Tilburg University

Tilburg Law School

Tilburg Institute for Law, Technology, and Society

Law and Technology (LLM)

Navigating the Tightrope: Examining the Practical Interplay of Public Security, Data Protection and Privacy in the Proposed Regulation Against Child Sexual Abuse

By Janne van de Loo

Student number: 2082416
Primary Supervisor: Dr. Lorenzo Dalla Corte
Secondary Supervisor: Lisa Rooij

A Master Thesis

for

the master's degree Law and Technology (LLM)

Final draft version 26th of May 2024

Acknowledgements

I would like to sincerely thank my primary supervisor, Dr. Lorenzo Dalla Corte, for his enthusiasm, patience, and guidance throughout the writing of this thesis. Without his help, this thesis would not have come to fruition. I also want to thank Lisa Rooij for her feedback and valuable insights, which helped elevate this thesis to another level.

Table of Contents

List of abbreviations

Abbreviation	Meaning
AG	Advocate General
CA	Coordinating Authority for Child Sexual Abuse Issues
CFR	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
CoE	Council of Europe
CSA	Child sexual abuse
CSAM	Child sexual abuse material
CSS	Client-Side Scanning
DRI	Digital Rights Ireland
E2EE	End-to-End encryption
EC	European Commission
ECHR	European Convention on Human Rights
ECtHR	The European Court of Human Rights
EDRi	European Digital Rights
EU	European Union
EU-Centre	EU-Centre on Child Sexual Abuse
FHE	Fully homomorphic encryption
FRA	The European Union Agency for Fundamental Rights
Grooming	Child solicitation
LQDN	La Quadrature du Net
MEP	Member of the European Parliament
ML	Machine learning
MS	Member State(s)
PI	Privacy International
Providers	Providers of hosting and interpersonal communication service providers
Tele2	Tele2 Sverige/Watson

TEU	Treaty on European Union
The Council	the Council of the European Union

I Introduction

1.1 Background and problem statement

"Not even East Germany's security police, the Stasi, had this level of surveillance": that is how Axelsson describes the proposal from the European Commission ('EC') for a new regulation on combatting child sexual abuse material ('the proposal').[1] MEP P. Breyer calls it 'the end of the Privacy of Digital Correspondence'[2] and NGO association European Digital Rights ('EDRi') adds to this that 'this law would turn the internet into a space that is dangerous for everyone's privacy, security and free expression.'[3] Conversely, more than 40 child rights organisations and the EC are in favour of this new proposed Regulation.[4] Furthermore, the EC claims that this proposed Regulation is necessary to guarantee children's fundamental rights to care, protect their well-being, mental health, and best interests, and support the public interest in effectively preventing, investigating, and prosecuting the serious crime of child sexual abuse.[5] The mentioned statements reveal clear divisions between proponents and opponents of the proposed Regulation.

However, for perspective, what is this proposal about, and what is its current state of affairs? To understand the proposal, it is first necessary to explain the current situation. Currently, there is a Regulation on a temporary derogation from Articles 5(1) and 6(1) of the e-Privacy Directive.[6] These articles protect the confidentiality of communication and traffic data, however, with this derogation it allows number-independent interpersonal communication services, such as Facebook Messenger, to voluntarily scan this data for the detection and removal of CSAM.[7] Adopted in 2021 and extended in 2024, this regulation is used by

[1] Henrik Sköld, 'Kritiserade EU-Förslaget: Så Kan Dina Vanliga Familjefoton Stämplas Som Pedofili' *SVT Nyheter* (8 April 2023) <www.svt.se/nyheter/utrikes/eu-forslaget-chat-control-kritiseras> accessed 25 July 2024.

[2] Patrick Breyer, 'Chat Control: The EU's CSEM Scanner Proposal' (*Patrick Breyer*) <https://www.patrick-breyer.de/en/posts/chat-control/> accessed 28 October 2023.

[3] EDRi, 'European Commission Must Uphold Privacy, Security and Free Expression by Withdrawing New Law, Say Civil Society' (*European Digital Rights,* 8 June 2022) <https://edri.org/our-work/european-commission-must-uphold-privacy-security-and-free-expression-by-withdrawing-new-law/> accessed 28 October 2023.

[4] 'IWF Voices Support for European CSAM Proposal in Open Letter to European Union' (1 June 2022) < www.iwf.org.uk/news-media/news/iwf-voices-support-for-european-csam-proposal-in-open-letter-to-european-union/> accessed 14 June 2024.

[5] Commission, 'Proposal for a Regulation of the European Parliament and the Council laying down rules to prevent and combat child sexual abuse' COM (2022) 209 final, 3.

[6] 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 274/41.

[7] Breyer (n 2); A. Baas, 'Artikel 5 Vertrouwelijk karakter van de communicatie – Wettelijk kader', (Lexplicatie, commentaar op regeling Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie, Wolters Kluwer 2021) <

unencrypted US communication services like Gmail and Facebook.[8] On May 11, 2022, the EC presented a new proposal for a regulation to prevent and combat child sexual abuse.[9] Following the ordinary legislative procedure, the proposal is currently in the first reading stage. After the 2024 European elections, trilogue meetings will be held between the Council of the European Union ('the Council') and the European Parliament ('EP'), with the EC acting as a mediator, to negotiate the amendments proposed by the EP on the EC's proposed Regulation.[10] To address the first question: the aim is to establish a clear legal framework to prevent and combat child sexual abuse ('CSA'), providing legal certainty to information society services regarding their responsibilities.[11]

This proposal has, potentially, a very wide scope, covering all relevant information society services; however, the most important categories are: the providers of hosting and interpersonal communication services ('providers').[12] Hosting services are used to store information provided by the recipient of the service and encompass several services such as web hosting and cloud computing.[13] Web hosting services, offered by companies like Endurance and Hetzner, provide individuals and businesses with space for their websites, ensuring smooth operation.[14] Cloud computing services, such as Microsoft Azure and Google Cloud Platform, provide on-demand access to a shared pool of configurable computing resources, such as storage and servers, that can quickly be provided via the internet.[15]

www.inview.nl/document/id8a05fd718eab42bdabf34e813d6ae5b0/lexplicatie-kernbeschrijving-bij-richtlijn-2002-58-eg-betreffende-de-verwerking-van-persoonsgegevens-en-de-bescherming-van-de-persoonlijke-levenssfeer-in-de-sector-elektronische-communicatie-richtlijn-betreffende-privacy-en-elektronische-communicatie?ctx=WKNL_CSL_1983&tab=tekst> accessed 18 June 2024.

[8] Breyer (n 2); 'Child Sexual Abuse Online: Current Rules Extended until April 2026 | News | European Parliament' (10 April 2024) <www.europarl.europa.eu/news/en/press-room/20240408IPR20311/child-sexual-abuse-online-current-rules-extended-until-april-2026> accessed 18 June 2024.

[9] COM (2022) 209 final, 3.

[10] 'Ordinary Legislative Procedure' (*European Parliament*) <www.europarl.europa.eu/infographic/legislative-procedure/index_en.html> accessed 19 May 2024; 'Interinstitutional Negotiations | Ordinary Legislative Procedure | European Parliament' (*olp*) <www.europarl.europa.eu/olp/en/interinstitutional-negotiations> accessed 27 May 2024.

[11] COM (2022) 209 final, 3.

[12] COM (2022) 209 final, ch I, art 2(f); COM (2022) 209 final, 2.

[13] John Moore and Ivy Wigmore, 'What Is Hosted Services? | Definition from TechTarget' (*IT Channel*, 1 October 2018) <www.techtarget.com/searchitchannel/definition/hosted-services> accessed 20 June 2024.

[14] 'Webhosting' (*Wikipedia*, 2023) <https://nl.wikipedia.org/w/index.php?title=Webhosting&oldid=66323253> accessed 26 November 2023.

[15] Ali Sunyaev, *Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies* (Springer International Publishing 2020) 198.

Interpersonal communication services, such as WhatsApp, Facebook Messenger and Snapchat, provide platforms for direct messaging, image sharing and video communication.[16] The proposal introduces that these providers can be ordered to detect known or new child sexual abuse material ('CSAM') or the solicitation of children ('grooming').[17] These orders can be executed through different methods, but the provider will need a certain form of analysis of the communication via client-side scanning ('CSS') or the altering of the encryption, to execute the detection order. These detection orders are aimed at the whole service and not a specific user, so all users of the ordered provider will be examined.[18]

This approach may lead to (mass) surveillance. While the proposal is distinctive in implying new techniques to achieve its goals, it simultaneously aligns itself with precedents from the Court of Justice of the European Union ('CJEU')[19] and the European Court of Human Rights ('ECtHR')[20] where they addressed (mass) surveillance. Similar concerns have been raised in the United States, notably during the Snowden revelations.[21]

Essentially, what the proposal and these examples have in common is that the government is prioritizing public security, but this comes at the expense of individual security. Fundamentally, this proposal, along with the aforementioned cases, initiates a clash between the value of public security and the values of privacy and data protection. Therefore, this thesis will explore how the proposal generates a conflict between public security, privacy and data protection. Specifically, the thesis aims to research the detection measures, focussing on the specific technical methods, such as CSS, that are deemed necessary to enhance public security. In other words: how does the proposal, when examined from a technical perspective, result in a conflict between the values of privacy and public security?

1.2 Research question and sub-questions

The question that is central to the matter discussed before is:

[16] 'Personal Communications Service' (*Wikipedia*, 2023) <https://en.wikipedia.org/w/index.php?title=Personal_Communications_Service&oldid=1174819071> accessed 26 November 2023.

[17] COM (2022) 209 final, ch II, art 7(1) and art 10(1).

[18] Ot van Daalen, 'Fundamental Rights Assessment of the Framework for Detection Orders under the CSAM Proposal' (IViR, 22 April 2023) <www.ivir.nl/publicaties/download/CSAMreport.pdf> accessed 26 November 2023.

[19] Judgement of 8 April 2014, *Digital Rights Ireland,* joined cases C-293/12 and C-594/12, EU:C:2014:238.

[20] *Klass and Others v. Germany*, 6 September 1978, Series A no. 28; *Big Brother Watch and Others v. the United Kingdom* [GC], nos. 58170/13 and 2 others, 25 May 2021.

[21] Zygmunt Bauman and others, 'After Snowden: Rethinking the Impact of Surveillance' (2014) 8 International Political Sociology 121 121-122.

"To what extent is the proposed CSAM regulation legitimate in the light of the implied technical measures, according to Article 52(1) CFR, concerning the limitations imposed on the rights in Articles 7 and 8 CFR?"

To answer the central question, the author will conduct research into the following sub-questions:

- What technical measures are implicated in the proposed CSAM regulation, and what do these entail?
- How have the CJEU and ECtHR addressed limitations of Articles 7 and 8 CFR, and Article 8 ECHR within (mass) surveillance jurisprudence, and what is the legal interpretation of Article 52(1) CFR and Article 8(2) ECHR regarding the limitations on the rights to privacy and data protection in the context of (mass) surveillance?
- Do the technical measures that are implied by the proposal engender a conflict between public security and privacy, and if yes, how?

1.3 Literature review

The central issue here is (mass) surveillance. Yet, what constitutes this? Various definitions exist. The European Union Agency for Fundamental Rights ('FRA') definition focuses on the untargeted collection of vastly different amounts of data.[22] In contrast, the definition of the Council of Europe ('CoE') focuses on 'strategic' surveillance and notes that mass surveillance has a proactive element to it.[23]

There are evidently various interpretations, each with its own set of advantages and drawbacks. This thesis focuses on the legitimacy of EU law, and thus, the decision has been made to adhere to the definition provided by the FRA. In their report, the FRA defines mass surveillance as: "[F]ar-reaching, complex and highly technologically advanced systems designed by US and some Member States' intelligence services to collect, store and analyse communication data, including content data, location data and metadata of all citizens around the world, on an unprecedented scale and in an indiscriminate and nonsuspicion-based

[22] Review Committee for the Intelligence and Security Services, 'Annual Report 2013-2014' (31 March 2014) < https://english.ctivd.nl/documents/annual-reports/2013/03/31/index> 45-46; European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental rights safeguards and remedies in the EU – 2023 update* (Publications Office of the European Union 2023) 15.

[23] Council of Europe, 'Mass Surveillance' (July 2018) <https://rm.coe.int/factsheet-on-mass-surveillance-july2018-docx/16808c168e > accessed 27 October 2023 1 (Factsheet mass surveillance).

manner."[24] Although the proposal is directed at providers and the FRA's definition focuses on intelligence services, the defining features such as 'indiscriminate and nonsuspicion-based manner' and the breadth of communication it encompasses make this definition suitable for this thesis.

Numerous scholars point out the vast number of problems that come with (mass) surveillance. These problems stretch from societal consequences to fundamental rights issues. First, we start with the societal issues. In the article of Maras, she states that mass surveillance will lead to the possible loss of citizens' trust and privacy.[25] Her reasoning entails that with the implementation of mass surveillance it deteriorates the divide between 'us' and 'them' (the ordinary law-abiding citizens and the criminals). In the words of Maras: 'The measures governments implement against *them* are accepted on the assumption that they do not and will not apply to *us*.' Yet, over time, individuals who were once part of *us* can find themselves classified as belonging to *them* when boundaries are redrawn.[26] In extent to this lies the trust of citizens, because no suspicions rise when the divide is upheld, nevertheless objections rise when the scope of the (mass) surveillance widens and normal law-abiding citizens themselves are being monitored which leads to the eroding of public trust in the government. In this sense Maras argues that the monitoring and storing of the information will result in a loss of privacy for the citizens.

Next to the societal impacts, there are also fundamental rights interferences. These interferences have been the subject of numerous ECtHR and CJEU judgments. These judgments can sketch a broad picture of the approaches the Courts have towards the interferences caused by (mass) surveillance.

To start, the ECtHR has pointed out in numerous judgments, such as *Szabó and Vissy v. Hungary*,[27] *Big Brother Watch* ('BBW'),[28] and *Liberty and Others v. United Kingdom*,[29] that mass surveillance measures illegitimately interfere with Article 8 of the European Convention on Human Rights ('ECHR'). Nevertheless, these interferences were not caused by mass surveillance itself, but through a lack clarity, safeguards, or proportionality of the measures. In

[24] European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU: Volume II: Field Perspectives and Legal Update* (Publications Office of the European Union 2017) 18.

[25] Marie-Helen Maras, 'The Social Consequences of a Mass Surveillance Measure: What Happens When We Become the "Others"?' (2012) 40 International Journal of Law, Crime and Justice 65 78.

[26] ibid.

[27] *Szabó and Vissy v. Hungary*, no 37138/14, 12 January 2016.

[28] *Big Brother Watch and Others v. the United Kingdom* (n 20).

[29] *Liberty and Others v. United* Kingdom, no 58243/00, 1 July 2008.

other words, the ECtHR does not deem mass surveillance *ipso jure* as an illegitimate interference but rather assess the legitimacy through a number of safeguards to prevent abuse of the mass surveillance.[30] However, it has to be stipulated that the ECtHR in any case "dislikes "blanket" measures that apply indiscriminately to a large class of people, since these prevent a case-by-case assessment of the need for an interference: a one-size-fits-all approach to human rights needs compelling justification."[31] The stance of the ECtHR becomes clear through cases, such as *Kennedy v. The United Kingdom* and *Breyer v. Germany*, where the ECtHR said there was an interference, however, this was not illegitimately since there were enough safeguards and the measures were proportionate.[32]

The CJEU has also issued several judgments, in cases like *Digital Rights Ireland* ('*DRI'*),[33] *Schrems I*,[34] and *Tele2 Sverige/Watson* ('*Tele2*'),[35] where they found that mass surveillance measures caused an illegitimate interference on Articles 7 and 8 of the Charter of the Fundamental Rights of the European Union ('CFR'). Yet, contrary to the ECtHR, the CJEU found that mass surveillance in itself causes illegitimate interferences with the right to privacy and data protection and underscores the importance of targeted surveillance that operates within certain parameters to protect fundamental rights.[36] Although, two side notes have to be made in this context. Firstly, in the *La Quadrature du Net* ('LQDN') case, did the CJEU break their mass surveillance prohibition and acknowledged that under strict circumstances and only for the goal of national security, mass surveillance could be deployed.[37] The second side note pertains to a recent case.[38] In this case, Advocate General ('AG') Szpunar called for a lowered threshold, permitting the retention and access of IP addresses and corresponding data for prosecuting copyright infringements.[39] Moreover, AG Szpunar suggests weakening safeguards,

[30] Factsheet mass surveillance (n 23) 1; Eliza Watt, *State Sponsored Cyber Surveillance* (Edward Elgar Publishing Limited 2021) 270; Eliza Watt, 'The Legacy of the Privacy versus Security Narrative in the ECtHR's Jurisprudence' [2022] Verfassungsblog <https://verfassungsblog.de/os6-privacy-vs-security/> accessed 15 July 2024.

[31] Gordon Nardell, 'Levelling up: Data Privacy and the European Court of Human Rights' in Serge Gutwirth, Yves Poullet and Paul De Hert (eds), *Data Protection in a Profiled World* (Springer Netherlands 2010) 46.

[32] *Breyer v. Germany*, no. 50001/12, §95-105, 30 January 2020; *Kennedy v. the United Kingdom*, no. 26839/05, §163 and 169, 18 May 2010.

[33] *Digital Rights Ireland* (n 19).

