposal explicitly refers to the UNCRC and Article 24(2) CFR, and that children's rights must be equally protected equally protected in the digital environment. After that, the recitals highlight that the protection of children, both offline and online is a union priority.[214]

---

[210] Some parts of the draft regulation have not been particularly criticised, for instance the issue of removal as it regards specific stored content and are technically and legally objectionable, see Matthias Bäcker and Ulf Buermeyer 'Comments on the planned obligations of internet service providers to combat sexualised violence against children (so-called chat control regulation)' *Verfassungdsblog* (18 August 2022)< https://verfassungsblog.de/my-spy-is-always-with-me/> Accessed 20 March 2023.

[211] Theresa Quintel, 'The Commission Proposal on Combatting Child Sexual Abuse" – Confidentiality of Communications at risk?' (2022) 8 EUR data Prot L rev 262

[212] See chapter 3.

[213]Explanatory memorandum, COM (2022) 209 final.

[214] Explanatory memorandum, COM (2022) 209 final.

In short, the proposal obliges providers of hosting services and providers of interpersonal communications services to assess and mitigate the risk of any misuse from their users (including children) on their services for online child sexual abuse purposes. If a residual risk remains after the providers have implemented the mitigating measures, providers could be ordered by national judicial authorities to detect, report, remove, or block access to child sexual abuse material (CSAM). Moreover, the proposed regulation obliges providers to report identified CSAM when they become aware of it to a newly established EU centre on Child Sexual Abuse (EU centre).[215] The proposal highlights that its essential that coordinating authorities should be fully independent. [216]

The proposed regulation targets four types of service providers. Firstly, it targets hosting services that store information on behalf of users and that often makes it available to third parties. Social media is included, such as Facebook, Twitter and Instagram. Secondly, it targets interpersonal communications services that are enabling the direct exchange of information between selected individuals. For example, e-mail services or instant messengers like WhatsApp or Signal. Thirdly, it targets software applications stores and internet access services.[217]

The draft regulation contains several procedural safeguards regarding to mitigate the risks of over blocking, guarantee transparency and legal protection. The EU Centre is also an important actor as it's a control body lacking any operational powers within the framework of the reporting procedure. The body is thought to do a plausibility check which may reduce the risk of false positives hits the detection system that creates severe consequences for the users concerned.[218]

5.2 Concerns regarding the proposal

5.2.1 General and indiscriminate detection orders

The *effectiveness* of the draft regulation in relation to interpersonal communication services is questioned by academics. According to the EU legislator, the rules apply only to providers of certain types of online services that have proven to be vulnerable to misuse for the purposes of spreading CSAM or solicitation (i.e., grooming).[219] Scholars also highlights that in relation to the proposals effectiveness there is also important to note that certain forums on which CSAM are being uploaded to will not fall within the scope of the proposal. Political pressures are needed on the states hosting the forums to tackle

[215] Quintel (n 212) 262.
[216] Recital 46 COM (2022) 209 final.
[217] Bäcker and Buermeyer (n 211).
[218] Quintel (n 212) 266.
[219] Explanatory memorandum,COM (2022) 209 final.

the problem.[220] Furthermore, the effectiveness on the proposal might not be established in all cases because the majority of CSAM is shared via platforms and forums and the illegal content remains online under a significant time period. [221]

Quintel question whether detection obligations are going to be carried out in a *targeted manner*. Upon the request of the coordinating authority of establishment i.e., the Member state authority primarily responsible for enforcing the regulation, a court or an independent administrative authority can impose further obligations on service providers by issuing an order to detect online child sexual abuse. The detection order may only be issued if the accompanying requirements that ensuring transparency and effective redress are meet.[222] The detection orders are issued if there is a *significant risk* that a service is used for online child abuse. What constitutes a significant risk in relation to the spread of known and unknown CSAM is described as 'appreciable extent for the dissemination of new child sexual abuse', despite any mitigation measures the provider may have taken or will take.[223]

Tuchtfeld argues that as the proposal does not focus on 'whether a service is used to a significant *extent* for child abuse, but whether there is a significant risk (regardless of the extent) of such use'. Tuchtfeld argues that the focus applied is going to result in that almost all usual available digital means of communication are likely to receive detection orders.[224]

Quintel have put forward a different argument relating to 'significant risk', namely that detection orders theoretically could be continuously renewed and thus result in a permanent scanning of communications. Quintel highlights that even if the steps to issue detection may look burdensome, the practical outcome may be quite straightforward. This due to the national implementation and which authorities that will be designated to be Coordinating authorities in the individual Member states.[225]

The EDPB and EDPS emphasis that 'a complex system of escalation from risk assessment and mitigation measures to a detection order cannot replace the required clarity of the substantive obligations' and that potential abuse may occur as a result of the absence of clear substantive norms. For instance,

---

[220] Quintel (n 212) 270.