[34] Judgement of 6 October 2015, *Schrems I, C*-362/14, EU:C:2015:650.

[35] Judgement of 21 December 2016, *Tele2/Watson*, joined cases C-203/15 and C-698/15, EU:C:2016:970.

[36] Watt, *State Sponsored Cyber Surveillance* (n 30) 264 and 268.

[37] Sarah Eskens, 'The Ever-Growing Complexity of the Data Retention Discussion in the EU: An In-Depth Review of La Quadrature Du Net and Others and Privacy International' (2022) 8 European Data Protection Law Review 143 143.

[38] Judgement of 30 April 2024, *Hadopi*, C-470/21, EU:C:2024:370.

[39] Opinion of AG Szpunar delivered on 28 September 2024, *Hadopi,* C-470/21, EU:C:2023:711, paragraphs 78-82; Theresa Bosl, 'Not You Again!: Mass Surveillance Before the CJEU and Why "Hadopi" Could Be a Game-

arguing that prior review is unnecessary for accessing IP addresses and corresponding personal data if the interference is not deemed 'particularly serious'.[40] This opinion is followed by the CJEU.[41]

In sum, while the Courts criticize (mass) surveillance, they also acknowledge its necessity for combating serious crime and ensuring national security, allowing for its limited use. The CJEU, in conjunction with the ECtHR, has tried to forge a consensus between public security and privacy with individual privacy at its core.[42] Although the ECtHR is more favourable towards mass surveillance, it supports the consensus through the wide margin of appreciation,[43] as seen in *BBW* where 'end-to-end safeguards' were established to protect the right to privacy and data protection.[44] The CJEU supports the consensus through a similar, yet more privacy friendly, approach that can be seen in cases like *Tele2*,[45] and *Ministerio Fiscal*.[46]

Next to the Courts are also the privacy experts that upfronted their concerns with (mass) surveillance. First, we look at the broader concerns regarding (mass) surveillance in the light of the EC(t)HR and then we look at the specific concerns on the present proposal from an EU-legal framework perspective.

Regarding the ECtHR, Zalnieriute expresses concerns about their approach to mass surveillance. She argues that the ECtHR adopts a proceduralist approach, which she calls "procedural fetishism," posing a threat to the right to privacy. Specifically, the ECtHR focuses on procedural safeguards rather than the legality of the mass surveillance measures themselves and assumes the proportionality, functionality, and effectiveness of these measures. In other words, the ECtHR prima facie affirms the legality of mass surveillance as long as established safeguards are met. Zalnieriute is concerned that this approach strengthens governments'

Changer for the Right to Privacy' [2023] Völkerrechtsblog <https://voelkerrechtsblog.org/not-you-again/> accessed 24 July 2024.

[40] ibid, paragraphs 98ff; ibid.

[41] *Hadopi* (n 38), paragraphs 77-85 and 124-131*;* 'Surveillance and Hadopi: EU Court Buries Online Anonymity a Little Further' (*La Quadrature du Net*, 30 April 2024) <www.laquadrature.net/en/2024/04/30/surveillance-and-hadopi-eu-court-buries-online-anonymity-a-little-further/> accessed 19 May 2024.

[42] Valsamis Mitsilegas and others, 'Data Retention and the Future of Large-Scale Surveillance: The Evolution and Contestation of Judicial Benchmarks' (2023) 29 European Law Journal 176 210-211.

[43] Elisabet Fura and Mark Klamberg, 'The Chilling Effect of Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA' in Josep Casadevall, Egbert Myjer and Michael O'Boyle (eds), *Freedom of expression: essays in honour of Nicolas Bratza* (Wolf Legal Publishers 2012) 472-473.

[44] *Big Brother Watch and Others v. the United Kingdom* (n 20), paras 350 and 360.

[45] *Tele2/Watson and Others* (n 35) paras 108-111.

[46] Judgement of 2 October 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, paragraphs 55-56.

positions in the surveillance debate. If governments can demonstrate adherence to safeguards, they can argue that mass surveillance measures do not illegitimately interfere with the right to privacy, even though these measures may still be extensive and intrusive.[47]

Although Zalnieriute voiced her opinion in 2021, it remains relevant, as the ECtHR maintained the same approach to mass surveillance in February 2024, as noted in Tuchtfeld's article.[48] Watt and Milanovic share similar concerns, arguing that the ECtHR even normalizes mass surveillance by rejecting the idea that such measures are categorically disproportionate and instead emphasizing safeguards.[49] Milanovic notes that the Court focuses on clear, detailed rules and safeguards and does not engage with the broader question of whether the benefits of such programs outweigh the intrusion into individuals' privacy, assuming that better-placed institutions within these states have already made such determinations.[50]

In the context of the EU legal framework, concerns are specific to the current proposal. The EDPB and EDPS[51] have stated that the proposal lacks necessity and proportionality, a viewpoint echoed in a report by Colneric.[52] Furthermore, a leaked legal service report suggests that it may compromise the essence of rights under Articles 7 and 8.[53] The provided information highlights concerns and criticism surrounding (mass) surveillance and the current proposal.[54]

[47] Monika Zalnieriute, ‘Procedural Fetishism and Mass Surveillance under the ECHR’ [2021] Verfassungsblog <https://verfassungsblog.de/big-b-v-uk/> accessed 12 July 2024.
[48] Erik Tuchtfeld, ‘No Backdoor for Mass Surveillance’ [2024] Verfassungsblog <https://verfassungsblog.de/no-backdoor-for-mass-surveillance/> accessed 17 July 2024.
[49] Eliza Watt, ‘Much Ado About Mass Surveillance - the ECtHR Grand Chamber “Opens the Gates of an Electronic ‘Big Brother’ in Europe” in Big Brother Watch v UK’ (*Strasbourg Observers*, 28 June 2021) <https://strasbourgobservers.com/2021/06/28/much-ado-about-mass-surveillance-the-ecthr-grand-chamber-opens-the-gates-of-an-electronic-big-brother-in-europe-in-big-brother-watch-v-uk/> accessed 17 July 2024; Marko Milanovic, ‘The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum För Rättvisa’ (*EJIL: Talk!*, 26 May 2021) <www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/> accessed 17 July 2024.
[50] Milanovic (n 49).
[51] ‘EDPB-EDPS Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Rules to Prevent and Combat Child Sexual Abuse’ (Adopted on 28 July 2022) <https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042022-proposal_en> accessed 4 November 2023 36 (EDPB-EDPS Joint Opinion 04/2022).
[52] Ninon Colneric, ‘Legal Opinion Commissioned by MEP Patrick Breyer, The Greens/EFA Group in the European Parliament’ (Hamburg, March 2021) <www.patrick-breyer.de/wp-content/uploads/2021/03/Legal-Opinion-Screening-for-child-pornography-2021-03-04.pdf> accessed 28 October 2023 29.
[53] Legal Service of the Council of the European Union, ‘Opinion of the Legal Service 8787/23’ (Brussels, 26 April 2023) <https://aeur.eu/f/6ql> accessed 28 October 2023 18-19 (Opinion Legal Service); ‘Leaked EU Council Legal Analysis: EU Chat Control Plans for Indiscriminately Searching Private Messages Doomed to Failure’ (*Patrick Breyer*, 8 May 2023) <www.patrick-breyer.de/en/leaked-eu-council-legal-analysis-eu-chat-control-plans-for-indiscriminately-searching-private-messages-doomed-to-failure/> accessed 28 October 2023.
[54] COM (2022) 209 final.

The consensus is that both (mass) surveillance and, in the current context, the proposal infringe upon the right to privacy.

However, the literature review reveals a notable gap in the examination of the impact of the proposal and the novel technical measures, such as CSS, on the conflict between security and the rights to privacy and data protection. Furthermore, the sources seldom examine the technical measures that are needed to execute the aim of the proposal. For example, the EDPB and the EDPS talk about the technical measures such as CSS and encryption, but do not explain what they entail and how they contribute to the conflict between public security and the right to privacy and data protection. Nevertheless, it is precisely these technological measures that give rise to the intersection of public security and privacy issues. This thesis will add to the discussion about the clash between public security and privacy in relation to the proposal. It stands out by shedding light on the technical details and how they play a part in this conflict.

1.4 Methodology

The research methodology chosen for addressing the research question is the legal doctrinal approach. This approach facilitates an examination of the prevailing legal framework and pursues objectives such as the interpretation of existing legal principles, providing clarity, offering explanations, and engaging in critical reflection.[55] This method is reflected in the sub-questions as well.

The first sub-question delves into the technical measures, such as CSS and End-to-End encryption ('E2EE'), that are needed to execute the aim of the proposal, focusing on the description and functioning of the technologies involved. Instead of offering a descriptive explanation of the law, this chapter provides a comprehensive overview of the current technologies that the proposal will want the provider to enact. In this context, the doctrinal method remains suitable as it furnishes insights into these technologies.

The second sub-question aligns with this method, aiming to enhance our understanding of the existing legal frameworks and the jurisprudence. To answer the second sub-question, the articles that establish the conditions for a legitimate restriction of fundamental rights for privacy and data protection will be examined. For Article 52(1) Charter of Fundamental Rights of the European Union ('CFR') the conditions 'provided for by the law', 'respect the essence of the right' and the 'necessity and proportionality' will be examined. As for Article 8(2) ECHR the

[55] Gijs van Dijck, Marnix Snel and Thomas van Golen, *Methoden van Rechtswetenschappelijk Onderzoek* (Boom Juridisch 2018) 84-85.

conditions ‘in accordance with the law’, ‘legitimate aim’ and ‘necessary in a democratic society’ will be researched. These conditions will be examined in conjunction with the jurisprudence of both the CJEU and the ECtHR. This sub-question will provide a comprehensive legal framework and it will address how the courts address the issue of limitations imposed on the rights of privacy and data protection. Despite the regulation falling under European Union law, the choice has been made to also involve both the ECHR and the ECtHR in the second and third sub-questions. This decision is based on the notion that the ECtHR and the CJEU have an extensive dialogue between them and the corresponding legal systems. Therefore, it is crucial to consider both to form a comprehensive understanding of the overall trends in the limitations that can be imposed on the right to privacy and data protection.

The third sub-question has analytical aspect as it compares the findings from the second chapter with those from third chapter of the thesis. The answers obtained from this chapter will enable a critical reflection in the conclusion, shedding light on how the technical components lead to a conflict between the values of privacy and public security.

1.5 Outline

The thesis structure is as follows: chapter II addresses the first sub-question, delving into the different types of technical measures and their practical implications. Chapter III sheds light on the second sub-question, exploring the limitations posed on privacy and data protection in the context of (mass) surveillance through an examination of the literature and the jurisprudence of the CJEU and ECtHR. In chapter IV, the focus turns to the third sub-question, analysing whether these technical measures create a conflict between public security and privacy and exploring the nature of any such conflict. Finally, chapter V concludes and answers the main research questions.

II The proposed CSAM regulation: technical aspects

This chapter explores the technical aspects of the proposal, beginning with the steps leading to a detection order[56] and the involved actors. It then focuses on the technical measures required to execute a detection order. The central question is: what technical measures are implicated in the proposed CSAM regulation, and what do these entail? Ultimately, the chapter finds that the proposed regulation coerces E2EE providers to use either CSS or server-side scanning to circumvent encryption and effectively execute the detection order.

2.1 The detection order

2.1.1 The preliminary steps

In the first section of Chapter 2 of the proposal, there are three preliminary obligations that providers must undertake regardless of their situation. These are: a risk assessment (1), the mitigation of the assessed risks (2), and the reporting of the risks and mitigations measures (3).[57]

Firstly, the providers must conduct risk assessments, which involves identifying, analysing, and assessing the risk of their service being used for online CSA.[58] This assessment considers criteria outlined in the proposal, such as any previously identified instances of online CSA and the manner in which users interact with the service.[59] Specific criteria related to grooming are also listed, including the extent of children's use of the service and the availability of functionalities that may contribute to grooming risks, such as image or video sharing.[60] However, concerns raised by both the EDPS and the EDBP highlight the potential broad margin of appreciation and interpretation due to the generic nature of some criteria and their commonality across online services, which may lead to a subjective rather than an objective assessment.[61]

After conducting the risk assessment, providers are required to implement reasonable measures to mitigate the identified risks. The proposal specifies that these measures may include adapting the provider's content moderation, recommender systems, decision-making processes, operation or functionalities of the service, or the content of enforcement of its terms

[56] A detection order is a task that can be imposed on providers to actively detect the dissemination of known or new CSAM or grooming, provided certain requirements are met.
[57] COM (2022) 209 final, 16, ch II, art 3 – 5.
[58] COM (2022) 209 final, ch II, art 3(1).
[59] COM (2022) 209 final, ch II, art 3(2)(a)-(e).
[60] COM (2022) 209 final, ch II, art 3(2)(e).
[61] EDPB-EDPS Joint Opinion 04/2022 (n 51) 14.

and conditions through appropriate technical and operational means and staffing.[62] Again, however, concerns are raised by the EDPB and the EDPS. These concerns centre around the potential lack of legal certainty and foreseeability in these measurers. While these measures may appear to reduce relevant risks, their effectiveness could be undermined by the complexity and subjectivity of the risk assessment process and the vagueness of terms such as ‘appreciable extent’ in determining acceptable risk levels post-implementation.[63]

After implementing the mitigation measures, the provider is required to report the identified risks and mitigation measures to the Coordinating Authority for Child Sexual Abuse Issues (‘CA’).[64] This obligation introduces a new actor: the CA. The CA, designated by the Member State ('MS') from one or more competent authorities, will be responsible for the application and enforcement at the national level once the Regulation is in force.[65] The CA has the authority to request judicial entities to issue detection, removal, or blocking orders against providers and possesses investigatory and enforcement powers, such as imposing fines.[66] This final preliminary obligation is crucial because the risk assessment and the chosen measures, essentially the content of the report, serve as the basis for determining if a detection order is necessary.[67]

2.1.2 Requirements and issuing of the detection order

After the preliminary obligations of the providers, the responsibility shifts to the CA. The CA has the power, under certain conditions, to request the competent judicial authority to issue a detection order. Once issued, the order compels the provider subjected to it to implement technologies to detect CSAM or grooming. However, no specific technologies are named; only requirements are listed to which the providers’ chosen technologies must adhere.[68] Here, the proposal introduces several key aspects.

First, it presents another relevant actor, ‘the competent judicial authority’; however, the proposal lacks a precise definition. Instead, the answer can be found in the preamble, where it states that a competent judicial authority, in line with the procedural rules set by the MS, should be capable of making informed decisions on detection orders, in particular, to ensure a fair

[62] COM (2022) 209 final, ch II, art 4(1).
[63] EDPB-EDPS Joint Opinion 04/2022 (n 51) 14.
[64] COM (2022) 209 final, ch II, art 5(1).
[65] COM (2022) 209 final, ch III, art 25(1)-(2).
[66] COM (2022) 209 final, ch II, art. 3(1), art 4(1), art 5(1), art 7(1), art 14(1), ch III, art 25(2), art 27(1), art 28 (1), and art 29.
[67] EDPB-EDPS Joint Opinion 04/2022 (n 51) 14; COM (2022) 209 final, ch II, art 7(4).
[68] COM (2022) 209 final, ch II, art 7(1) and (4) and art 10(1)-(3).

balance of the fundamental rights at stake.[69] For example, in the Netherlands, an investigative judge can issue such orders, given their role in authorizing police searches of premises or data carriers.[70]

Secondly, the proposal outlines conditions that must be met before a detection order can be issued.[71] These conditions are as follows: firstly, there must be evidence indicating a significant risk of the service being used for online CSA. The criterion of a 'significant risk' is detailed in paragraphs 5, 6, or 7 of Article 7, depending on the type of detection order that is considered (known CSAM, new CSAM or grooming).[72]

For known CSAM, a significant risk exists if, despite mitigation measures, the service is likely to be used to an appreciable extent for disseminating known CSAM, with evidence of such use in the last 12 months.[73] For new CSAM, there must be likelihood and factual evidence similar to known CSAM, and a prior detection order for known CSAM must have been issued, leading to a significant number of CSAM reports by the provider.[74] Regarding a grooming detection order, a significant risks exists if the provider qualifies as a provider of interpersonal communication services, it is likely that the service is used to an appreciable extent for grooming, and there is evidence of such use.[75] In addition to evidence of a significant risk, it is required that the negative consequences for affected parties do not outweigh the reasons for issuing a detection order, ensuring a fair balance between fundamental rights.[76] If these conditions are met, the detection order can be issued, and the provider must implement detection technologies.[77]

Also, here the EDPB and the EDPS place some critical notes. For one, even with the specification of 'significant risk', the conditions are 'dominated' by vague legal terms like 'appreciable extent' and 'significant number' and are repetitive because evidence of former abuse contributes to establishing the likelihood of future abuse. This could lead to inconsistent interpretations and legal uncertainty among competent judicial authorities across MS, which

[69] COM (2022) 209 final, rec 24.
[70] Jan-Jaap Oerlemans and Maša Galič, 'Cybercrime investigations' in Wytske van der Wagen, Jan-Jaap Oerlemans and Marleen Weulen Kranenbarg (eds), *Essentials in Cybercrime: A Criminological Overview for Education and Practice* (Eleven International Publishing 2021) 201.
[71] COM (2022) 209 final, ch II, art 7(4).
[72] COM (2022) 209 final, ch II, art 7(4)(a) and (5)-(7).
[73] COM (2022) 209 final, ch II, art 7(5)(a) and (b).
[74] COM (2022) 209 final, ch II, art 7(6)(a) and (b).
[75] COM (2022) 209 final, ch II, art 7(7).
[76] COM (2022) 209 final, ch II, art 7(4)(b).
[77] COM (2022) 209 final, ch II, art 7(1).

disrupts the uniform application of the detection orders for communication service providers.[78] Additionally, the legal service of the EC argues that the proposal lacks a clear methodology for assessing the risk of CSA and specifying a meaningful threshold for justifying the introduction of a detention order, which may affect the clarity and precision of the regime for issuing detection orders.[79]

Lastly, it indicates that the addressed provider must take measures as specified in Article 10 of the proposal, i.e., implementing technologies to detect CSAM or grooming. The article further states that the provider can acquire the technologies through the EU Centre on Child Sexual Abuse ('EU Centre') or choose to use its own technologies; providers are not required to use any specific technologies ('technology-neutral'). However, regardless of the technologies used, they must meet specific requirements to adequately fulfil the detection order.[80] With this reference to Article 10, the proposal highlights two additional important details: the EU Centre and the technologies used and their requirements, which will also be clarified in that order.

In short, the EU Centre can be seen as the backbone of the Regulation. It takes on tasks such as facilitating the implementation of provisions concerning the detection, reporting, removal or disabling of access to, and blocking of online CSA,[81] gathering and sharing information and expertise on how to combat CSAM and grooming,[82] and facilitating cooperation among the relevant parties, such as Europol and the CA's.[83] Additionally, the EU Centre will establish and maintain databases of reports provided by the providers of potential CSAM or grooming and of indicators of CSAM and grooming to be used in detection technologies.[84]

At first glance, Article 10 of the proposal seems adequately nuanced; it is technology-neutral, giving providers some freedom, and it only needs them to adhere to a set of requirements.[85] However, 'the devil is in the detail', and in this case, the technology must be *effective* in detecting the dissemination of known or new CSAM or grooming. This poses a challenge for encrypted interpersonal communication service providers, like WhatsApp and

[78] EDPB-EDPS Joint Opinion 04/2022 (n 51) 16.

[79] Opinion Legal Service (n 53) 8; 'Leaked EU Council Legal Analysis: EU Chat Control Plans for Indiscriminately Searching Private Messages Doomed to Failure' (n 53).

[80] COM (2022) 209 final, rec 4, ch II, art 10(2) and (3).

[81] COM (2022) 209 final, ch IV, art 40(2) and art 43(1)-(4).

[82] COM (2022) 209 final, ch IV, art 40(2) and art 43.

[83] COM (2022) 209 final, ch IV, art 40(2), art 43(6), and art 52-54.

[84] COM (2022) 209 final, ch IV, art 44(1) and art 45.

[85] There are four requirements: the technologies must be (1) effective, (2) unable to extract more information than strictly necessary, (3) in accordance with the state of the art and the least intrusive in terms of the right to privacy and data protection, and (4) sufficiently reliable in terms of false positives.

Signal.[86] These providers utilize encryption, encoding messages to make them unreadable, while decryption deciphers encrypted messages into a readable form. Both processes require a 'key', without which encryption or decryption is impossible. Encrypted providers encode the original message (the plaintext) into encrypted data (the ciphertext), which can only be reverted to plaintext and read by the recipient with the correct key.[87] There are different types of encryption, but in the context of interpersonal communications services end-to-end encryption ('E2EE')[88] is the most commonly used and plays a crucial role for ensuring stronger privacy and data protection, but at the same time, it lessens public security due to the secrecy.[89] E2EE ensures that only the ends (the sender and receiver) can read the message's content, preventing the service provider from analysing the content during transit.[90]

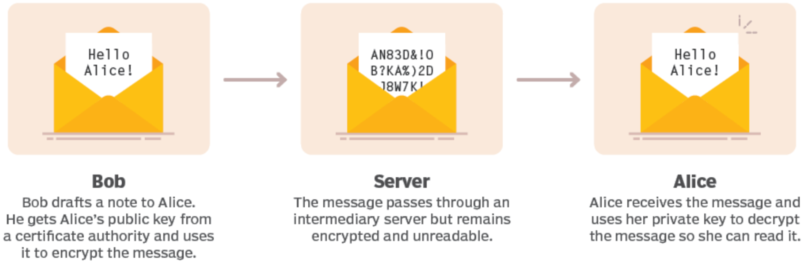

Hello Alice!
AN83D&!O B?KA%)2D J8W7K!
Hello Alice!
Bob
Bob drafts a note to Alice. He gets Alice's public key from a certificate authority and uses it to encrypt the message.
Server
The message passes through an intermediary server but remains encrypted and unreadable.
Alice
Alice receives the message and uses her private key to decrypt the message so she can read it.

Figure 2.1 How end-to-end encryption, with asymmetric key encryption, works.[91]

In contrast, unencrypted providers, as their name suggests, do not encrypt messages. This essentially means that every original message stays in plaintext format, allowing 'everyone' to read the content of the message. The result is less or no data protection and/or privacy but enhanced public security. Notable examples include Skype, Snapchat, and Instagram.[92]

[86] 'Messaging App Security: Which Are the Best Apps for Privacy?' (*Kaspersky*, 20 November 2023) < www.kaspersky.com/resource-center/preemptive-safety/messaging-app-security> accessed 24 February 2024.

[87] Seth James Nielson, *Discovering Cybersecurity: A Technical Introduction for the Absolute Beginner* (Apress Berkeley 2023) 94-95.

[88] Specifically, the messenger services use E2EE with asymmetric key encryption. However, for clarity regarding the main message, this is not further elaborated. See source for elaboration on technical details: Amir Diafi, 'Deep Diving into End-to-End Encryption (E2EE) 🔐 ' (*Medium*, 24 October 2022) <https://amirdiafi.medium.com/deep-diving-into-end-to-end-encryption-e2ee-2b05d3dca2ed> accessed 22 July 2024.

[89] EDPB-EDPS Joint Opinion 04/2022 (n 51) 27.

[90] Nielson (n 87) 171.

[91] Ben Lutkevich and Madelyn Bacon, 'What Is End-to-End Encryption (E2EE) and How Does It Work?' (*Security*) <www.techtarget.com/searchsecurity/definition/end-to-end-encryption-E2EE> accessed 22 July 2024.

[92] 'End-to-End Versleutelde Chats | Instagram-Helpcentrum' <https://help.instagram.com/3490194014566528> accessed 24 February 2024; Thomas Brewster, 'FBI Wiretap Opens Window To Murderous Drug Gang—And A Crucial Flaw In Snapchat Privacy' (*Forbes, 23 May 2022*) <www.forbes.com/sites/thomasbrewster/2022/05/23/fbi-snapchat-surveillance-exposes-a-murderous-mexican-gang-and-snaps-weakness/> accessed 24 February 2024; eSafety Commissioner, 'Basic Online Safety

To continue, according to the EC, metadata[93] alone is not an effective tool for detecting CSAM or grooming.[94] This implies that some form of content analysis is necessary for effective detection. While unencrypted interpersonal communication services can always analyse message content, encrypted services face a challenge in this. Due to E2EE, it is impossible for providers to analyse the content, because only the ends have the keys to decrypt the ciphertext. This presents an obstacle for E2EE services in analysing and detecting CSAM or grooming, potentially resulting in failure of the detection order. However, E2EE services have two potential solutions to meet the requirements deriving from a detection order. One solution involves analysing the message content at the endpoints, either before encryption or after decryption, known as CSS.[95] The second solution, known as server-side scanning, would require services to alter their encryption protocols to allow the scanning of content on their services.[96]

2.2 The technical measures

2.2.1 Client-side scanning

CSS refers to systems that analyse content on user devices ('clients') before encryption, thereby bypassing E2EE entirely. In this context, 'client' refers to one's own devices, such as smartphones, laptops, and potentially smartwatches and speakers.[97] There are two methods to execute CSS: (i) the scanning and matching are done on the client itself, or (ii) the scanning is done on the client, but the content is matched on a remote server. CSS on the client itself can be further divided into sub-methods: (ia) using functionally unique digital fingerprints ('perceptual hashing'), or (ib) employing machine learning ('ML').[98] While there are different methods, it has to be noted that it is likely that these methods will be used simultaneously in

Expectations' (December 2022) <www.esafety.gov.au/sites/default/files/2022-12/BOSE%20transparency%20report%20Dec%202022.pdf> accessed 24 February 2024 12-17.

[93] Riana Pfefferkorn, 'Content-Oblivious Trust and Safety Techniques: Results from a Survey of Online Service Providers' (2022) 1 Journal of Online Trust and Safety <https://tsjournal.org/index.php/jots/article/view/14> accessed 24 July 2024 2.
"*We consider metadata to be information about a message, file, or user, as distinguished from the information in the message or file, which we consider content. Thus a picture transmitted in the body of a message is content, while a picture used as the avatar for a user or user group would be considered metadata.*"

[94] Commission, 'Commission staff working document impact assessment report accompanying the document Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse' SWD (2022) 209 final 28.

[95] Hal Abelson and others, 'Bugs in Our Pockets: The Risks of Client-Side Scanning' (2024) 10 Journal of Cybersecurity < https://doi.org/10.1093/cybsec/tyad020> accessed 24 February 2024 15.

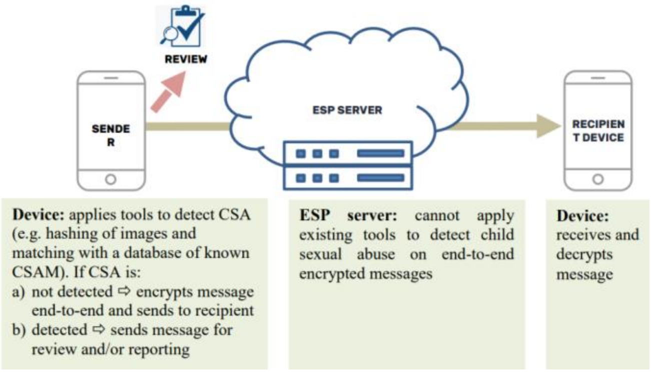
[96] EDPB-EDPS Joint Opinion 04/2022 (n 51) 28; van Daalen (n 18) 10.

[97] Abelson and others (n 95) 9.

[98] 'Fact Sheet: Client-Side Scanning' (*Internet Society, 2 September 2022*) <www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/> accessed 24 February 2024 (Fact Sheet: CSS).

order to avoid the pitfalls of the techniques independent of each other.[99] However, for the sake of explainability, these three methods will be assessed independently, including their respective advantages and disadvantages.

CSS all done on the client itself ('CSS on the client'), using hashes, operates as follows: hashes are algorithms capable of converting a large file, like an image or a video, into short and unique 'fingerprints'. A database of known CSAM hashes is installed on the client, and when the user attempts to send a message, the content is hashed and compared to the hashes in the database before encryption. If a match is found, indicating potential CSAM, the message is flagged for inspection. The advantages of this method are that it is able to detect known CSAM and it is relatively easy to implement since the software can be installed through a normal update cycle, such as Windows Update or Apple/Android System Update.[100] However, there are several disadvantages. Firstly, it cannot detect new CSAM since these hashes are not in the database and it cannot detect grooming, because hashing cannot detect text-based threats.[101] Additionally, depending on the client, the database needs to be limited to work properly, requiring significant storage space and computational capacity for updating. Furthermore, from a security standpoint, the software could be subverted to not detect or report CSAM or grooming, detect other content erroneously, or introduce false positives to overwhelm reporting systems.[102]



Device: applies tools to detect CSA (e.g. hashing of images and matching with a database of known CSAM). If CSA is:
a) not detected ⇨ encrypts message end-to-end and sends to recipient
b) detected ⇨ sends message for review and/or reporting

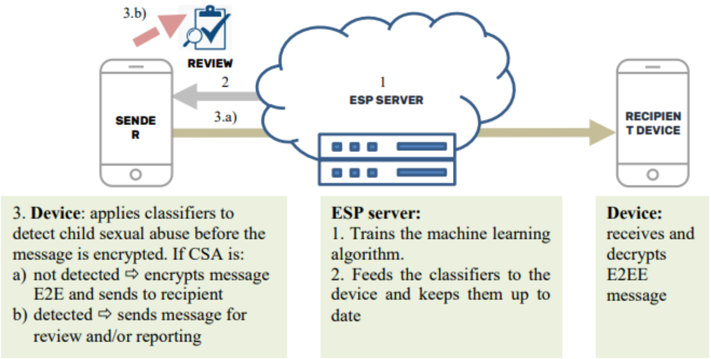
ESP server: cannot apply existing tools to detect child sexual abuse on end-to-end encrypted messages

Device: receives and decrypts message

Figure 2.3 CSS on the client using hashing.[103]

[99] Sigurður Ragnarsson, 'AI Content Moderation: Use, Types, & Integration With Hash Matching' (*Videntifier New Site*, 13 December 2023) <www.videntifier.com/post/ai-content-moderation> accessed 23 May 2024.
[100] In theory it is also possible to detect grooming within this solution via technology similar to spam filters. However, this is deemed not feasible by the experts. For this reason, will be assumed that this method can only be used for the detection of known CSAM, see: SWD (2022) 209 final, 282, 287-288; Abelson and others (n 95) 10.
[101] SWD (2022) 209 final, 296; Kaspar Rosager Ludvigsen, Shishir Nagaraja and Angela Daly, 'YASM (Yet Another Surveillance Mechanism)' (2022) arXiv, <http://arxiv.org/abs/2205.14601> accessed 5 April 2024 5.
[102] SWD (2022) 209 final, 293-295; Ludvigsen, Nagaraja and Daly (n 101) 3; Fact Sheet: CSS (n 98).
[103] SWD (2022) 209 final, 294.

The second method is CSS using ML. With this method, there is no database on the client; instead, it utilizes classifiers. The provider trains an ML algorithm using extensive labelled and verified examples of CSAM and grooming to generate classifiers. These classifiers are then sent to the client, which can use these to determine if the content of a message needs to be reported based on the classifiers. The advantages of this method include its ability to detect grooming and both new and known CSAM, as the algorithm continuously learns and generates new classifiers. However, there are several disadvantages associated with this approach. These include relatively high error rates, the need to keep the ML algorithms updated with well-labelled data, and the requirement for significant feedback on the quality of classification. Furthermore, substantial development is still needed to fully utilize this method. Additionally, there is a risk that the classifiers on the client could be compromised and manipulated to evade detection or flood the reporting systems, potentially leading to security risks and decreased privacy.[104]



3. **Device**: applies classifiers to detect child sexual abuse before the message is encrypted. If CSA is:
a) not detected ⇨ encrypts message E2E and sends to recipient
b) detected ⇨ sends message for review and/or reporting

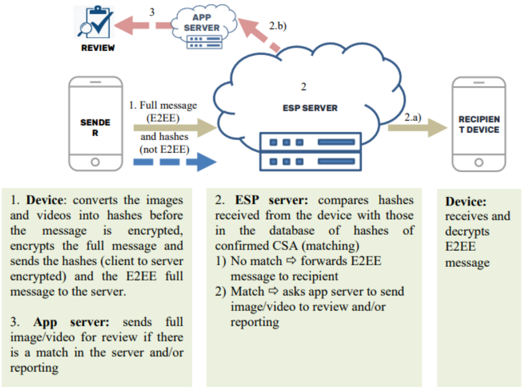
ESP server:
1. Trains the machine learning algorithm.
2. Feeds the classifiers to the device and keeps them up to date

Device: receives and decrypts E2EE message

Figure 2.4 On client CSS with ML.[105]

The third method involves the use of remote servers, which is essentially similar to the first method. However, a crucial difference is that the comparison of hashes occurs on a remote server instead of the client itself. The advantages of this method include the ability to compare hashes with an unlimited database, and the implementation is relatively straightforward. However, there are disadvantages to consider. This method only detects known CSAM, meaning grooming and new CSAM could go undetected. Additionally, the hashing algorithm could be compromised, leading to false positives or the introduction of non-CSAM hashes. Furthermore, privacy and data protection may be compromised due to the security issues and the visibility of hashes to the server.[106]

[104] SWD (2022) 209 final, 299-300; Ludvigsen, Nagaraja and Daly (n 101) 3.
[105] SWD (2022) 209 final, 299.
[106] SWD (2022) 209 final, 296.



1. **Device**: converts the images and videos into hashes before the message is encrypted, encrypts the full message and sends the hashes (client to server encrypted) and the E2EE full message to the server.

3. **App server:** sends full image/video for review if there is a match in the server and/or reporting

2. **ESP server:** compares hashes received from the device with those in the database of hashes of confirmed CSA (matching)
1) No match ⇨ forwards E2EE message to recipient
2) Match ⇨ asks app server to send image/video to review and/or reporting

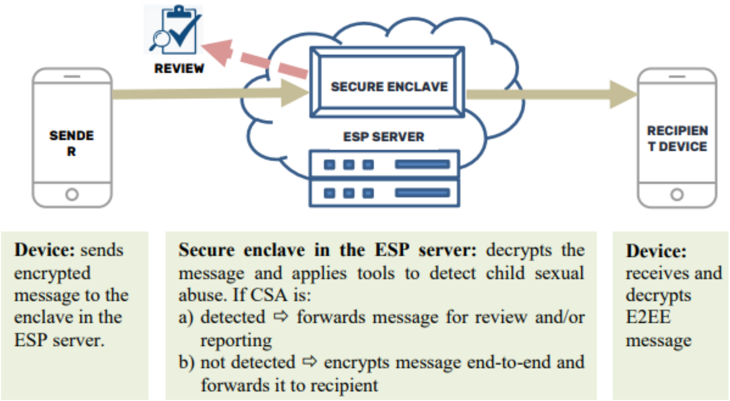
Device: receives and decrypts E2EE message

Figure 2.5 CSS with use of remote server.[107]

2.2.2 Sever-side scanning

Another method is server-side scanning, which can be achieved by altering the encryption protocol of the E2EE service.