[221] The European Data Protection Board and The European Data Protection Supervisor, 'Joint Opinion 04/2022 on the Proposal of the European Parliament and of the Council Laying down rules to prevent and combat child sexual abuse' (2022).

[222] Article 7 COM (2022) 209 final.

[223] Article 7 COM (2022) 209 final.

[224] Erik Tuchtfeld, 'Thank you very much, your mail is perfectly fine' (Verfassungsblog 18 August 2022) <https://verfassungsblog.de/thank-you-very-much-your-mail-is-perfectly-fine/> accessed 21 may 2023.

[225] Quintel (n 212) 270.

the notion of 'significant risk' leaves the Member states with a broad margin of appreciation and legal uncertainty of how the right should be balanced.[226]

Irrespectively of how the services became aware of the CSAM they must report the content concerned to the EU Centre. In other words, it includes both the content that the services collected because of its own risk management or because of a detection order. However, as soon as messages that are not manifestly unfounded are detected (automatically) they will first be forwarded to the EU Centre. After that, if the suspicion is confirmed (how remains unclear), to Europol or national security authorities.[227] Scholars therefore raises concerns about messages being forwarded on a regular (general) basis rather than on an exceptional basis. [228]

Quintel argues that CSAM today could be removed from service providers by other available means and from more relevant sources. She suggests preventative methods, like detecting harmful behaviour by analysing metadata and for instance preventing the distribution of CSAM by banning certain users from accessing the relevant services. Quintel argues that where CSAM could be identified by *less intrusive means,* the provisions in the draft regulation would not fulfil the necessity requirement.[229]

5.2.2 Depictions of sexualised violence

The detection orders impose an obligation on interpersonal communications service and hosting service providers to actively search for CSAM. The detection order may concern three types of content. Hosting services must actively search for already known depictions of sexualised violence as well as unknown depictions of sexualised violence. Beyond that, interpersonal services must also actively search for solicitation of children for sexual purposes.[230]

Providers of hosting services and providers of interpersonal communication services that have received a detection order shall execute it by installing and operating technologies to detect the dissemination of known or new CSAM.[231] The EU Centre is to provide them with detection technology, such as databases of indicators, without any costs.[232] The EU legislator withholds

[226] The European Data Protection Board and The European Data Protection Supervisor, 'Joint Opinion 04/2022 on the Proposal of the European Parliament and of the Council Laying down rules to prevent and combat child sexual abuse' (2022)

[227] Article 12 and 48 COM (2022) 209 final.

[228] Tuchtfeld (n 225).

[229] Quintel (n 212) 271.

[230] Bäcker and Buermeyer (n 211).

[231] Article 10.1 COM (2022) 209 final.

[232] Article 44 COM (2022) 209 final.

that detection must be based on the indicators by the EU centre, irrespectively the choice of technology the providers choose.[233]

Rojszack underlines (thus in relation to the Interim Regulation) that the EU legislator in principle have not exclude any technical means used to identify illegal material. Moreover, Rojszack emphasises that there is an analysis of the provisions in the proposal that shows that the legislature has created framework for service providers to develop a use new ways of user surveillance which would be more effective in detecting infringement. Rojszack adds 'it is worth bearing in mind that even the most legitimate aim cannot justify the introduction of a widespread system of surveillance, not to mention one operated under the supervision of public authorities.'[234]

Nevertheless, the proposal sets out certain requirements regarding the technologies used for detecting dissemination for unknown CSAM and behaviours that signalises solicitation of children for sexual purposes. The proposal encourages a 'technological neutral approach' and give providers the responsibility deploy the most effective and less intrusive technical means to execute detection orders.[235] The technique must at the same time only use information strictly necessary to identify patterns pointing to grooming or CSAM.[236] Furthermore, the technologies used must also be adequate trustworthy in that they are limited to the maximum extent possible rates of false positives regarding detection.[237] The providers must perform any necessary review on an anonymous basis and take steps to identify users in case potential CSAM is detected.[238]

Despite these requirements set out in law concerning the technique used, scholars are concerned of the technique used to detect known and unknown depictions of sexualised violence. After considering state of the art and the foreseeable state of the art, scholars argue that there are two possible technical implementations today. The two possible technical implementations are hash value-based removal of known depictions of sexualised violence and self-learning algorithms concerning unknown CSAM. [239]

Hash values are often used regarding the identification of already known depictions of sexualised violence. Hash values are like a digital footprint that originates from a file. It is not possible to compute the underlying file from the hash value. Detection based on hash values works by comparing the hash

[233] Explanatory memorandum, COM (2022) 209 final.

[234] Although this argument relates to the interim proposal, there is no difference regarding the statement as the proposal and the interim regulation do not regulate the issue.