With altering the encryption, the client sends an encrypted message to the server, where it is decrypted in a secure enclave to scan the content before re-encrypting it for transmission to the receiver. The advantages of this method include a simplified detection process and existing usage in other applications. Moreover, it can detect grooming and both new and known CSAM. However, only a few companies have access to this solution due to its operational complexity. Additionally, this solution heavily relies on the security of the enclave; if the enclave is compromised, it could jeopardize privacy and data protection.[108] Furthermore, this method essentially breaks the E2EE because the message is decrypted for scanning before it reaches the other end.[109]



Device: sends encrypted message to the enclave in the ESP server.

Secure enclave in the ESP server: decrypts the message and applies tools to detect child sexual abuse. If CSA is:
a) detected ⇨ forwards message for review and/or reporting
b) not detected ⇨ encrypts message end-to-end and forwards it to recipient

Device: receives and decrypts E2EE message

Figure 2.6 Altering encryption protocol.[110]

[107] SWD (2022) 209 final, 296.
[108] SWD (2022) 209 final 301-302.
[109] EDPB-EDPS Joint Opinion 04/2022 (n 51) 28.
[110] SWD (2022) 209 final, 301.

2.3 Conclusion

The proposal outlines three preliminary obligations for providers: conducting a risk assessment, implementing risk mitigation measures, and reporting these to the CA. However, the EDPS and EDPB are concerned about the objectivity and complexity of the risk assessment process and the vague terms for determining acceptable risk levels, which increases legal uncertainty.[111] After these steps, the CA can request a judicial authority to issue a detection order for CSAM and/or grooming, but the EDPS and EDPB criticize the vague conditions for such orders, which could lead to arbitrary decisions across MS. If issued, providers must follow Article 10's requirements. Although technology-neutral, the proposal's 'effectiveness' requirement poses challenges for E2EE providers. Proposed technical solutions include client-side and server-side scanning, each with various pros and cons.

[111] EDPB-EDPS Joint Opinion 04/2022' (n 51) 14 and 16.

III Privacy, data protection and (mass) surveillance: legal interpretations and limitations

This chapter will focus on the rights to privacy and data protection, particularly the limitations imposed on them in the context of (mass) surveillance and the perspectives of the CJEU and the ECtHR regarding these limitations in their (mass) surveillance jurisprudence. First, it will provide a brief overview of these rights. Secondly, it will delve into the level of protection offered by both courts. Thirdly, it will explore the specific boundaries for (mass) surveillance laid down by the CJEU in their case law. Finally, it will conclude with an interim conclusion. The central message is that the rights to privacy and data protection can be legitimately interfered upon by (mass) surveillance measures if these fulfil the conditions and safeguards set out by the (case) law. However, legitimate interference is only possible if the (mass) surveillance pertains to metadata; content data is always off-limits.

3.1 A brief overview of the rights to privacy and data protection

Article 8(1) ECHR protects the right to respect for private and family life, home and correspondence. The concept of 'private life' is broadly interpreted by the ECtHR and cannot be exhaustively defined.[112] It encompasses the right to build relationships with others and includes personal interactions falling under the notion of 'private life'[113] The ECtHR has ruled that 'private life' should not be interpreted strictly in relation to the processing of personal data.[114] However, the processing of personal data only falls under the protection of Article 8 ECHR when private life is affected. This occurs when there is a compilation of data on a specific person, through the processing or use of personal data, or when the disclosure of personal data goes beyond what was normally foreseen.[115] This interpretation extends to Article 7 CFR, which mirrors Article 8 ECHR in scope and meaning due to Article 52(3) CFR, stating that corresponding rights in the CFR have at least the same scope and meaning as laid down in the ECHR. This is also supported by the explanation of the CFR and the CJEU.[116] Additionally, the

[112] *Niemietz v. Germany*, 16 December 1992, §29, Series A no. 251-B; *Pretty v. the United Kingdom*, no. 2346/02, §61, ECHR 2002-III; *Peck v. the United Kingdom,* no. 44647/98, §57, ECHR 2003-I; Council of Europe and European Court of Human Rights, 'Guide on Article 8 of the European Convention on Human Rights: Right to Respect for Private and Family Life, Home and Correspondence' (2017) 16; Herke Kranenborg, 'Recht op eerbiediging van privé-, familie- en gezinsleven' in Gerrit-Jan Zwenne and Herke Kranenborg (eds), *Tekst & Commentaar Privacy- en gegevensbeschermingsrecht* (8th edition Wolters Kluwer 2022).

[113] *Breyer v. Germany* (n 32), paragraph 73.

[114] *Amann v. Switzerland* [GC], no. 27798/95, §65, ECHR 2000-II.

[115] *Breyer v. Germany* (n 32), paragraph 75.

[116] Explanations relating to the Charter of Fundamental Rights [2007] OJ C303/02 17 33; Judgement of 14 February 2019, *Sergejs Buivids v Datu valsts inspekcija,* C–345/17, EU:C:2019:122, paragraph 65; Herke Kranenborg, 'Recht op eerbiediging van het privéleven, het familie- en gezinsleven, de woning en de communicatie' in Gerrit-Jan Zwenne and Herke Kranenborg (eds), *Tekst & Commentaar Privacy- en gegevensbeschermingsrecht* (8th edition Wolters Kluwer 2022).

meaning and scope of Article 7 CFR are determined not only by the text of the ECHR but also by the case law of the ECtHR.[117] Regardless, this does not preclude that CFR rights can have a larger scope of protection than the equivalent rights in the ECHR.[118]

Furthermore, there is Article 8 CFR, which embodies the right to data protection in the CFR. Unlike Article 7 CFR, Article 8 CFR does not have a direct equivalent in the ECHR, but the right is contained within the ECtHR's case law on Article 8 ECHR. This leads to a complex relationship between Article 7 CFR and Article 8 CFR, because Article 7 CFR corresponds to Article 8 ECHR, including the ECtHR's case law on the protection of personal data.[119] Furthermore, in cases where the legality of interferences involving the processing of personal data is assessed, the CJEU systematically evaluates the issue in light of both the right to the protection of personal data and the right to respect for private life.[120] This indicates that Article 8 CFR covers – a substantial part of – Article 7 CFR in cases regarding the processing of personal data, because Article 8 CFR comes into play whenever personal data are processed without any privacy requirement.[121] However, some scholars suggest that instead of conceiving Article 7 and 8 CFR in parallel, Article 8 CFR is to be seen as a *lex specialis*; its normative underpinning is derived not from its wording but from secondary EU legislation and CJEU's and ECtHR's case law, which emphasizes the value of Article 8 CFR to protect the individual's control over their personal data.[122]

Nevertheless, these rights are not absolute and can be subject to legitimate interference under Article 8(2) ECHR or Article 52(1) CFR. Both the ECtHR and the CJEU have established a level of protection in the context of (mass) surveillance through the criteria for assessing the legitimacy of the interfering measure, determining when such interferences are permissible.

[117] Explanations relating to the Charter of Fundamental Rights (n 117) 32-33.
[118] Article 52(3) CFR.
[119] *Digital Rights Ireland* (n 19) paragraphs 34-36; Tobias Lock, 'Article 8 CFR' in Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (Oxford University Press 2019) 2122-2123;
[120] Herke Kranenborg, 'Recht op bescherming van persoonsgegevens' in Gerrit-Jan Zwenne and Herke Kranenborg (eds), *Tekst & Commentaar Privacy- en gegevensbeschermingsrecht* (8th edition Wolters Kluwer 2022).
[121] Council of Europe and others, *Handbook on European Data Protection Law – 2018 Edition* (Publications Office of the European Union 2018) 19-20; Manon Oostveen, 'Why Privacy ≠ Data Protection (and How They Overlap) – Digital Society Blog' (*HIIG*, 4 May 2016) <www.hiig.de/en/why-privacy-≠-data-protection-and-how-they-overlap/> accessed 19 April 2024.
[122] Orla Lynskey, 'The Data Retention Directive Is Incompatible with the Rights to Privacy and Data Protection and Is Invalid in Its Entirety: *Digital Rights Ireland*' (2014) 51 Common Market Law Review 1789 1808; Orla Lynskey, 'Control over Personal Data in a Digital Age: Google Spain v AEPD and Mano Costeja Gonzalez' (2015) 78 The Modern Law Review 522 529; Lock (n 120) 2123; Kranenborg (n 113).

3.2 Level of protection

Since the proposal is secondary EU law, the CJEU emphasizes that the examination of the measure's interference "must be undertaken solely in the light of the fundamental rights guaranteed by the Charter."[123] According to Article 52(1) CFR, an interference is legitimate if the measure (i) is provided for by law, (ii) respects the essence of the rights, (iii) is subject to the principle of proportionality, and (iv) is necessary and genuinely meets objectives of general interest recognized by the Union. However, under Article 6(3) of the Treaty on European Union ('TEU') and Article 52(3) CFR, the CJEU, when analysing the conditions of Article 52(1) CFR, must also consider the criteria of Article 8(2) ECHR as interpreted in the case law of the ECtHR.[124] The criteria in Article 8(2) ECHR are as follows: (1) in accordance with the law (similar to the first conditions of the CFR), (ii) pursuing a legitimate aim (similar to the last condition of the CFR), and (iii) necessary in a democratic society (similar to the third condition of the CFR. The term "the essence of the right" is unique to Article 52(1) CFR and does not have a direct equivalent in Article 8(2) ECHR.[125]

Firstly, the measure must be provided for by law. According to both the ECtHR and the CJEU, this requirement implies that the interfering measure must have a basis in law that is in the public domain in some way.[126] Furthermore, this law should be accessible and foreseeable, adhering to the rule of law.[127] In legal terms, 'accessible' means citizens should have clear guidance on applicable rules, 'foreseeable' means norms must be precise for behaviour regulation, and adherence to the rule of law requires clear definitions to prevent arbitrariness in limitations on rights.[128] However, it can also be formulated in terms which are sufficiently open to be able to adapt to different scenarios and keep pace with changing circumstances.[129] Moreover, requiring full foreseeability would dimmish the effectiveness of (mass) surveillance. Thus, this requirement in the context of (mass) surveillance does not obligate MS to enact legal provisions listing exhaustively detailed situations that may prompt a decision to initiate such

[123] EDPS, 'Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit' (17 April 2017) <www.edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf> accessed 20 July 2024 6.
[124] ibid.
[125] Sébastien Van Drooghenbroeck and Cecilia Rizcallah, 'The ECHR and the Essence of Fundamental Rights: Searching for Sugar in Hot Milk?' (2019) 20 German Law Journal 904 909.
[126] Eleni Kosta, *Surveilling Masses and Unveiling Human Rights - Uneasy Choices for the Strasbourg Court* (PrismaPrint 2017) 24-25.
[127] Ilina Georgieva, 'The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Article 17 ICCPR and Article 8 ECHR' (2015) 31 Utrecht Journal of International and European Law 104 118.
[128] The Sunday Times *v. the United Kingdom (no 1),* 26 April 1979, §49 and 87, Series A no. 30; Kosta (n 127) 24; Kranenborg (n 113).
[129] Judgement of 21 June 2022, *Ligue des droits humains*, C-817/19, EU:C:2022:491, paragraph 114.

surveillance operations. Domestic law must provide citizens with clear indications regarding the circumstances and conditions under which security actors are authorized to access private sector databases. This entails specifying the extent of discretion granted to competent authorities and outlining how this discretion will be exercised clearly enough to protect individuals against arbitrary interference. Specifically, the law should establish objective criteria linking the data to be transferred with the objectives pursued, ensuring a clear and precise delineation of the scope of data transfer. Furthermore, it is crucial to define in concrete terms the nature of offenses for which data is collected and transferred to law enforcement authorities, especially in the context of mass surveillance where only serious criminal offenses are considered.[130]

Additionally, the interfering measure must respect the essence of the right. Although this notion is not explicitly stated in Article 8(2) ECHR, the protection of the essence of the fundamental right can be found in Article 17 ECHR.[131] The primary purpose of this concept is to prevent the core of a fundamental right from being undermined or rendered impossible to exercise. In terms of the CJEU, the interference cannot "call into question" the fundamental right itself. Meaning that the interference should not make it impossible to exercise the fundamental right.[132] According to Brkan, this safeguard serves to protect fundamental rights against extreme interferences that lack justification, as a lack of justification can prevent a proper proportionality assessment and potentially impair the essence of the fundamental right.[133] The only real-life example where the essence was compromised is the Schrems case, where the CJEU ruled that "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded *as compromising the essence* of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter".[134]

[130] Plixavra Vogiatzoglou, 'Mass Surveillance, Predictive Policing and the Implementation of the CJEU and ECtHR Requirement of Objectivity' (2019) 10 European Journal of Law and Technology <https://www.ejlt.org/index.php/ejlt/article/view/669> accessed 16 March 2024 6.
[131] Van Drooghenbroeck and Rizcallah (n 126) 908.
[132] Maja Brkan, 'The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning' (2019) 20 German Law Journal 864 869.
[133] ibid 868.
[134] Emphasis added; *Schrems I* (n 34), paragraph 94.

Thirdly, the interfering measure must adhere to the principle of proportionality. This principle can be divided into three cumulative sequential sub-tests: suitability, necessity and proportionality *stricto sensu*.[135]

Firstly, the suitability test is a preliminary assessment to determine whether the measure is appropriate for achieving its stated objectives.[136] The outcome of the suitability test is simple; the measure is suitable or unsuitable. Yet, within the suitability test lies a nuance: the judicial scrutiny upon the objectives themselves.[137] Namely, the measure taken must genuinely meet objectives of general interest recognized by the Union. These include a variety of general objectives of the EU which are affirmed in Article 3 TEU, such as the promotion of peace and of the well-being of its peoples, security and justice in which free movement of persons is ensured, in conjunction with appropriate measures to prevent and combat serious crime.[138] Within the context of (mass) surveillance measures often the interests of preventing and fighting serious crime in order to ensure public security are pursued by the MS. Both courts have affirmed that these interests are suitable to employ (mass) surveillance measures.[139] For example, data retention can be suitable for fighting serious crime as it enables law enforcement to access past data crucial for such investigations.[140]

Secondly, the chosen measure must be necessary, meaning that no other suitable, equally effective, but less restrictive measures are available to achieve the same goal.[141] However, this does not mean the interference with the fundamental right must be minimal; rather, it should be precisely tailored to its goal.[142]

Lastly, the measure must be proportional in *stricto sensu*, striking a balance between the benefits to the public and the harm to fundamental rights. This involves a careful assessment of the benefits gained versus the impact on individual rights.[143] In comparison to the other sub-tests, has proportionality *stricto sensu* a 'moral nature' and is not a 'threshold judgement',

[135] Lorenzo Dalla Corte, 'On Proportionality in the Data Protection Jurisprudence of the CJEU' (2022) 12 International Data Privacy Law 259 261.
[136] ibid 267.
[137] ibid.
[138] Explanations relating to the Charter of Fundamental Rights (n 117) 17-35.
[139] *Digital Rights Ireland* (n 19), paragraphs 41-44; Judgement of 6 October 2020, *La Quadrature du Net*, joined cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 126; Kranenborg (n 100).
[140] Dalla Corte (n 136) 267.
[141] Eva Brems and Laurens Lavrysen, '"Don't Use a Sledgehammer to Crack a Nut": Less Restrictive Means in the Case Law of the European Court of Human Rights' (2015) 15 Human Rights Law Review 139 142.
[142] Ioannis Kouvakas, 'The Watson Case: Another Missed Opportunity for Stricto Sensu Proportionality' (2017) 2 Cambridge Law Review 173 177.
[143] Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* (Cambridge University Press 2012) 321.

because it is a value-laden comparison meant to determine whether the relation between the benefit and the harm deriving from an interference with a fundamental right is proper.[144] Yet, it should be noted that in practice the CJEU merges the necessity test and the proportionality *stricto sensu* into one. Namely because the necessity test entails devising suitable means that provide for a lower interference than the ones employed by the measure challenged: that requires comparing the means that have been adopted with entirely hypothetical alternatives, an exercise which can easily verge towards *stricto sensu* proportionality's axiological nature.[145] This results in the CJEU often focusing on the necessity sub-test and incorporating considerations that might (also) pertain to the proportionality sub-test.

3.3 Safeguarding from (mass) surveillance

CSS and server-side scanning are both content scanning methods that can be used to discover if the user is transmitting harmful content, such as CSAM. Essentially, they are surveillance methods.[146] For this reason, it is important to delve into the specific parameters established by the CJEU regarding (mass) surveillance methods. Over the years, the CJEU, in conjunction with the ECtHR, has developed a body of case law concerning (mass) surveillance, in which they established certain safeguards for the protection of the rights to privacy and data protection.[147] This case law is crucial when assessing the principle of proportionality. For a period of time, it was thought that the Courts were aligned.[148] However, recent cases like *Centrum for Rättvisa v. Sweden*[149] and *BBW*[150] suggest a divergence between the CJEU and ECtHR, with the latter deviating from the high standards set by the CJEU and leaning towards a less privacy-friendly approach.[151] Due to this divergence and word limitations, the next section will mostly focus on the parameters established in CJEU cases.

Digital Rights Ireland ('DRI') marked a crucial moment when the CJEU established a strict scrutiny test for measures that seriously interfere with human rights. It applied a rigorous proportionality test under the CFR and clarified the boundaries of privacy and data protection.

[144] Dalla Corte (n 136) 270.
[145] ibid.
[146] Abelson and others (n 95) 8.
[147] Kosta (n 127) 42 203.
[148] Mitsilegas and others (n 42)
[149] Centrum för rättvisa v. Sweden [GC], no. 35252/08, 25 May 2021.
[150] *Big Brother Watch and Others v. the United Kingdom* (n 20).
[151] Watt, 'Much Ado About Mass Surveillance - the ECtHR Grand Chamber "Opens the Gates of an Electronic 'Big Brother' in Europe" in Big Brother Watch v UK' (n 49); Mitsilegas and others (n 42) 201-205.

Furthermore, it outlined parameters for legislators when designing data retention schemes.[152] Essentially, *DRI* requires guarantees at all stages of the data processing cycle, including data collection, retention conditions, access, use and monitoring.[153] In *DRI*, the CJEU set the first parameters, requiring clear and precise rules defining the extent of the interference.[154] This entails the following. Firstly, the CJEU deemed indiscriminate data retention in law enforcement unacceptable. Data collection is only permissible in situations threatening public security, limiting measures to a specific time period, geographical area, or individuals likely involved in serious crimes, or to persons whose data could contribute to law enforcement.[155] Secondly, regarding access to collected data, retroactive access and use of retained data should be strictly necessary, adhering to procedural and substantive conditions. Access by national authorities should be limited to preventing, detecting, and prosecuting precisely defined serious offenses. Requests for data access should be reasoned and subject to prior review by a court or an independent administrative body ensuring compliance with constitutional and legislative limits on data access and use. Safeguards should authorize only a limited number of persons to access and use data in line with specific requests.[156] The second parameter concerned the retained data. The CJEU emphasized the need for effective mechanisms to ensure a very high level of protection and security. Specifically, data retention should be under the control of an independent authority and located within the EU.[157]

A year later, the CJEU made another important decision in *Schrems I*.[158] This case is a crucial factor for (mass) surveillance measures as it establishes a minimum standard for what constitutes 'forbidden territory'. Specifically, the CJEU ruled in this case that legislation allowing "public authorities to have access on a generalized basis to the content of electronic communications" violates the essence of the fundamental right to privacy.[159] Additionally, they

[152] Marie-Pierre Granger and Kristina Irion, 'The Court of Justice and The Data Retention Directive in Digital Rights Ireland: Telling Off The EU Legislator and Teaching a Lesson in Privacy and Data Protection' (2014) 39 European Law Review 834 844.
[153] ibid 848.
[154] *Digital Rights Ireland* (n 19), paragraph 54; ibid 842 - 843.
[155] ibid, paragraphs 57 – 59; ibid 848.
[156] ibid, paragraphs 61 – 62; ibid 849.
[157] Article 29 Data Protection Working Party, 'Statement on the Ruling of the Court of Justice of the European Union (CJEU) Which Invalidates the Data Retention Directive 14/EN WP 220' <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp220_en.pdf> accessed 20 May 2024 2.
[158] *Schrems I* (n 34); *Digital Rights Ireland* (n 19), paragraphs 57-61.
[159] ibid, paragraph 93; Brkan (n 133) 875.

determined that the essence of the right to effective judicial protection was also violated because EU citizens lacked any legal remedies to access, modify, or erase their personal data.[160]

Later, the CJEU followed up on *DRI* in the Tele2/Watson case ('Tele2'). In this case, the CJEU closely adhered to the principles established in *DRI* and reiterated that any interference must be related to serious crime, with clear and precise rules defining the scope and application of data retention, along with minimum safeguards for effective protection.[161] In addition to these reiterations, the CJEU introduced two safeguards. First, it stated that once there was no danger to the investigation, individuals affected should be notified, granting them the opportunity to exercise their right to a remedy.[162] Secondly, the implementation of data processing measures must be effectively supervised by a judicial body or at least by an independent authority.[163]

After *DRI* and *Tele2*, the CJEU further elaborated on data retention in *Privacy International* ('PI') and *La Quadrature du Net* ('LQDN'). The novelty of these later cases lies not in the standards the CJEU used, but in how these standards were applied. In *PI*, the standards were applied to the transmission of data instead of retention, while in *LQDN*, the standards were applied to legislation aimed at protecting national security rather than combating serious crime.[164] In *PI*, the CJEU stated that the transmission of data to intelligence services was to be treated on par with data retention and access.[165] Therefore, the same requirements stemming from the principle of proportionality should apply. The general and indiscriminate transmission exceeds the limits of what is strictly necessary, because there is no link between the persons affected and the objective of national security. In *LQDN*, the CJEU diverged and stated that general and indiscriminate retention of data can be permissible, but only in the case of *national security* and under specific conditions. The CJEU bars legislation mandating general and indiscriminate data retention for combatting serious crime, even if the governments have positive obligation under Article 3, 4 and 7 CFR. Once more, the CJEU supported the targeted

[160] ibid, paragraph 95; ibid 868.

[161] *Tele2/Watson* (n 35), paragraphs 109 – 111; Lorna Woods, 'EU Law Analysis: Data Retention and National Law: The ECJ Ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber)' (*EU Law Analysis*, 21 December 2016) <https://eulawanalysis.blogspot.com/2016/12/data-retention-and-national-law-ecj.html> accessed 20 April 2024.

[162] ibid, paragraph 121; ibid.

[163] ibid, paragraph 123; Vogiatzoglou (n 131) 7; 'Joined Cases Tele2 Sverige AB v Post- Och Telestyrelsen and Secretary of State for the Home Department v. Watson' (*Global Freedom of Expression*) <https://globalfreedomofexpression.columbia.edu/cases/joined-cases-tele2-sverige-ab-v-post-och-telestyrelsen-c-20315-secretary-state-home-department-v-watson/> accessed 20 May 2024.

[164] Eskens (n 37) 147.

[165] Judgement of 6 October 2020, *Privacy International*, C-623/17, EU:C:2020:790, paragraph 41.

retention of traffic and location data for combatting serious crime. Additionally, in 2022, the CJEU reaffirmed its stance from *LQDN* in its *SpaceNet* ruling.[166]

Until recently, these were the established safeguards; however, a recent judgment changed the 'prior review' safeguard.[167] In short, the CJEU ruled that prior review by a court or an independent body is not required for access to retained data if the access is not considered a serious interference.[168]

To summarize, the following points can be distilled from the explanation above for assessing the proportionality principle: firstly, if the interference with the rights to privacy and data protection is serious, prior review or authorization is required to access private sector databases.[169] Secondly, there should be clear and objective criteria for data access and usage by competent authorities.[170] Thirdly, effective supervision by independent authorities over the competent authorities is necessary, especially if personal data is transferred to different authorities.[171] Fourthly, during data retention, security and protection must be ensured through appropriate technical and organizational means.[172] Fifthly, individuals subject to these measures should be notified of data access, unless notification would jeopardize the objective being served. Sixthly, subjected individuals must have an effective remedy to obtain information or access to data related to them.[173]

Lastly, it should be underscored that the aforementioned conditions, and thus the allowance of (mass) surveillance measures, apply only to the retention and transmission of traffic and location data (i.e., metadata). However, the implied technical measures involve scanning the actual content of communications, which could be deemed to compromise the essence of the right to privacy and may be considered illegitimate without even assessing the principle of proportionality.

[166] Alessandra Silveira and Tiago Sérgio Cabral, 'Again: On the Prohibition of Generalised and Indiscriminate Retention of Metadata for the Purpose of Combating Serious Crime' (*Official Blog of UNIO*, 6 October 2022) <https://officialblogofunio.com/2022/10/06/again-on-the-prohibition-of-generalised-and-indiscriminate-retention-of-metadata-for-the-purpose-of-combating-serious-crime/> accessed 28 April 2024.
[167] *Hadopi* (n 38), paragraphs 124-131.
[168] Marco Mauer, 'The Unbearable Lightness of Interfering with the Right to Privacy' [2024] Verfassungsblog <https://verfassungsblog.de/the-unbearable-lightness-of-interfering-with-the-right-to-privacy/> accessed 24 July 2024.
[169] Vogiatzoglou (n 131) 6; Mauer (n 166).
[170] ibid.
[171] ibid 7.
[172] ibid.
[173] ibid.

3.4 Conclusion

If one only looks at the conditions in Article 52(1) CFR and Article 8(2) ECHR, one could conclude that they are quite similar in scope and meaning, which could lead to similar legitimate limitations on both rights in both legal frameworks. Although the Courts were initially aligned in their interpretations of these conditions, they have recently begun to diverge. The CJEU addresses the limitations in a more privacy-friendly manner, resulting in a stricter regime for (mass) surveillance, particularly for fighting serious crime, with numerous safeguards. In contrast, the ECtHR has adopted a more lenient approach towards (mass) surveillance and is more willing to impose limitations on privacy and data protection in the interest of public security, such as national security and combating serious crime.

IV Exploring the legitimacy of the technical measures

After reviewing the proposal's technical aspects, including privacy rights and surveillance boundaries, it is crucial to assess if these measures align with legal frameworks. This chapter will analyse this alignment, synthesize relevant chapters, and explore conflicts between public security and privacy. Finally, it will offer a conclusion, focusing on whether the proposal's technical measures create such conflicts. This chapter focuses on the final sub-question: do the technical measures that are implied by the proposal engender a conflict between public security and privacy, and if yes, how?

4.1 Technical measures: legitimate or not?

Before proceeding with the assessment, a recap is necessary: in Chapter 2, technical measures form part of the detection order regime. Providers assess risks, report to the CA, and may receive a detection order if evidence of risk exists. Providers then employ technologies to detect harmful content, choosing methods as per the requirements of Article 10(3) of the proposal. Due to E2EE, providers face a choice: CSS or server-side scanning. These measures must comply with Article 52(1) CFR, ensuring that they are provided for by law, respect the essence of the rights, and adhere to the principle of proportionality. While the first two conditions are universal for CSS and server-side scanning, proportionality must be assessed individually because of the individual features of the technologies. Lastly, it is important to mention that, normally, the CJEU would not proceed with their assessment if they deem a requirement not fulfilled, however, due to the level of disputability of the interpretation of the requirements and for the sake of the completeness of this research all three conditions will be assessed.[174]

4.1.1 Provided for by law

This condition requires that the framework for detection orders and, consequently, the technical measures, have a basis in the law, are accessible, foreseeable, and adhere to the rule of law. Additionally, the EDPB and EDPS stressed that given the potentially significant impact on a large number of data subjects (potentially all users of interpersonal communication services), there needs to be a high level of legal certainty, clarity, and foreseeability of the legislation to ensure that the proposed measures are genuinely effective in achieving their objectives while being the least detrimental to the fundamental rights at stake.[175] On the other hand, the legislator

[174] Koen Lenaerts, 'Limits on Limitations: The Essence of Fundamental Rights in the EU' (2019) 20 German Law Journal 779 786.

[175] EDPB-EDPS Joint Opinion 04/2022 (n 51) 15.

can formulate the proposed Regulation with sufficiently open terms to be able to adapt to changing circumstances and to not dimmish the effectiveness of the surveillance.

In this context, Articles 7 and 10 of the proposal need to be assessed, as they impose the obligation on providers to install and operate the technical measures. Notably, Articles 7(8) and 10(2)(3) of the proposal aim to provide clarity and precision while maintaining technological neutrality. Article 7(8) of the proposal discusses the use of '*sufficiently reliable detection technologies*' that limit errors regarding detection and their impact on users' rights, while also requiring the use of the least intrusive measures. Similarly, Article 10(2) of the proposal emphasizes technology neutrality, stating that 'providers shall not be required to use any specific technology,' and Article 10 (3) of the proposal reiterates the objectives outlined in Article 7(8) of the proposal. In essence, the choice of technology is left to the providers, as the proposal only sets out parameters within which they must operate.[176]

However, one could argue that the EU Centre, by providing technologies in consideration of the requirements, offers some guidance, and by extent accessibility and foreseeability, to the providers. Nonetheless, using these provided technologies does not alter the providers' responsibility to comply with the requirements, leaving them with a similar range of choices.[177] The lack of accessibility, foreseeability, and adherence to the law is further illustrated by the impact assessment report of the EC. The report discusses *'possible solutions*,' indicating that there is no definitive answer on which technical measures to take.[178] It simply lists numerous technical solutions that would 'fit' the conditions set out in the proposal.

Yet, it is of the utmost importance to know what technology is used and how it is employed to understand the limitations it imposes. For instance, CSS can be employed at the app level (e.g. WhatsApp or Signal) or it can be employed on the whole operating system (e.g. your whole phone).[179] This choice significantly affects the limitations on the rights to privacy and data protection, as in the former case only the specific app is scanned, while in the latter, everything on the device is subject to scanning.

However, despite the aforementioned, due to the latitude afforded to the legislator in formulating the terms, this point can also be debated as to whether the technical measures are provided for by law.

[176] Opinion Legal Service (n 53) 8.
[177] COM (2022) 209 final, ch II, art 10(1)-(3).
[178] SWD (2022) 209 final, 288.
[179] Abelson and others (n 95) 24.

4.1.2 Respect the essence of the right

A detection order for E2EE providers would inherently entail some form of CSS or sever-side scanning. CSS is inherently an indiscriminate and untargeted method of access to content of electronic communications as it scans the data before it gets encrypted and for it to be effective it has to scan every bit of content to signal potential CSAM or grooming.[180] This same line of reasoning can be projected on server-side scanning, but with this method it is done on the server instead of the client itself.

On the other side, the EC's impact assessment report highlighted that they only considered solutions that respect fundamental rights and Article 10(3)(b) of the proposal specifies that the technology service providers use must only extract the minimum information necessary to detect CSAM or grooming, conform to industry standards, and be the least intrusive option available. However, it is crucial to note that not extracting irrelevant communication does not automatically exclude the need to screen all interpersonal communication data of every user, even those with no evidence of any link to child sexual abuse offenses.[181] Moreover, according to van Daalen, it also does not matter if the analysed content is hashed or unhashed, because it still requires a form of analysis of all the content.[182]

Taking this into consideration, in the case of *Schrems I*, the CJEU ruled that legislation allowing public authorities access on a generalized basis to electronic communications compromises the essence of the fundamental right to privacy guaranteed by Article 7 CFR.[183] Therefore, it can be concluded that the implied technical measures pose a serious risk of compromising the essence of privacy and data protection rights. This is especially true as the technical measures seek to authorize access on a generalized, through automated and systemic surveillance, to the content of electronic communications and personal data of all users, regardless of any direct or indirect link to child sexual abuse activities.

While it is highly likely that the technical measures compromise the essence of the right, it is still important to assess their compliance with the principle of proportionality. Because *Schrems I* is the only case that was decided on this issue, so strong substantiation on this matter is scarce. However, even if these measures pass the test of respecting the essence,

[180] Ludvigsen, Nagaraja and Daly (n 101) 1.
[181] COM (2022) 209, ch I, art 1(1); Opinion Legal Service (n 53) 19.
[182] van Daalen (n 18) 15.
[183] *Schrems I* (n 34), paragraoh 94.

they would still impose serious limitations on privacy and data protection rights, as all content data is automatically analysed and proportionality still needs to be assessed.[184]

4.1.3 Proportionality

4.1.3.1 Suitability

The proposal's objective is to address the misuse of online services for CSA within the internal market.[185] This objective aligns with the EU's recognition of combating serious crime as a matter of general interest, particularly concerning the protection of children from exploitation and child pornography, which the CJEU has emphasized as inherently serious issues.[186] It is without a doubt that the pursued objective is an objective of general interest recognized by the Union. However, questions arise regarding the suitability of the proposed detection orders and subsequent technical measures in achieving this objective and their alignment with the stated goal.

To begin, all detection orders,[187] and consequently all implied technical measures, are suitable for addressing the objective of the Regulation, as they can detect some form of CSAM or grooming, thereby tackling the misuse of online services for CSA. While this is a binary assessment, it should be noted that some variants are 'more suitable' for addressing the objective than others, as they can fulfil all the different detection orders. Specifically, CSS on the client and CSS using a remote server can only detect known CSAM; moreover, is CSS on the client limited by its smaller database.[188] In contrast, CSS with ML and server-side scanning can detect both known and new CSAM and grooming. The key distinction for CSS with ML lies in the use of classifiers, which are sent to the client and function more like parameters, rather than relying on hashes as the other CSS methods do. Server-side scanning decrypts the message on the server, allowing the provider to detect CSAM or grooming as if E2EE were not in place.[189]

Moreover, doubts emerge regarding the genuine nature of the objective.[190] The deployment of detection methods indiscriminately across all devices, rather than specifically targeting known or suspected perpetrators of CSAM, raises concerns. Some, including the president of the EDPS, suggest that the EU may be leveraging children's rights as a guise for

[184] *La Quadrature du Net and Others* (n 140), paragraph 174.