[235] Recital 26 COM (2022) 209 final.

[236] Article 10(3)c COM (2022) 209 final.

[237] Article 10(3)d COM (2022) 209 final.

[238] Explanatory memorandum, COM (2022) 209 final.

[239] Article 10(3)d COM (2022) 209 final.

values from a file present on the hosting service with hash values of known depictions from the indicators from the EU Centre. Perceptual hashing is used to still recognise pictures after minor changes such as size or colouring. However, a disadvantage with perceptual hashing is that its prone of false positives since it does not calculate the hash values from the entire file but only of structural properties of the picture.[240]

Self-learning algorithms could be used to automatically detect unknown depictions of sexualised violence. Algorithms identify patterns in training data and apply the patterns on the content located at the hosting services. This type of technology is susceptible to false positives because with today's technology evaluation of contextual elements are often proved to be inadequate. Consequently, important balancing operations of conflicting values, production and distribution are not made. However, the false positives may be reduced with refined technology but are not likely to be eliminated. [241]

Scholars have highlighted that the precision of the detection system may have an impact on the right to confidential communications. In the impact assessment regarding the draft regulation, it is unclear of how the results of already existing detection systems of sexual violence was made. Therefore, is it hard to draw any conclusions of how many false positives the draft regulation through the indicators may create. [242]

Automatic detection of infringement has previously been discussed in society and legal doctrines regarding the implementation of a provision in the Copyright in the Digital Single Market Directive (EU) 2019/790 (CDSM Directive). The provision obliged certain hosting service providers to ensure that certain copy-right protected works would not be available on their platforms or not uploaded to the platforms. The case concerned how Article 15(1) e-Commerce Directive should be interpretated.[243] The requirement could only be implemented through automatic filtering systems.[244]

The Court of Justice of the European Union approved the controversial provision in the CDSM Directive by referring to the safeguards implemented in the directive in *Poland V. European Parliament and Council*.[245] The implemented safeguards were for instance provisions that mitigate the risks of over blocking and complaint mechanisms. The court also stated that services providers only are required to detect and block content that has been designated

[240] Bäcker and Buermeyer (n 211).
[241] Ibid.
[242] Ibid.
[243] See chapter 3.
[244] Bäcker and Buermeyer (n 211).
[245] Case C-401/19 *Poland V. European Parliament and Council* [2022] ECLI:EU:C:2022:297.

by them by the rights holders. If the services providers are needed to assess the lawfulness of the content through a detailed legal examination based on copyrights rules, they are not required to block the content. The CJEU stated that the provision 'provides an additional safeguard for ensuring that the right to freedom of expression and information of users of online content-sharing services is observed that this means that 'the providers of those services cannot be required to prevent the uploading and making available to the public of content which, in order to be found unlawful, would require an independent assessment of the content by them'. [246] There are also procedural safeguards to protect the confidentiality of communication inherent in the CDSM-Directive.[247]

The automatic filtering technology used to achieve the aim is very similar to the technology used to discover sexual violence. Bäcker and Buyermeier deems the provisions in the proposal concerning the use of hash values as legitimate because the proposal also contains technical and procedural requirements to reduce the risk of excessive detection, ensure transparency and legal protection. Thus, only in relation to known CSAM on hosting service providers because it wouldn't violate any reasonable expectations on confidential communication. Concerning new CSAM, Bäcker and Buyermeier argues that unknown CSAM only are permissible if their detection systems have high precision supported by robust findings with ongoing evaluations throughout the usage. This because of contextualisation and balancing problems. Furthermore, that the use of sufficiently precise system is mandatory for service providers. This may lead to the result that certain unknown content (content that are more likely to be identified more precisely) only are searched for. Scholars particularly highlight that there should be a predefined threshold of false positives outcomes within a defined time window and if the practical usage falls under the threshold the scanning must be withdrawn. [248]

Nevertheless, this is not the first time the CJEU touched upon how Article 15(1) e-Commerce Directive should be interpretated. In *L'Oréal v. eBay* the CJEU stated, 'that the measures required of the online service provider concerned cannot consist in an active monitoring of all the data of each of its customers in order to prevent any future infringement of intellectual property rights via that provider's website'. [249]

The issue of interpretating 15(1) e-Commerce Directive have been brought up to the court several times regarding impact on different fundamental rights. Wilman argues that the case law following up until *Poland V. European*

[246] Bäcker and Buermeyer (n 211).
[247] Bäcker and Buermeyer (n 211).
[248] Wilman (n 204) 4.
[249] Ibid 6; Case C-324/09 *L'Oréal v. eBay* [2011] ECLI:EU:C:2011:474.