[185] COM (2022) 209 final, ch I, art 1(1).

[186] *Digital Rights Ireland* (n 19), paragraph 126; *Ligue des droits humains* (n 130), paragraph 149.

[187] Detection order for: known CSAM (1), new CSAM (2), and grooming (3).

[188] SWD (2022) 209 final, 296.

[189] SWD (2022) 209 final, 301.

[190] Although, in the (leaked) legal service document of the Council they state that the objective is undoubtedly to protect children and combat grooming and dissemination of CSAM. See: Opinion Legal Service (n 53) 11.

broader surveillance initiatives.[191] This prompts debate about whether the true objective is child protection or if it aligns with objectives that intrude upon personal data protection.[192] However, further exploration of this topic falls outside the scope of this thesis.

4.1.3.2 Necessity

Are all the detection orders, and consequently the technical measures, necessary to achieve the objective, or are there other suitable, less infringing measures that can accomplish the same goal just as effectively? It is important to note that due to differences in detection orders, the detection order for known CSAM will be discussed separately from the other two.

First, is a detection order for known CSAM necessary, or are there less infringing measures that can accomplish the same objective in addressing known CSAM? While Ludvigsen et al. suggest alternative measures, they do not offer concrete solutions.[193] Rosenzweig, on the other hand, proposes methods such as disrupting CSAM discovery on the dark web and examining non-encrypted public conduct to identify potential malicious behaviour. These approaches, including encouraging user reporting and limiting dissemination capabilities, have shown effectiveness in hindering CSAM distribution.[194] To add to the alternatives Rosenzweig lists, Wilson and Michel state that fully homomorphic encryption ('FHE') is a viable solution for this objective.[195] FHE allows image scanning while data remains encrypted, eliminating the need to scan content before encryption.[196]

[191] EDRi, 'Is Surveilling Children Really Protecting Them? Our Concerns on the Interim CSAM Regulation' (*European Digital Rights (EDRi)*) <https://edri.org/our-work/is-surveilling-children-really-protecting-them-our-concerns-on-the-interim-csam-regulation/> accessed 25 May 2024; Natasha Lomas, 'Europe's CSAM-Scanning Plan Is a Tipping Point for Democratic Rights, Experts Warn' (*TechCrunch*, 24 October 2023) <https://techcrunch.com/2023/10/24/eu-csam-scanning-edps-seminar/> accessed 21 May 2024; Viktoria Tomova, 'Guise of "Children's Rights" Weakens Internet Privacy Laws and Increases Mass Surveillance | TechPolicy.Press' (*Tech Policy Press*, 13 December 2023) <https://techpolicy.press/guise-of-childrens-rights-weakens-internet-privacy-laws-and-increases-mass-surveillance> accessed 21 May 2024.

[192] See example: Apostolis Fotiadis Zandonini Luděk Stavinoha, Giacomo, 'Europol Sought Unlimited Data Access in Online Child Sexual Abuse Regulation' (*Balkan Insight*, 29 September 2023) <https://balkaninsight.com/2023/09/29/europol-sought-unlimited-data-access-in-online-child-sexual-abuse-regulation/> accessed 21 May 2024.

[193] Ludvigsen, Nagaraja and Daly (n 101) 12.

[194] Paul Rosenzweig,'The Law and Policy of Client-Side Scanning' (*Default*) <www.lawfaremedia.org/article/law-and-policy-client-side-scanning> accessed 2 May 2024; 'Encryption and Lawful Access: Evaluating Benefits and Risks to Public Safety and Privacy | United States Senate Committee on the Judiciary' <https://www.judiciary.senate.gov/committee-activity/hearings/encryption-and-lawful-access-evaluating-benefits-and-risks-to-public-safety-and-privacy> accessed 25 May 2024 (see 'QFRS p 7' from J. Sullivan.

[195] Optalysys, 'FHE: An Alternative to Client-Side Scanning?' (*Optalysys*, 31 July 2023) <https://medium.com/optalysys/fhe-an-alternative-to-client-side-scanning-e58491b1c00> accessed 23 May 2024; Tim Bernard, 'The Landscape of CSAM Detection: Challenges and Innovations' <www.unitary.ai//articles/the-present-and-future-of-detecting-child-sexual-abuse-material-on-social-media> accessed 25 May 2024.

[196] Hany Farid, 'An Overview of Perceptual Hashing' (2021) 1 Journal of Online Trust and Safety <https://tsjournal.org/index.php/jots/article/view/24> accessed 24 May 2024 16.

From the aforementioned alternatives, it can be deduced that a detection order for known CSAM, and thus for CSS on the client and for CSS with a remote server, may not be necessary to achieve the objective, as there are less restrictive measures available. Consequently, this measure may be deemed disproportionate, failing to adhere to the principle of proportionality. Thus, the assessment of proportionality *stricto sensu* may not be necessary given the disproportionate nature of this technical measure.

To continue, are the detection orders for new CSAM and grooming, and thus for CSS with ML and server-side scanning, necessary? The necessity of these detection orders arises from the lack of alternatives capable of detecting new CSAM and grooming, thus hindering the achievement of the objective. According to Lee et al. and several other sources, the only effective way to detect new CSAM is through the use of ML and classifiers, i.e. using detection technology such as CSS with ML or server-side scanning.[197] Similarly, the necessity of addressing grooming is highlighted by al-Khateeb and Epiphaniou, who assert that such detection measures are crucial despite the availability of other mitigation measures.[198] This underscores the necessity of these orders, as without them, and the technologies that enable detection, the objective of addressing the misuse of services for distributing new CSAM and grooming would not be met.

4.1.3.3 Proportionality stricto sensu

Finally, the new CSAM and grooming detection orders and subsequent usage of the technical measures must adhere to proportionality *stricto sensu*, ensuring a balance between the benefits gained and the impact on fundamental rights.[199] In other words, they must effectively detect (new) CSAM and grooming to address the misuse of providers' services while minimizing interference with individuals' private communication

To start, the CJEU stipulates that limitations to the rights of privacy and data protection should be the exception not the rule and that there cannot be a general and indiscriminate restriction of the rights of privacy and data protection, but the limitation has to be targeted, limited and nuanced.[200] In this light the parameters for (mass) surveillance come into play as they apply substantive and procedural safeguards to the measure e.g. who is subjected, who has

[197] Bernard (n 194); ‘Explaining the Technology for Detecting Child Sexual Abuse Online’ (*CRIN*, 10 November 2023) <https://home.crin.org/readlistenwatch/stories/explainer-detection-technologies-child-sexual-abuse-online> accessed 25 May 2024; Hee-Eun Lee and others, ‘Detecting Child Sexual Abuse Material: A Comprehensive Survey’ (2020) 34 Forensic Science International: Digital Investigation 301022 7.
[198] Haider M al-Khateeb and Gregory Epiphaniou, ‘How Technology Can Mitigate and Counteract Cyber-Stalking and Online Grooming’ (2016) 2016 Computer Fraud & Security 14 14-15.
[199] *La Quadrature du Net and Others* (n 140), paragraph 131.
[200] *Tele2/Watson* (n 35), paragraphs 89 and 104; *La Quadrature du Net* (n 140), paragraphs 111 and 142.

access, and how long can the measure be deployed. This is to ensure that the inference that these detection orders cause is limited to what is strictly necessary to achieve the objective. Here it is also important to stress that the CJEU stated in *LQDN* that the need to ensure that the interference is limited to what is strictly necessary is all the greater where personal data are subjected to automated processing, particularly where there is a significant risk of unlawful access to data.[201]

The proposal includes several safeguards. First, the CA requesting a detection order must target and specify the order to minimize harm and ensure a fair balance between fundamental rights. In this light, the CA has to take into account relevant parameters, which includes the availability of sufficiently reliable technologies, the impact the measures have on the parties affected and require the taking of the least intrusive measures from among several equally effective measures.[202] Additionally, the duration of detection order deployment should be limited to what is strictly necessary, but cannot be longer than 24 months for CSAM or 12 months for grooming and, where possible, CSS will only be deployed to a part or component to which the risk is limited.[203] Furthermore, the issuance of a detection order must involve independent judicial oversight, and providers and affected users have the right to challenge the order in court.[204] For the providers there is another set of additional safeguards when a detection order is issued. They have to ensure regular human oversight to ensure the reliability and intervene in the case of errors.[205] Secondly, they have to establish a complaint mechanism for users and have to inform the users of the kinds of detection technologies they use, how they work and what that means for the confidentiality of the communications and that findings must be reported to the EU-Centre and inform them on their rights to redress and complaints.[206] Lastly, the providers must take measures to ensure that when detection is deployed that the technologies and processed data are solely and strictly used for executing the detection order.[207]

These safeguards seem promising; there several procedural and substantive safeguards, such as a time limit, the detection shall, where it is possible, only be deployed to a specific part

[201] *La Quadrature du Net* (n 140); Judgement of 16 July 2020, *Schrems II,* C-311/18, EU:C:2020:559, paragraph 176.
[202] COM (2022) 209 final, ch II, art 7(8).
[203] COM (2022) 209 final, ch II, art 7(8)(9).
[204] COM (2022) 209 final, ch II, art 7(1) and art 9(1).
[205] COM (2022) 209 final, ch II, art 10(4)(c).
[206] COM (2022) 209 final, ch II, art 10(4)(d).
[207] COM (2022) 209 final, ch II, art 10(4)(a)(b) and 10(5).

or component of the service, and there is judicial oversight when the measure is issued. However, the proposal lacks in several areas when placing safeguards.

First, is it unclear under what circumstances and conditions the detection will be applied, as noted by the EDPB and the EDPS in their opinion.[208] They stated that the conditions for issuing a detection order, including CSS or server-side scanning deployment, were vague, leading to legal uncertainty and potential arbitrary application across different MS.[209] Additionally, and order is likely to be deployed to the entire service rather than specific parts, as the proposal states that a detection order applies if there is a significant risk of CSAM or grooming use within the service. Therefore, an order, and as a consequence CSS with ML or server-side scanning, will affect all users.[210] Moreover, while there is independent oversight during an issuance of an order, ongoing supervision for evaluation of the detection order is handled by the CA responsible for combating online CSA, raising concerns about its independence.[211] In essence, the proposal fails to adhere to the CJEU's parameters for (mass) surveillance: the detection lacks targeting, deployment conditions are unclear, and implementation oversight lacks independence.

Zooming in on the specific technical measures there are additional concerns. To start, the EDPS and EDPB emphasize that encryption technologies, particularly E2EE, are crucial for protecting the rights to privacy and data protection, and their use should not be prevented or discouraged. In the context of these detection orders, server-side scanning could be a potential technical solution to fulfil the requirements. However, server-side scanning is fundamentally incompatible with E2EE, as it would break the end-to-end communication channel to decrypt, scan, and detect the message midway. The incentive for providers to comply with the detection order, in order to avoid heavy fines, could lead to the abandonment of E2EE and, consequently, compromise the protection of fundamental rights.

Moreover, a practical concern for both server-side scanning and CSS with ML is the number of human moderators required, in addition to the detection technologies, to inspect and classify CSAM or grooming. Abelson et al. cited Facebook's use of 15,000 moderators, with critics arguing that this number should be doubled. Given this, how will the situation be managed in the future if detection becomes mandatory for more providers?

[208] *Privacy International* (n 166), paragraph 68.
[209] EDPB-EDPS Joint Opinion 04/2022 (n 51) 16.
[210] van Daalen (n 18) 11.
[211] COM (2022) 209 final, ch II, art 9(3)(4), ch III art 25; van Daalen (n 18) 12.

Lastly, several scholars argue that deploying CSS offers no significant benefits for public security. According to Ludvigsen et al., CSS is ineffective for detecting CSAM because it cannot effectively fulfil its intended purpose.[212] CSS operates similarly to antivirus software, constantly surveilling the system and attempting to detect all events within a given framework. However, like antivirus software, CSS for CSAM cannot be perfect because the definition of CSAM can never encompass all existing types. Essentially, CSAM will always exist, even with CSS in use.[213] Furthermore, circumvention is inevitable; even if CSS were perfect, adversaries could upload an image, which would be scanned and detected by the CSS as CSAM. The adversary could then delete the picture and use alternative methods to distribute CSAM, rendering the CSS redundant and unable to fulfil its purpose. Additionally, aggressive circumvention is possible, as CSS can be exploited by attackers, creating the same problem it is trying to solve. As the authors put it, "The goals of any CSS will therefore be in conflict with its capabilities at all times."[214] Furthermore, there is no foolproof way to prevent misuse and thus avoid violating the very purpose of the systems. It must be assumed that there will always be a certain risk of adversarial failures, and there is no way to mitigate every risk. Constantly scanning live activity on a system means that CSS acts more like a vulnerability than a tool to achieve its goals.[215] In summary, because CSS cannot fulfil its purpose, either due to the assumption of universal circumvention or because it cannot technically or practically achieve its goals, it will not be effective in fighting CSAM by itself.

In summary, the exposition highlights the severe impact of the detection orders for new CSAM and grooming, and the subsequent use of CSS with ML or server-side scanning, on the fundamental rights to privacy and data protection. The detection order subjects all users of a service to content scanning, infringing upon their private communications. Furthermore, the proposal lacks essential safeguards; there is no independent oversight of the detection order's implementation, and deployment conditions are unclear, potentially leading to arbitrary outcomes. Additionally, the EDPS and EDPB argue that server-side scanning is fundamentally incompatible with E2EE, a crucial technology for ensuring the privacy and confidentiality of communication. Experts also question the practicality of implementing the detection order and the efficacy of CSS in achieving its intended objectives. It is evident that the detection orders for new CSAM and grooming, and the associated technical measures,

[212] Ludvigsen, Nagaraja and Daly (n 101) 3.
[213] ibid.
[214] ibid; Abelson and others (n 95) 12-13, 26-30.
[215] Ludvigsen, Nagaraja and Daly (n 101) 4.

lack proportionality *stricto sensu*, as they impose significant limitations on privacy and data protection rights with minimal benefits for public security.

4.2 A conflict between public security and privacy?

From all the aforementioned reasons, it is clear that CSS and server-side scanning cause a conflict between public security and privacy. But the more interesting question is: how do these technical measures create a conflict?

Understanding this requires a look back in time. Until the 1970s, most encryption methods were vulnerable to being 'cracked,' meaning governments were not concerned about the general public using cryptography since they could decrypt it. However, the 1970s marked a turning point as cryptography advanced significantly, providing the public with access to 'uncrackable' encryption.[216] This development posed challenges for governments worldwide, as law enforcement found wiretaps and computer searches useless when encountering encrypted data.[217] In response, governments lobbied for the weakening of encryption. One notable example is the Clipper Chip, an encryption device equipped with a built-in master key, allowing government access to encrypted communications.[218] This mirrors the proposed server-side scanning method by the EC, where service providers act as intermediaries, decrypting, scanning, and then re-encrypting messages before transmission to recipients.[219]

To come back to the proposal, the EDPB and EDPS state that encryption contributes fundamentally to the respect for private life and confidentiality of communications and that E2EE is crucial for interpersonal communications.[220] They go on to state that even though the proposal does not establish a systematic interception obligation, the possibility of a detection order would heavily weigh on the choices providers make regarding E2EE, seeing the small timeframe they have to comply and the heavy penalties if they fail to adhere to the order.[221] Moreover, while the proposal is technology-neutral, the detection order is structural incompatible with E2EE.[222] This would lead to service providers offering less encrypted services, which would undermine the respect for the fundamental rights of privacy and data

[216] Bert-Jaap Koops and Eleni Kosta, 'Looking for Some Light through the Lens of "Cryptowar" History: Policy Options for Law Enforcement Authorities against "Going Dark"' (2018) 34 Computer Law & Security Review 890 892-893.
[217] ibid 893.
[218] Harold Abelson and others, 'Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications ‡' (2015) 1 Journal of Cybersecurity 69 70-71.
[219] SWD (2022) 209 final 301.
[220] EDPB-EDPS Joint Opinion 04/2022 (n 51) 27.
[221] COM (2022) 209 final, ch III, art 35; ibid 28.
[222] ibid 28.

protection and could even have a chilling effect on the freedom of expression.[223] Essentially, the obligation to use the technical measure of server-side scanning would create a conflict between public security and privacy at a fundamental level, as the measure would render E2EE useless by breaking the very essence of E2EE, which is that the contents can only be seen by the endpoints. In this light, one needs to look at CSS. Its proponents claim that CSS is the solution to the encryption versus public safety debate: it offers privacy because it does not impede E2EE, yet it still has the ability to investigate serious crime. However, Abelson et al. argue that this is moot, as the content still gets scanned before encryption, akin to an agent constantly going through your belongings in your house.[224] In this sense, CSS creates an even bigger conflict between public security and privacy, as it circumvents encryption completely by monitoring all content prior to encryption.

In conclusion, server-side scanning would create a conflict between privacy and public security, as it undermines the essence and usage of E2EE. Additionally, while CSS was hailed to save encryption and still be usable for fighting serious crime, by enabling CSS, the conflict would get even bigger because CSS inherently scans every bit of content on the device, undermining privacy and data protection even more than server-side scanning already did.[225]

4.3 Moving forward with the proposal

This thesis examined the EC's version of the proposed Regulation, as it was the most relevant for research purposes and was the only version available at the commencement of this study. However, during the course of this research, both the EP and the Council presented their amendments to the EC's proposed Regulation.[226] To provide a comprehensive overview, these amendments will be briefly discussed.