Parliament and Council is a bit unclear regarding what the provision aims to achieve and how it should be interpretated. Wilson emphasises that CJEU have shifted focus from at the one hand the service providers interests, and on the other hand, the user's rights. Wilson states that it is realistic to conclude that the clause is not only about protecting the rights of the persons harmed by illegal online content and of the service providers concerned. Instead, the most recent rulings seem to confirm what the previous case law suggested: That the provision also seeks to protect the rights of the users of the services.[250]

Wilman continues that there is an emerging general rule on EU internet law concerning services providers are not made subject to general obligations to monitor the data they transmit or store for their users. The argument is based on the fact that the rule has been founded in secondary EU law and have to a great extent been constructed by CJEU in the light of the rights set out in the CFR.[251]

5.2.3 Solicitation of children for sexual purposes

Detection orders for interpersonal communication also target solicitation of children for sexual purposes i.e., grooming. The detection systems services providers use is needed to both identify and examine communication between people. The examination requires a complex assessment of the content and context of the communication to find sufficiently substantiated indications of grooming. Bäcker and Buyermeyer are doubtful whether a sufficient level of precision can be achieved in the nearest future and arguing that the available technique today would result in that most classifications are likely to be false positives. The EDPB and the EDPS want to have the provisions concerning grooming removed due to their intrusiveness.[252]

Many voices out of a fundamental rights perspective have been raised regarding the provision as they argue it breaches the confidentiality of communications and that the EU-legislator 'treads on unchartered territory'. Compared to the providers of hosting services where the content is meant for the general public and are targeted to an undefined number of people, the communication on interpersonal communication services meant to be kept private. The hosting service providers knowledge and analysis of the stored content does not undermine any reasonable expectations of privacy, as it would regarding interpersonal communication services.[253]

[250] Wilman (n 204) 5.
[251] Wilman (n 204) 6.
[252] Recital 57 COM (2022) 209 final.
[253] Bäcker and Buermeyer (n 211).

The Commission refers to end-to-end encryption as an 'important tool to guarantee the security and confidentiality of communications of users, including those of children'.[254] Tutchfelt argues that it unmanageable for interpersonal communications not to circumvent end-to-end encryption to follow the imposed obligation, which results in that end-to-end encryption becomes obsolete.[255] Bäcker and Buyermeyer continues that it places a disincentive for service providers to use end-to-end encryption and what type of detection mechanism that being implemented various in their depth of intrusion, although the vital problem still is that hits are reported to an authority without (initially) informing the concerned individuals.[256] The EDPB and EDPS have also raised similar concerns about the impact on encryption.[257]

Moreover, the detection order requires, if not restricted to groups or users, the entire traffic on the interpersonal services to be reviewed for CSAM irrespectively of what technology used to actively search for grooming. As a result, scholars maintain that a detection obligation related to the communications on the entire service in practise mean a comprehensive scanning of all chats histories, irrespectively of a probable cause against individual persons. The practical outcome of scanning of all chat histories is therefore conceived as a total monitoring of certain files or the whole traffic on the interpersonal services (both grooming and images/movies), which breaches fundamental human rights.[258]

Scholars argue that a comparison of bulk surveillance and the practical outcome of the provisions concerning detection obligations on interpersonal communications services providers shows many similarities. Bulk surveillance (strategic telecommunications surveillance) is conducted by intelligence services in European Union for the purposes of foreign reconnaissance purposes.[259]

5.3 General concerns

Tuchfelt argues that when allowing these types of technique, the margin left for intensifying the act of surveillance would be to change the type of content the data bases is looking for, for instance terrorism, organised crime and face news. Moreover, Tuchfelt also argue about chilling effects on user participation beyond the area of private life.[260]

[254] Recital 26 COM (2022) 209 final.
[255] Tuchtfeld (n 225).
[256] Bäcker and Buermeyer (n 211).
[257] Ibid.
[258] Ibid.
[259] These cases have previously been discussed in chapter 4.
[260] Tuchtfeld (n 225).

The proposal also referred to *La quadrature du Net aoe* as following 'In connection to combating criminal offences against minors, the Court of Justice of the EU has noted that at least some of the fundamental rights mentioned can give rise to positive obligations of the relevant public authorities, including the EU legislature, requiring them to adopt legal measures to protect the rights in question'. Tuchfelt argues that is 'precisely the existence of these obligations to protect that makes the draft a scandal'. Tuchfelt base his argument on that although it's recognized that children have a right to be protected by the state, the outcome of the case was that the laws on bulk data retention was considered disproportionate and emphasizes that there 'is no indication that the CJEU will come to another conclusion.'[261]

[261] Tuchtfeld (n 225).