Starting with the EP, they proposed several amendments, with the most important ones outlined here. The most important amendment is the exclusion of E2EE messenger providers from the scope of the Regulation.[227] Additionally, they propose targeted scanning of specific persons or groups linked to CSAM, rather than deploying measures across the entire service, which could be used for grooming or disseminating CSAM.[228] Lastly, the EP also aims to reject

[223] ibid 28.
[224] Ludvigsen, Nagaraja and Daly (n 101) 2.
[225] ibid.
[226] Note: the Council still has to reach a final agreement, so the amendments are not yet definitive, see: Breyer (n 2).
[227] 'Report on the Proposal for a Regulation of the European Parliament and of the Council Laying down Rules to Prevent and Combat Child Sexual Abuse (COM (2022)0209 – C9-0174/2022 – 2022/0155(COD))' (2023) <www.europarl.europa.eu/doceo/document/LIBE-AM-746814_EN.pdf> accessed 25 May 2024 112.
[228] ibid 92.

scanning for grooming for providers included in the scope.[229] These amendments are favourable in terms of privacy and data protection, especially the exclusion of E2EE messenger services. This exclusion would significantly reduce the impact on privacy and data protection rights. Providers would not be burdened by the fear of heavy penalties for E2EE use, allowing for its effective continued use and effective protection of private communications.[230]

In comparison, the Council only introduced two notable amendments, while their version largely mirrors the EC's proposal.[231] The first amendment stipulates that using AI for the detection of new CSAM would only result in the disclosure of chats if the material is flagged twice.[232] Although Breyer is not enthusiastic, it is a step forward in acknowledging the experimental nature and unknown error rate of current detection technology, which could result in numerous false positives. The second amendment excludes searches for grooming, for similar reasons related to the unreliability of experimental technologies.[233] Although this can be seen as a slight improvement over the EC's proposal by rejecting untested technologies, it still includes E2EE providers within its scope, potentially leading to similar privacy concerns as the EC's version.[234]

Lastly, a recent ECtHR case should be highlighted in the context of this proposed Regulation's proceedings, as it could be seen as a call for the European Union to amend it.[235] Specifically, in the *Podchasov* case,[236] the ECtHR ruled that mandating the decryption of E2EE data violates Article 8 of the ECHR. According to Lakra, the ECtHR even considered decryption of E2EE data *in principle* against the right to privacy, contrasting with their procedural approach to data retention.[237] In short, the ECtHR here emphasizes the importance

[229] ibid 102.

[230] 'Why CEPIS Welcomes Amendments to EU's Rules Combatting Child Sexual Abuse' (*CEPIS*, 31 October 2023) <https://cepis.org/why-cepis-welcomes-amendments-to-eus-rules-combatting-child-sexual-abuse/> accessed 26 May 2024.

[231] 'Proposal for a Regulation of the European Parliament and of the Council Laying down Rules to Prevent and Combat Child Sexual Abuse - Partial Mandate for Negotiations with the European Parliament' (Document number 11277/24, 14 June 2024) <www.patrick-breyer.de/wp-content/uploads/2024/06/csam_cleaned.pdf> accessed 20 July 2024 (The Council Partial Mandate CSAM).

[232] ibid 61; Breyer (n 2).

[233] ibid 61; ibid.

[234] ibid.

[235] Tuchtfeld (n 48).

[236] Podchasov v. Russia, no. 33696/19, 13 February 2024; Rudraksh Lakra, 'Cracking the Code: How Podchasov v. Russia Upholds Encryption and Reshapes Surveillance' (*EJIL: Talk!*, 13 March 2024) <www.ejiltalk.org/cracking-the-code-how-podchasov-v-russia-upholds-encryption-and-reshapes-surveillance/> accessed 19 March 2024.

[237] Ibid, paragraph 80; ibid.

of E2EE, which Tuchtfeld hopes the European Union will consider since their proposal also implicitly asks for the decryption for E2EE data.[238]

In the end there is currently one proposal and two versions with amendments, however, the Council still has to take a definitive stance on their amendments. After this, trilogue negotiations can be started between the EC, the Council and the EP for the final version of the Regulation. It is up in the air what this version will look like in terms of limiting the rights to privacy and data protection.

4.4 Conclusion

In conclusion, the technical measures outlined are likely not legitimate under Article 52(1) CFR. First, their legality is questionable due to the lack of clear legislative guidance, potentially resulting in arbitrary choices by providers. Second, these measures may compromise the essence of the right to a private life and data protection, as they grant public authorities access on a generalized basis to communication data. Last, they fail to adhere to the principle of proportionality; many measures are deemed unnecessary, and those considered necessary are not adequately balanced in their impact on privacy and data protection against benefits for public security. Furthermore, this assessment underscores the enduring tension between public security and privacy and data protection, as governments seek to circumvent encryption to enhance public security. However, E2EE is fundamental for privacy, and compromising it in the name of public security does not justify the means. It is important to note that this assessment is based on the EC's proposed version, and potential changes from EP and Council amendments can bring changes to the assessment.

[238] Tuchtfeld (n 48).

V Conclusion

If two things are clear, it is that children should be protected, especially in the online environment as more and more parts of their lives happen online, and that the circulation and dissemination of CSAM should be stopped.[239] However, the million-dollar question is, "how?". The European Commission (EC) tried to answer this question with the CSAM proposal, but the answer came at a cost: limitations on the rights to privacy and data protection. This thesis examined to what extent the proposed CSAM regulation is legitimate according to Article 52(1) CFR, considering the limitations it imposes on Articles 7 and 8 CFR. In particular, this thesis focused on the various technical detection measures, as these are the backbone of the CSAM proposal and the elements that, in practice, actually cause the interference with the fundamental rights of privacy and data protection.

The detection technologies come into play after a provider receives a detection order, which can be issued after providers have fulfilled their three mandatory cumulative obligations: risk assessment, risk mitigation, and reporting the risks and mitigation measures to the CA. After these steps, the CA can request the issuance of a detection order under certain conditions. The prerequisites under which a detection order can be issued are already vague, facilitating legal uncertainty and arbitrariness. Once a detection order has been issued, providers are not bound to specific detection technologies, as long as the technology is effective. This is problematic for encrypted service providers, as they cannot scan the content of messages, which is necessary for effectiveness; this forces them *de facto* to deploy CSS or server-side scanning methods. Consequently, this is the critical point of the proposed Regulation that needs to be assessed according to Article 52(1) CFR, because both technologies impose severe limitations on the rights to privacy and data protection, and it is necessary to assess to what extent these interferences are legitimate.

First and foremost, it is debatable whether these technologies are provided for by law. The real problem lies not in the techno-neutrality embedded in the proposed Regulation, as the legislator is allowed to use sufficiently open terms to avoid diminishing the effectiveness of surveillance. However, even in the accompanying report, the EC cannot provide a definitive list of technologies that will adhere to their own requirements, instead listing them as possible solutions with numerous ifs', but's, and may's. Yet, the features of the chosen technology will significantly impact the limitations on the rights to privacy and data protection. In this light, it

[239] Paul Bleakley and others, 'Moderating Online Child Sexual Abuse Material (CSAM): Does Self-Regulation Work, or Is Greater State Regulation Needed?' (2024) 21 European Journal of Criminology 231 236.

can be argued that the proposed measures are neither foreseeable nor accessible to the legislator herself, the providers responsible for them, and especially the users subjected to these technologies. Additionally, it is likely that the proposed Regulation will compromise the essence of the rights, as it forces providers to use certain technologies that give public authorities generalized access to electronic communications by breaking or circumventing E2EE, which is fundamental to these rights. Lastly, it is highly likely that CSS and server-side scanning will not adhere to the principle of proportionality. The reason is that most of the technologies lack necessity, as the misuse of providers could be addressed through less intrusive means. Moreover, while CSS with the use of ML passed the necessity sub-test, it could not be considered proportional *stricto sensu*, since the benefits gained could not balance the limitations imposed on privacy and data protection rights. The severity of the limitations is also worsened by the lack of procedural and substantive safeguards. In conclusion, the interferences imposed on Articles 7 and 8 CFR by CSS and server-side scanning, and by extension the CSAM proposal, are likely to be illegitimate to the extent that they do not adhere to the principle of proportionality. However, it is also probable that the proposed Regulation could fail to meet the requirement provided by law or compromise the essence of the rights; however, these points are more prone to debates.

Ultimately, this thesis demonstrates the impact that the proposal has on the conflict between public security and privacy and data protection, by examining the technical aspects of the proposal, including how CSS and server-side scanning methods work and how they infringe on privacy and data protection rights in real life. Particularly, the way CSS works demonstrates the significant impact of the proposal, as it could be even more infringing than server-side scanning. In this context, the proposed Regulation's approach to circumventing or breaking encryption for security purposes, especially in combating online CSA, can be understood within a historical framework, where governments have sought ways to counter the widespread use of 'uncrackable' encryption.

Further research needs to be conducted, especially once the Regulation is finalised. As discussed in the last chapter, this thesis focused on the version of the proposal presented by the EC. It is worth noting that amendments brought forward by the EP, during the writing process of this thesis, could potentially align this proposed Regulation more closely with the CFR and mitigate its impact on the conflict. However, it is also important to acknowledge that the approach of the Council was more aligned with the version proposed by the EC. For this reason, further, more definitive research must be done once the proposed Regulation is finalized to capture the full the impact of the Regulation on the conflict between public security and privacy and data protection.

Bibliography

Primary sources

EU Legislation

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 (Text with EEA relevance), 274/41 OJ L § (2021). http://data.europa.eu/eli/reg/2021/1232/oj/eng.

Case law CJEU

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources ea and Kärntner Landesregierung ea, No. Joined Cases C-293/12 and C-594/12 (ECJ EU 8 April 2014).

La Quadrature du Net and Others v Premier ministre and Others, No. Joined Cases C-511/18, C-512/18, C-520/18 (ECJ 6 October 2020).

La Quadrature du Net ea v Premier ministre and Ministère de la Culture, No. Case C-470/21 (ECJ 30 April 2024).

Ligue des droits humains ASBL v Conseil des ministres, No. Case C-817/19 (ECJ 21 June 2022).

Maximillian Schrems v Data Protection Commissioner, No. Case C-362/14 (ECJ 6 October 2015).

Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, No. Case C-623/17 (ECJ 6 October 2020).

Proceedings brought by Ministerio Fiscal, No. Case C-207/16 (ECJ 2 oktober 2018).

Sergejs Buivids v Datu valsts inspekcija, No. Case C-345/17 (ECJ 14 February 2019).

Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson ea, No. Joined Cases C-203/15 and C-698/15 (ECJ EU 21 December 2016).

Case law ECtHR

Amann v. Switzerland, No. 27798/95 (ECtHR [GC] 16 February 2000).

Big Brother Watch and Others v. the United Kingdom, No. 58170/13, 62322/14, 24960/15 (ECtHR [GC] 25 May 2021).

Breyer v. Germany, No. 50001/12 (ECtHR 30 January 2020).

Centrum För Rättvisa v. Sweden, No. 35252/08 (ECtHR [GC] 25 May 2021).

Klass and Others v. Germany, No. 38581/16, 41914/16, 57510/16, 62644/16, 7190/17,10973/17, 12530/17, 19411/17, 22087/17, 28475/17, 78165/17 (ECtHR 6 September 1978).

Liberty and Others v. the United Kingdom, No. 58243/00 (ECtHR 1 July 2008).

Niemietz v. Germany, No. 57546/13, 57855/13, 57861/13, 57887/13, 59929/13, 59937/13, 64092/13 (ECtHR 16 December 1992).

Peck v. the United Kingdom, No. 60898/00 (ECtHR 28 January 2003).

Podchasov v. Russia, No. 33696/19 (ECtHR 13 February 2024).

Pretty v. the United Kingdom, No. 81519/12, 40547/15, 51218/15, 61276/15, 12995/16, 19138/16, 52032/16, 55072/16, 24510/17, 26747/17, 60448/17, 22122/19, 44686/19 (ECtHR 29 April 2002).

Szabó and Vissy v. Hungary, No. 37138/14 (ECtHR 12 January 2016).

The Sunday Times v. the United Kingdom (no. 1), No. 6538/74 (ECtHR 26 April 1979).

Roman Zakharov v. Russia, No. 47143/06 (ECtHR [GC] 4 December 2015).

Secondary sources

Books

Barak A, *Proportionality: Constitutional Rights and Their Limitations* (Cambridge University Press 2012).

Council of Europe and others, *Handbook on European Data Protection Law – 2018 Edition* (Publications Office of the European Union 2018).

Dijck G, Snel M, Golen T, *Methoden van Rechtswetenschappelijk Onderzoek* (Boom Juridisch 2018).

European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU: Volume II: Field Perspectives and Legal Update* (Publications Office of the European Union 2017).

Fura E and Klamberg M, 'The Chilling Effect of Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA' in Josep Casadevall, Egbert Myjer and Michael O'Boyle (eds), *Freedom of expression: essays in honour of Nicolas Bratza* (Wolf Legal Publishers 2012).

Kosta E, *Surveilling Masses and Unveiling Human Rights - Uneasy Choices for the Strasbourg Court* (PrismaPrint 2017).

Kranenborg H, 'Recht op bescherming van persoonsgegevens' in Gerrit-Jan Zwenne and Herke Kranenborg (eds), Tekst & Commentaar Privacy- en gegevensbeschermingsrecht (8th edition Wolters Kluwer 2022).

——, 'Recht op eerbiediging van privé-, familie- en gezinsleven' in Gerrit-Jan Zwenne and Herke Kranenborg (eds), *Tekst & Commentaar Privacy- en gegevensbeschermingsrecht* (8th edition Wolters Kluwer 2022).

——, 'Recht op eerbiediging van het privéleven, het familie- en gezinsleven, de woning en de communicatie' in Gerrit-Jan Zwenne and Herke Kranenborg (eds), Tekst & Commentaar Privacy- en gegevensbeschermingsrecht (8th edition Wolters Kluwer 2022).

Lock T, 'Article 8 CFR' in Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (Oxford University Press 2019).

Nardell G, 'Levelling up: Data Privacy and the European Court of Human Rights' in Serge Gutwirth, Yves Poullet and Paul De Hert (eds), *Data Protection in a Profiled World* (Springer Netherlands 2010).

Nielson SJ, *Discovering Cybersecurity: A Technical Introduction for the Absolute Beginner* (Apress Berkeley 2023).

Oerlemans JJ, Galič M, 'Cybercrime investigations' in Wytske van der Wagen, Jan-Jaap Oerlemans and Marleen Weulen Kranenbarg (eds), *Essentials in Cybercrime: A Criminological Overview for Education and Practice* (Eleven International Publishing 2021).

Sunyaev A, *Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies* (Springer International Publishing 2020).

——, *Surveillance by Intelligence Services: Fundamental rights safeguards and remedies in the EU – 2023 update* (Publications Office of the European Union 2023).

Watt E, *State Sponsored Cyber Surveillance* (Edward Elgar Publishing Limited 2021)

Articles and working papers

Abelson H, and others, 'Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications ‡' (2015) 1 Journal of Cybersecurity 69.

——, and others, 'Bugs in Our Pockets: The Risks of Client-Side Scanning' (2024) 10 Journal of Cybersecurity < https://doi.org/10.1093/cybsec/tyad020> accessed 24 February 2024.

Bauman Z, and others, 'After Snowden: Rethinking the Impact of Surveillance' (2014) 8 International Political Sociology 121.

Bleakley P, and others, 'Moderating Online Child Sexual Abuse Material (CSAM): Does Self-Regulation Work, or Is Greater State Regulation Needed?' (2024) 21 European Journal of Criminology 231.

Brems E, and Lavrysen L, '"Don't Use a Sledgehammer to Crack a Nut": Less Restrictive Means in the Case Law of the European Court of Human Rights' (2015) 15 Human Rights Law Review 139.

Brkan M, 'The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning' (2019) 20 German Law Journal 864.

Buono I and Taylor A, 'Mass Surveillance in the Cjeu: Forging a European Consensus'. The Cambridge Law Journal 76, no. 2 (2017): 250–53.

Commission, 'Commission staff working document impact assessment report accompanying the document Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse' SWD (2022) 209 final.

Council of Europe and European Court of Human Rights, 'Guide on Article 8 of the European Convention on Human Rights: Right to Respect for Private and Family Life, Home and Correspondence' (2017).

Daalen O, ‘The right to encryption: Privacy as preventing unlawful access’. Computer Law & Security Review 49 (1 July 2023): 105804. https://doi.org/10.1016/j.clsr.2023.105804.

Dalla Corte L, ‘On Proportionality in the Data Protection Jurisprudence of the CJEU’ (2022) 12 International Data Privacy Law 259.

Drooghenbroeck S and Rizcallah C, ‘The ECHR and the Essence of Fundamental Rights: Searching for Sugar in Hot Milk?’ (2019) 20 German Law Journal 904.

Eskens S, ‘The Ever-Growing Complexity of the Data Retention Discussion in the EU: An In-Depth Review of La Quadrature Du Net and Others and Privacy International’ (2022) 8 European Data Protection Law Review 143.