6 The balance between the two fundamental rights

The theoretical starting point of this thesis was to consider privacy as a 'part and parcel' for children's participatory rights online or as a prism in which when lights being shed on shows a spectrum of participatory rights. Chapter 2 pointed out that soft law and scholars advocates a holistic approach, meanwhile a review of legislation showed us that a protectionist approach was expressed. The balance between children's right to protection and privacy in case law is difficult to grasp, because of the principle of best interest of the child and the insufficient case law concerning children's rights.

When comparing policies, legal doctrines, legislation, and case law regarding the best interest of the child in a digital context, it seems that the principle only applicable on a case-by-case basis and lacks substantive value. This makes it difficult to understand how the best interest of the child principle should play out in rulings, especially in rights conflicts. The CFR nor the case law give guidance.

However, some guidance could be found in the UNCRC regarding the conflict of fundamental rights. The general Comment states: 'If harmonisation is not possible, authorities and decision-makers will have to analyse and weights the rights of all those concerned, bearing in mind that the right of the child to have his or her best interest taken, high priority', but the question of what happens when several children's interests' conflicts against each other is still not answered.[262]

The lack of guidance is of course in the line with the UNCRC other guidelines, namely that the principle 'is dynamic and does not attempt to describe any given situation in any given time'. Nevertheless, there are some tendencies from the CJEU and the ECtHR that could be used to start a discussion 1) presumed interests and 2) The best interest of a child as confirming and supporting interpretation of the existing law.[263] Presumed interest are constructed in the light of social and cultural contexts where the digital environment can be such context. Due to the increasingly pressure on privacy online, perhaps children's digital privacy can be one of the presumed interests too?[264]

Secondly, the tendencies of the CJEU to support and confirm the existing interpretation of applicable law is also difficult to deduce anything from, primarily regarding the principle of best interest of the child as case-by-case applicable. Nevertheless, by taking the argument and consider it in relation of the CJEU recent case law concerning privacy online, one can argue that the

[262] See chapter 2.2.
[263] See chapter 2.2
[264] See chapter 4.2.2.2

CJEU still would be a firm protector of such rights even when protecting children and when the best interest of the children comes at stake.

However, if we consider the best interest of a child as a general principle that has the function to fill out gaps in the EU legal order, interpretate secondary law and serve as a yardstick to test the validity of secondary law while simultaneously, this adds something in the equation. In event of a general principles clash with secondary legislation, this is in favour for a possible disruptive approach in relation to the CJEU strong commitment to respect personal privacy. Moreover, the inconsistencies in ECtHR case law concerning a primary or a paramount consideration of the best interests of the child principle can have a significant impact on the balance, which is further contributed by which and how strong the interest are interpreted to be.[265]

But as a thought experiment, what happens if we take the issues of child protection and individual child privacy to its outer limits? If child protection prevails over privacy: this means that chilling effects may occur, children's participation rights are interreference and opens possibilities for new type of surveillance technique and eventually mass surveillance. At the other way around, if child privacy prevails over child protection this will result in severe harm for children not only once, but potentially many times if the pictures are reproduced, disseminated, and shared all over the internet.

Of course, this is not reasonable to believe is the best interest of the child, especially not when considering that a balance between participation and protection rights as acknowledged by UNCRC and the Article 52 (1) CFR must be struck. This raises questions like how paramount individual privacy is and how much criminality in terms of sexual exploitation is the society is willing to accept for the benefit of safeguarding privacy?

To answer the first research question 'What is the current state of balance between children's fundamental right to privacy and right to protection from sexual exploitation in EU digital spheres?' it can be concluded that there is difficult to draw a balance in case law concerning children's digital right to protection and privacy.

The next research question explores these aforementioned questions because the provisions in the proposal to combat child sexual abuse (aim to protect children) have similarities with circumstances in CJEU previous case law concerning the essence of privacy and the legitimate limitations. These case law have also been considered to constitute emerging EU legal principles on the internet.

[265] Se chapter 4.2.2.2

Firstly, the proposal follows the approach that earlier legislation, namely the protectionist approach.[266] The proposal also follows the obligations imposed by case law from the ECtHR.[267] Thus, this proposal appears to be more balanced because children are mentioned to enjoy the internet in particular and are not only focused on the dangers and children as a vulnerable group.

Although keeping the contextualisation in mind and the aim of the proposal to protect children, the proposal should acknowledge participatory rights in the forms of children's sexual behaviour online. This because the lines are blurred between illegitimate and legitimate sexual conduct and that the proposal tangents on children's digital participatory rights (sexual exploration) remits and their right to privacy. This is not mentioned in the recitals, in contrast to the CSAM-Directive. Moreover, preventative measures concerning monitoring have previously been deemed to be lawful if certain safeguards are meet and if the assessment of lawfulness of the content does not require a detailed legal examination. The contextualisation problem problematises this requirement as well as the different expectations on privacy service providers.[268]

However, Leanarets suggested that there is a special test for privacy concerning information technologies, namely 1) whether the essence of a right is compromised and 2) a proportionality test.[269]

The starting point here is that the CJEU does not allow general indiscriminate retention for the purposes of serious crimes, because of the hierarchy set out in *La Quandrature du Net aoe.* The prohibition on general indiscriminate retention have been tested and reconfirmed several times in the CJEU case law. Nevertheless, targeted retention is deemed to be lawful for the purposes of preventing serious crimes, for instance in relation to geographical targeting. However, as scholars have emphasised, the targeted retention of individuals are difficult because traffic data does not automatically allow for the categorisation of individuals, and it seems difficult to target the transnational digital sphere.[270]

The scholars have many doubts against the proposal that can be summarised as follows: The effectiveness, the targeted actors, the targeted manner (scope and extent), unclear wording, not excluding any technical means, general reporting obligation and strong connection to authorities, not informing individuals, safeguards for monitoring, chilling effects, statement in la quadrature and the entire traffic. [271]

[266] Se chapter 2.5
[267] Se chapter 4.2.2.2
[268] Se chapter 5.2.2
[269] Se chapter 4.3.2
[270] Se chapter 4.3.2
[271] Se chapter 4.3.2

The ‘essence of privacy’ can be interfered with if the authorities have access on a general basis to the content and if there is no possibility for an individual to pursue legal remedies to have access to personal data relating to him.[272] It seems possible when considering the critics arguments of that the scope and extent of the detection order may be renewed and applied to all services due to the unclear word of ‘significant effect’. Moreover, that individuals not at the initial stage are informed is an argument relating to remedies, because if an individual not aware of what the individual have being accused of it is hard to seek remedy. Besides, the close cooperation with Europol and the general reporting obligation makes the content easily go to the authorities. Thus, there are safeguards inherent in the proposal that seeks to address these issues, such as the EU Centre roles to do a plausibility check on the content. [273]

Moreover, it also seems (more) conceivable that even if the proposal survives the ‘essence of privacy test’ it might fall on the proportionality test when considering the critics arguments. Firstly, because the effectiveness is questioned and that there are other less intrusive measures to consider. Secondly, because the CJEU in *Dwyer* have deemed national legislation illegal concerning traffic and location data with a retention period of 4-10 weeks, meanwhile in the proposal the retention period is 6-24 months and concerns the actual communication and messages regarding the new unchartered water of interpersonal services. [274]

To answer the question of ‘how (to what extent) does the EU proposal to combat child sexual abuse online impact the balance between children’s fundamental right to privacy and right to protection online in transnational digital spheres?’ It seems conceivable, with the current case law in mind and if the criticism is valid, that if the proposal is considered lawful it would have a significant impact the current ‘adult’ balance regarding privacy and children’s protection. Perhaps even on the essence of privacy.

Concerning the impact on the balancing on children’s rights, there are statements, recitals and case law that are in favour that children merit extra protection of their privacy online. But there is also case law that stated that investigating crimes (in general) can prevail over children privacy. However, as children are bearers of all rights as adults, they are entitled at least the same rights as adult and as for now, the same conclusion must be drawn here.

[272] Se chapter 4.3.2
[273] Se chapter 4.3.2
[274] Se chapter 4.3.2

Bibliography

Primary Sources

Consolidated version of the Treaty on European Union [2016] OJ C 202/1.

Charter of Fundamental Rights of the European Union [2016] OJ C 202/1.

European Convention on Human Rights [1950].

United Nations Convention on the Rights of the Child [1989].

Treaty on the Functioning of the European Union [2016] The Treaty on the Functioning of the European Union OJ 202/01.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) [2000] OJ L 178/1.

Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography (CSAM-Directive) [2011] OJ L 335/1.

Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA [2017] OJ L 88/6.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277/1.

Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA, [2012] OJ L 315/57.

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) [2016] OJ L 119/1.

Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision

of audiovisual media services (Audiovisual Media Services Directive) (codified version) (Text with EEA relevance), [2010] OJ L 95/1.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, e-Privacy Directive) [2002] OJ L 201/37.

Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse [2021] OJ L 278/69.

Secondary Sources

Journal articles

Büchi M and Festic N and Latzer M, 'The Chilling Effects of Digital Dataveillance:Theoretical Model and an Empirical Research Agenda' (2022) Big Data & Society 1,14. < https://journals.sagepub.com/doi/full/10.1177/20539517211065368> Accessed 10 May.

Chatzinikolaou, A 'Sexual images depicting children: The EU legal framework and online platforms' policies' 11(1) 2020 European Journal of Law and Technology < https://ejlt.org/index.php/ejlt/article/view/740 > Accessed 7 May.