——, Explanations relating to the Charter of Fundamental Rights [2007] OJ C303/02 17.

Farid H, ‘An Overview of Perceptual Hashing’ (2021) 1 Journal of Online Trust and Safety <https://tsjournal.org/index.php/jots/article/view/24> accessed 24 May.

Georgieva I, ‘The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Article 17 ICCPR and Article 8 ECHR’ (2015) 31 Utrecht Journal of International and European Law 104.

Granger MP, and Irion K, ‘The Court of Justice and The Data Retention Directive in Digital Rights Ireland: Telling Off The EU Legislator and Teaching a Lesson in Privacy and Data Protection’ (2014) 39 European Law Review 834.

Khateeb HM, and Epiphaniou G, ‘How Technology Can Mitigate and Counteract Cyber-Stalking and Online Grooming’ (2016) 2016 Computer Fraud & Security 14.

Koops BJ, Kosta E, ‘Looking for Some Light through the Lens of “Cryptowar” History: Policy Options for Law Enforcement Authorities against “Going Dark”’ (2018) 34 Computer Law & Security Review 890.

Kouvakas I, ‘The Watson Case: Another Missed Opportunity for Stricto Sensu Proportionality’ (2017) 2 Cambridge Law Review 173.

Lee HE, and others, ‘Detecting Child Sexual Abuse Material: A Comprehensive Survey’ (2020) 34 Forensic Science International: Digital Investigation 301022.

Lenaerts K, ‘Limits on Limitations: The Essence of Fundamental Rights in the EU’ (2019) 20 German Law Journal 779.

Ludvigsen KR, Nagaraja S, and Daly A, ‘YASM (Yet Another Surveillance Mechanism)’ (2022) arXiv, <http://arxiv.org/abs/2205.14601> accessed 5 April 2024.

Lynskey O, ‘Control over Personal Data in a Digital Age: Google Spain v AEPD and Mano Costeja Gonzalez’ (2015) 78 The Modern Law Review 522 529.

——, ‘The Data Retention Directive Is Incompatible with the Rights to Privacy and Data Protection and Is Invalid in Its Entirety: Digital Rights Ireland’ (2014) 51 Common Market Law Review 1789.

Maras MH, ‘The Social Consequences of a Mass Surveillance Measure: What Happens When We Become the “Others”?’ (2012) 40 International Journal of Law, Crime and Justice 65.

Mitsilegas V and others, ‘Data Retention and the Future of Large-Scale Surveillance: The Evolution and Contestation of Judicial Benchmarks’ (2023) 29 European Law Journal 176.

Pfefferkorn R, ‘Content-Oblivious Trust and Safety Techniques: Results from a Survey of Online Service Providers’ (2022) 1 Journal of Online Trust and Safety <https://tsjournal.org/index.php/jots/article/view/14> accessed 24 July 2024.

Vogiatzoglou P, ‘Mass Surveillance, Predictive Policing and the Implementation of the CJEU and ECtHR Requirement of Objectivity’ (2019) 10 European Journal of Law and Technology <https://www.ejlt.org/index.php/ejlt/article/view/669> accessed 16 March 2024.

Papers and reports

Colneric N, Legal Opinion Commissioned by MEP Patrick Breyer, The Greens/EFA Group in the European Parliament’ (Hamburg, March 2021) <www.patrick-breyer.de/wp-content/uploads/2021/03/Legal-Opinion-Screening-for-child-pornography-2021-03-04.pdf> accessed 28 October 2023.

Daalen O, ‘Fundamental Rights Assessment of the Framework for Detection Orders under the CSAM Proposal’ (IViR, 22 April 2023) <www.ivir.nl/publicaties/download/CSAMreport.pdf> accessed 26 November 2023.

——, ‘EDPB-EDPS Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Rules to Prevent and Combat Child Sexual Abuse’ (Adopted on 28 July 2022) <https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042022-proposal_en> accessed 4 November 2023

——, ‘Explanations relating to the Charter of Fundamental Rights (2007). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32007X1214%2801%29.

Gross O, ‘Misguided response’ [2002/2003] 27/6 Boston Review http://www.bostonreview.net/BR27.6/gross.html accessed 27 October 2023.

——, Report on the Proposal for a Regulation of the European Parliament and of the Council Laying down Rules to Prevent and Combat Child Sexual Abuse (COM(2022)0209 – C9-0174/2022 – 2022/0155(COD))’ (2023) <www.europarl.europa.eu/doceo/document/LIBE-AM-746814_EN.pdf> accessed 25 May 2024.

Review Committee for the Intelligence and Security Services, ’Annual Report 2013-2014’ (31 March 2014) < https://english.ctivd.nl/documents/annual-reports/2013/03/31/index>.

Proposal of Regulations by European Commission

Proposal for a regulation of the European Parliament and the Council laying down rules to prevent and combat child sexual abuse (n.d.). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2022:209:FIN.

Online sources

Article 29 Data Protection Working Party, ‘Statement on the Ruling of the Court of Justice of the European Union (CJEU) Which Invalidates the Data Retention Directive 14/EN WP 220’ <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp220_en.pdf> accessed 20 May 2024.

Bernard T, ‘The Landscape of CSAM Detection: Challenges and Innovations’ <www.unitary.ai//articles/the-present-and-future-of-detecting-child-sexual-abuse-material-on-social-media> accessed 25 May 2024.

Bosl T, ‘Not You Again!: Mass Surveillance Before the CJEU and Why “Hadopi” Could Be a Game-Changer for the Right to Privacy’ [2023] Völkerrechtsblog <https://voelkerrechtsblog.org/not-you-again/> accessed 24 July 2024.

Brewster T, ‘FBI Wiretap Opens Window To Murderous Drug Gang—And A Crucial Flaw In Snapchat Privacy’ (*Forbes, 23 May 2022*) <www.forbes.com/sites/thomasbrewster/2022/05/23/fbi-snapchat-surveillance-exposes-a-murderous-mexican-gang-and-snaps-weakness/> accessed 24 February 2024.

Breyer P, ‘Chat Control: The EU’s CSEM Scanner Proposal’ (*Patrick Breyer*) <https://www.patrick-breyer.de/en/posts/chat-control/> accessed 28 October 2023.

——, ‘Child Sexual Abuse Online: Current Rules Extended until April 2026 | News | European Parliament’ (10 April 2024) <www.europarl.europa.eu/news/en/press-

room/20240408IPR20311/child-sexual-abuse-online-current-rules-extended-until-april-2026> accessed 18 June 2024.

Council of Europe, ‘Mass Surveillance’ (July 2018) <https://rm.coe.int/factsheet-on-mass-surveillance-july2018-docx/16808c168e > accessed 27 October 2023.

Diafi A, ‘Deep Diving into End-to-End Encryption (E2EE) 🔐 ’ (Medium, 24 October 2022) <https://amirdiafi.medium.com/deep-diving-into-end-to-end-encryption-e2ee-2b05d3dca2ed> accessed 22 July 2024.

EDPS, ‘Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit’ (17 April 2017) <www.edps.europa.eu/sites/default/files/publication/17-0601_necessity_toolkit_final_en.pdf> accessed 20 July 2024.

EDRi, ‘European Commission Must Uphold Privacy, Security and Free Expression by Withdrawing New Law, Say Civil Society’. European Digital Rights (EDRi, 8 June 2022) <https://edri.org/our-work/european-commission-must-uphold-privacy-security-and-free-expression-by-withdrawing-new-law/> Accessed 28 October 2023.

——, ‘Is Surveilling Children Really Protecting Them? Our Concerns on the Interim CSAM Regulation’ (*European Digital Rights (EDRi)*) <https://edri.org/our-work/is-surveilling-children-really-protecting-them-our-concerns-on-the-interim-csam-regulation/> accessed 25 May 2024.

——, ‘Encryption and Lawful Access: Evaluating Benefits and Risks to Public Safety and Privacy | United States Senate Committee on the Judiciary’ <https://www.judiciary.senate.gov/committee-activity/hearings/encryption-and-lawful-access-evaluating-benefits-and-risks-to-public-safety-and-privacy> accessed 25 May 2024.

——, ‘End-to-End Versleutelde Chats | Instagram-Helpcentrum’ <https://help.instagram.com/3490194014566528> accessed 24 February 2024

eSafety Commissioner, ‘Basic Online Safety Expectations’ (December 2022) <www.esafety.gov.au/sites/default/files/2022-12/BOSE%20transparency%20report%20Dec%202022.pdf> accessed 24 February 2024.

——, ‘Explaining the Technology for Detecting Child Sexual Abuse Online’ (CRIN, 10 November 2023) <https://home.crin.org/readlistenwatch/stories/explainer-detection-technologies-child-sexual-abuse-online> accessed 25 May 2024.

——, ‘Fact Sheet: Client-Side Scanning’ (*Internet Society, 2 September 2022*) <www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/> accessed 24 February 2024.

Fotiadis A, Stavinoha L, and Zandonini G, ‘Europol Sought Unlimited Data Access in Online Child Sexual Abuse Regulation’ (*Balkan Insight*, 29 September 2023) <https://balkaninsight.com/2023/09/29/europol-sought-unlimited-data-access-in-online-child-sexual-abuse-regulation/> accessed 21 May 2024.

——, ‘Interinstitutional Negotiations | Ordinary Legislative Procedure | European Parliament’ (*olp*) <www.europarl.europa.eu/olp/en/interinstitutional-negotiations> accessed 27 May 2024.

——, ‘Joined Cases Tele2 Sverige AB v Post- Och Telestyrelsen and Secretary of State for the Home Department v. Watson’ (*Global Freedom of Expression*) <https://globalfreedomofexpression.columbia.edu/cases/joined-cases-tele2-sverige-ab-v-post-och-telestyrelsen-c-20315-secretary-state-home-department-v-watson/> accessed 20 May 2024.

Lakra R, ‘Cracking the Code: How Podchasov v. Russia Upholds Encryption and Reshapes Surveillance’ (EJIL: Talk!, 13 March 2024) <www.ejiltalk.org/cracking-the-code-how-podchasov-v-russia-upholds-encryption-and-reshapes-surveillance/> accessed 19 March 2024.

La Quadrature du Net, ‘Surveillance and Hadopi: EU Court Buries Online Anonymity a Little Further’, 30 April 2024. https://www.laquadrature.net/en/2024/04/30/surveillance-and-hadopi-eu-court-buries-online-anonymity-a-little-further/.

——, ‘Leaked EU Council Legal Analysis: EU Chat Control Plans for Indiscriminately Searching Private Messages Doomed to Failure’ (*Patrick Breyer*, 8 May 2023) <www.patrick-breyer.de/en/leaked-eu-council-legal-analysis-eu-chat-control-plans-for-indiscriminately-searching-private-messages-doomed-to-failure/> accessed 28 October 2023

Legal Service of the Council of the European Union, ‘Opinion of the Legal Service 8787/23’ (Brussels, 26 April 2023) <https://aeur.eu/f/6ql> accessed 28 October 2023

Lomas N, ‘Europe’s CSAM-Scanning Plan Is a Tipping Point for Democratic Rights, Experts Warn’ (*TechCrunch*, 24 October 2023) <https://techcrunch.com/2023/10/24/eu-csam-scanning-edps-seminar/> accessed 21 May 2024.

Lutkevich B, Bacon M, ‘What Is End-to-End Encryption (E2EE) and How Does It Work?’ (*Security*) <www.techtarget.com/searchsecurity/definition/end-to-end-encryption-E2EE> accessed 22 July 2024.

Mauer M, ‘The Unbearable Lightness of Interfering with the Right to Privacy’ [2024] Verfassungsblog <https://verfassungsblog.de/the-unbearable-lightness-of-interfering-with-the-right-to-privacy/> accessed 24 July 2024.

——, ‘Messaging App Security: Which Are the Best Apps for Privacy?’ (Kaspersky, 20 November 2023) <www.kaspersky.com/resource-center/preemptive-safety/messaging-app-security> accessed 24 February 2024.

Moore J and Wigmore Y, ‘What Is Hosted Services? | Definition from TechTarget’ (*IT Channel*, 1 October 2018) <www.techtarget.com/searchitchannel/definition/hosted-services> accessed 20 June 2024.

Milanovic M, ‘The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum För Rättvisa’ (*EJIL: Talk!*, 26 May 2021) <www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/> accessed 17 July 2024.

Oostveen M, ‘Why Privacy ≠ Data Protection (and How They Overlap) – Digital Society Blog’ (*HIIG*, 4 May 2016) <www.hiig.de/en/why-privacy-≠-data-protection-and-how-they-overlap/> accessed 19 April 2024.

Optalysys, ‘FHE: An Alternative to Client-Side Scanning?’ (*Optalysys*, 31 July 2023) <https://medium.com/optalysys/fhe-an-alternative-to-client-side-scanning-e58491b1c00> accessed 23 May 2024.

——, ‘Ordinary Legislative Procedure’ (European Parliament) <www.europarl.europa.eu/infographic/legislative-procedure/index_en.html> accessed 19 May 2024.

——,‘Personal Communications Service’ (*Wikipedia*, 2023) <https://en.wikipedia.org/w/index.php?title=Personal_Communications_Service&oldid=1174819071> accessed 26 November 2023.

——, ‘Proposal for a Regulation of the European Parliament and of the Council Laying down Rules to Prevent and Combat Child Sexual Abuse - Partial Mandate for Negotiations with the

European Parliament' (Document number 11277/24, 14 June 2024) <www.patrick-breyer.de/wp-content/uploads/2024/06/csam_cleaned.pdf> accessed 20 July 2024.

Ragnarsson S, 'AI Content Moderation: Use, Types, & Integration With Hash Matching' (*Videntifier New Site*, 13 December 2023) <www.videntifier.com/post/ai-content-moderation> accessed 23 May 2024.

——, 'Regulation to Prevent and Combat Child Sexual Abuse'. In Wikipedia, 18 October 2023. https://en.wikipedia.org/w/index.php?title=Regulation_to_Prevent_and_Combat_Child_Sexual_Abuse&oldid=1180761196#cite_note-3.

Rosenzweig P. 'The Law and Policy of Client-Side Scanning' (Default) <www.lawfaremedia.org/article/law-and-policy-client-side-scanning> accessed 2 May 2024.

Silveira A, and Cabral TS, 'Again: On the Prohibition of Generalised and Indiscriminate Retention of Metadata for the Purpose of Combating Serious Crime' (*Official Blog of UNIO*, 6 October 2022) <https://officialblogofunio.com/2022/10/06/again-on-the-prohibition-of-generalised-and-indiscriminate-retention-of-metadata-for-the-purpose-of-combating-serious-crime/> accessed 28 April 2024.

Sköld H, 'Kritiserade EU-Förslaget: Så Kan Dina Vanliga Familjefoton Stämplas Som Pedofili' SVT Nyheter (8 April 2023) <www.svt.se/nyheter/utrikes/eu-forslaget-chat-control-kritiseras> accessed 25 July 2024.

——, 'Surveillance and Hadopi: EU Court Buries Online Anonymity a Little Further' (La Quadrature du Net, 30 April 2024) <www.laquadrature.net/en/2024/04/30/surveillance-and-hadopi-eu-court-buries-online-anonymity-a-little-further/> accessed 19 May 2024.

Tomova V, 'Guise of "Children's Rights" Weakens Internet Privacy Laws and Increases Mass Surveillance | TechPolicy.Press' (*Tech Policy Press*, 13 December 2023) <https://techpolicy.press/guise-of-childrens-rights-weakens-internet-privacy-laws-and-increases-mass-surveillance> accessed 21 May 2024.

Tuchtfeld E, 'No Backdoor for Mass Surveillance' [2024] Verfassungsblog <https://verfassungsblog.de/no-backdoor-for-mass-surveillance/> accessed 17 July 2024.

Watt E, 'Much Ado About Mass Surveillance - the ECtHR Grand Chamber "Opens the Gates of an Electronic 'Big Brother' in Europe" in Big Brother Watch v UK' (*Strasbourg Observers*, 28 June 2021) <https://strasbourgobservers.com/2021/06/28/much-ado-about-mass-

surveillance-the-ecthr-grand-chamber-opens-the-gates-of-an-electronic-big-brother-in-europe-in-big-brother-watch-v-uk/> accessed 17 July 2024.

——, 'The Legacy of the Privacy versus Security Narrative in the ECtHR's Jurisprudence' [2022] Verfassungsblog <https://verfassungsblog.de/os6-privacy-vs-security/> accessed 15 July 2024.

——, 'Webhosting' (Wikipedia, 2023) <https://nl.wikipedia.org/w/index.php?title=Webhosting&oldid=66323253> accessed 26 November 2023

——, 'Why CEPIS Welcomes Amendments to EU's Rules Combatting Child Sexual Abuse' (*CEPIS*, 31 October 2023) <https://cepis.org/why-cepis-welcomes-amendments-to-eus-rules-combatting-child-sexual-abuse/> accessed 26 May 2024.

Woods L, 'EU Law Analysis: Data Retention and National Law: The ECJ Ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber)' (*EU Law Analysis*, 21 December 2016) <https://eulawanalysis.blogspot.com/2016/12/data-retention-and-national-law-ecj.html> accessed 20 April 2024.

Zalnieriute M, 'Procedural Fetishism and Mass Surveillance under the ECHR' [2021] Verfassungsblog <https://verfassungsblog.de/big-b-v-uk/> accessed 12 July 2024.