Gustin, M 'Challenges of Protecting Children's Rights in the Digital Environment' (2022) 6 ECLIC

Jacobsen, A 'Children's rights in the European Court of Human rights – An emerging Power Structure' in The International Journal of Children's Rights (2016) 24 (3)

Kravchuk, N 'Privacy as a New Component of "The best interest of the Child"' (2021) 29 (1) The international Journal of Children's Rights

Lenaerts K, 'Limits on Limitations: The essence of Fundamental Rights in the EU' (2019) 20 German Law Journal

Macenaite M, 'From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU general data protection regulation' (2017) 19(5) New media & Society

Maxwell, F 'Children's Rights, The Optional Protocol and Child Sexual Abuse Material in the Digital Age' (2022) 31(1) The International Journal of Children's Rights

Milkaite I and Lievens E, 'Children's rights to Privacy and Data Protection Around the world: Challenges in the Digital Realm'10(1) 2019 European Journal of Law and Technology < https://ejlt.org/index.php/ejlt/article/view/674> Accessed 16 May.

Nawaila M and Kanbul S and Ozdamli F, 'A review on the Rights of Children in the Digital Age' (2018) 94 Children and Youth Services Review 390.

O'Flaherty M and Samardžić-Marković S, 'Handbook on European law relating to the rights of the child' (Publication Office of the European Union 2022)

Quintel, T 'The Commission Proposal on Combatting Child Sexual Abuse" – Confidentiality of Communications at risk?' (2022) 8 EUR data Prot L rev 262

Rojszczak, M 'Online content filtering in EU law- A coherent framework or jigsaw puzzle?' (2022) 47 Computer Law & Security Review < https://www.sciencedirect.com/science/article/pii/S0267364922000826> Accessed 30 April.

Tracol X, 'The joined cases of Dwyer, SpaceNet and VD and SR before the European Court of Justice: The Judgements of the Grand Chamber about data retention continue falling on deaf ears in Member states' (2023) 48 Computer Law and Security Review

Vincet J, 'New EU rules would require chat apps to scan private messages for child abuse: The proposal has been called unworkable and invasive by privacy experts' The Verge (11 May 2022) < https://www.theverge.com/2022/5/11/23066683/eu-child-abuse-grooming-scanning-messaging-apps-break-encryption-fears > Accessed 18 May 2023.

Wilman F, 'Two emerging principles of EU internet law: A comparative analysis of the prohibitions of general data retention and general monitoring obligations' (2022) 46 Computer Law & Security review

Literature

Celeste, E *Digital Constitutionalism: The Role of Internet Bills of Rights* (Routledge 2023)

Goldner Lang I, 'The Child's Best Interest as a Gap Filler and Expander of EU Law in Internal Situations' in Katja S. Ziegler and others (eds.) *Research Handbook on General Principles of EU Law* (2019 Edward Elgar Publishing)

Goonesekere S, 'The Interrelated and Interdependent Nature of Children's Rights' in Jonathan Todres and Shani M King (eds.) *The Oxford Handbook of Children's rights law* (2020 Oxford Handbooks)

Greer S and Gerards J and Slowe R (eds.), 'The fundamental Rights Jurisprudence of the European Court of Justice' in *Human Rights in the Council of Europe and the European Union: Achievements, Trends and challenges* (Cambridge University Press 2018)

Hettne J and Okten Eriksson I, 'EU legal methodology: Theory and impact on Swedish law enforcement' (2nd edn Norstedts Juridik 2011)

Hijmans, H *The European Union as Guardian of Internet Privacy; The Story of Art 16 TFEU* (Springer 2016)

Kranenborg, H 'Article 8' in Steve Peers and others (eds.) *The EU Charter of Fundamental rights: A commentary* (2021 Hart publishing)

Lebeck C, *EU-charter on Fundamental rights* (2nd edn 2016 Studentlitteratur AB)

Lievens E and others, 'Children's Rights and Digital Technologies' in Ursula Kilkelly and Ton Liefaard (eds.) *International Human Rights of Children* (2019) Springer

Kaesling, K 'Children's digital rights: realizing the potential of the CRC' in Ellen Marrus and Pamela Laufer-Ukeles (eds.), *Global Reflections on Children's Rights and the Law: 30 years after the Convention on the Rights of the Child* (1st ed Routledge 2021).

Kaesling K, 'A Rights-Based Approach to Children Digital Participation in the Multi-Level System of the European Union' in Nina Dethloff Katharina Kaesling and Louisa Specht- Riemenschneider (eds.) *Families and New Media* (2023 Springer)

Kleineman J, 'legal dogmatic method' in Maria Nääv and others (eds.) Legal methodology (2th edn Studentlitteratur AB 2018)

Lamont, R 'Article 24' in Steve Peers and others (eds.) *The EU Charter of Fundamental rights: A commentary* (2021 Hart publishing)

Mangan, D 'Article 7 (Private Life, Home and Communications)' in Steve Peers and others (eds.) *The EU Charter of Fundamental rights: A commentary* (2021 Hart publishing)

Peers S and Prechal S 'Article 52' in Steve Peers and others (eds.) *The EU Charter of Fundamental rights: A commentary* (2021 Hart publishing)

Reichel J, 'EU-legal dogmatic method' in Maria Nääv and others (eds.) Legal methodology (2th edn Studentlitteratur AB 2018)

Stalford, H *Children and the European Union: rights, welfare and accountability*, (Hart publishing 2012)

Websites

Boffey, D 'EU lawyers say plan to scan private messages for child abuse may be unlawful',The Guardian (8 May 2023) < https://www.theguardian.com/world/2023/may/08/eu-lawyers-plan-to-scan-private-messages-child-abuse-may-be-unlawful-chat-controls-regulationhttps://www.theguardian.com/world/2023/may/08/eu-lawyers-plan-to-scan-private-messages-child-abuse-may-be-unlawful-chat-controls-regulation> Accessed 18 May 2023.

Bäcker M and Buermeyer U, 'Comments on the planned obligations of Internet Service providers to combat sexualised violence against children: so-called chat control regulation' (2022) *Verfassungdsblog* (18 August 2022)< https://verfassungsblog.de/my-spy-is-always-with-me/> Accessed 20 March 2023.

Torn,'Open Letter: Thorn and 90+ Organizations Welcome the EU's Proposal to Prevent and Combat child Sexual Abuse' (31 May 2022) < https://www.thorn.org/blog/open-letter-thorn-and-50-organizations-welcome-the-eus-proposal-to-prevent-and-combat-child-sexual-abuse/> Accessed 18 may 2023.

Other sources:

Commission, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications, Proposal for a Regulation on e-Privacy)' COM (2017) 010 final.

Commission, ‘Proposal for a Regulation of the European Parliament and of the Council laying down rules to Prevent and Combat Child Sexual Abuse’ COM (2022) 209 final.

The European Data Protection Board and The European Data Protection Supervisor, ‘Joint Opinion 04/2022 on the Proposal of the European Parliament and of the Council Laying down rules to prevent and combat child sexual abuse’ (2022)

European Commission, “New better internet for kids strategy (BIK+): Compendium of EU formal texts concerning children in the digital world” (2022)

United Nations Committee on the Rights of the Child, ‘General Comment nr 14 [2013] on the Right of the Child to have his or her Best Interests taken as a Primary Consideration (General Comment nr 14)’ (adopted on 29 May 2013, CRC/C/GC/14)

United Nations Committee on the Rights of the Child, ‘General Comment nr 25 [2021] on Children’s rights in relation to the Digital Environment (General comment nr 25)’ (adopted on 2 March 2021, CRC/C/GC/25)

Table of cases

European Court of Justice

Joined Cases C-92/09 and C-93/09 *Volker Und Markus Schecke GbR and Harmut Eifert V Land Hessen* [2010] ECR I-11063.

Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd V. Minister for Communications* [2014] ECLI:EU:C:2014:238.

Joined Cases C-203/15 and C-698/15 *Tele 2 Sweden and Watson (Tele 2)* ECLI:EU:C: 2016:970.

Case 207/16 *Ministerio Fiscal* [2018] ECLI:EU:C:2018:788

Case 511/18 *La quadrature du net and Others* [2020] ECLI:EU:C:2020:791

Case 311/18 *Facebook Ireland and Schrems* [2020] ECLI:EU:C:2020:559

Case 140/20 *Commissioner of An Garda Siochana* [2022] ECLI:EU:C:2022:258

Case 739/19 *SpaceNet* [2022] ECLI:EU:C:2022:854

Case 623/17 *Privacy International* [2020] ECLI:EU:C:2020:790

Case 339/20 *VD and SR* [2022] ECLI:EU:C:2022:703

Case C-401/19 *Poland V. European Parliament and Council* [2022] ECLI:EU:C:2022:297.

Case C-324/09 *L'Oréal v. eBay* [2011] ECLI:EU:C:2011:474.

C-311/18 Data Protection Commissioner V Facebook Ireland Ltd and Maximillian *Schrems (Schrems II)* [2020] QBECLI:EU:C: 2020:559.

C-362/15 *Maximilian Schrems v Data protection Commissioner (schrems)* [2015] ECLI:EU:C:2015:650.

European Court of Human Rights

Marper v. UK [2008] App no 30562/04 and 30566/04)

K.U. v. Finland [2008] App no. 2872/02

Aleksey Ovichinnikov v. Russia [2010] App no. 24061/04)

Avilkina and others v. Russia [2013] App no. 1585/09