Council of the European Union
General Secretariat

Interinstitutional files:
2022/0155 (COD)

Brussels, 23 May 2023

WK 6707/2023 INIT

LIMITE

JAI	**FREMP**
ENFOPOL	**TELECOM**
CRIMORG	**COMPET**
IXIM	**MI**
DATAPROTECT	**CONSOM**
CYBER	**DIGIT**
COPEN	**CODEC**

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

INFORMATION

From:	General Secretariat of the Council
To:	Law Enforcement Working Party (Police)
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse - European Parliamentary Research Service – complementary impact assessment

Delegations will find attached the complementary impact assessment published by the European Parliamentary Research Service.

European Parliament

Proposal for a regulation laying down the rules to prevent and combat child sexual abuse

Complementary impact assessment

STUDY

EPRS | European Parliamentary Research Service

Ex-Ante Impact Assessment Unit
PE 740.248 – April 2023

EN

Proposal for a regulation laying down rules to prevent and combat child sexual abuse

Complementary impact assessment

On 11 May 2022, the European Commission presented a proposal for a regulation laying down rules to prevent and combat child sexual abuse, with an accompanying impact assessment. The European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) requested the present complementary impact assessment of the proposal.

Without disputing the need to protect children against child sexual abuse, this study focuses on specific aspects of the proposal. It reviews the problem definition in the Commission's impact assessment, it assesses the impact of the proposal on the internet and on fundamental rights, it considers whether the prohibition of the general monitoring obligations is respected, and it assesses the necessity and proportionality of the proposed measures. It also reviews the European Commission's cost-benefit analysis underpinning the proposed creation of an EU centre to prevent and counter child sexual abuse.

This complementary impact assessment finds:

(1) a number of weaknesses in the European Commission's problem definition; notably it only discusses the challenges posed by end-to-end encryption in the fight against child sexual abuse material online to a limited extent;

(2) that, despite the potential for their abuse, technologies to detect known sexual abuse material are accurate, whereas technologies to detect new child sexual abuse material and grooming are of substantially lower accuracy and that detection of material in end-to-end-encrypted communication poses risks and vulnerabilities for individuals and society;

(3) that obligations stemming from the proposal for information society services to detect, report and remove from their services known content, new content and grooming would have positive impacts on the protection of children, but at the same time would violate some fundamental rights of users, the prohibition of generalised data retention and general monitoring obligations;

(4) that the new binding obligations stemming from detection orders for providers of information society services to detect, report, and remove new child sexual abuse material and grooming from their services would likely fail the proportionality test;

(5) that for the creation of an EU centre to prevent and counter child sexual abuse, the most cost-efficient option would be an EU centre with some functions hosted by Europol and others in an independent organisation under Member State law.

EPRS | European Parliamentary Research Service

AUTHORS

This study has been written by Gabriëlle op 't Hoog, Linette de Swart, Dr Jan Essink, Guus van der Born, Yannick Ritmeester, Dr Anna Sekuła, Geert Smit of Ecorys, Dr Niovi Vavoula and Andreas Karapatakis of Queen Mary University London, Professor Jeanne Mifsud-Bonnici of Rijksuniversiteit Groningen, Professor Bart Preneel of KU Leuven and quality reviewed by Professor Valsamis Mitsilegas of University of Liverpool at the request of the Ex-ante Impact Assessment Unit of the Directorate for Impact Assessment and European Added Value, within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament.

ADMINISTRATOR RESPONSIBLE

Dr Katharina Eisele and Hubert Dalli, Ex-Ante Impact Assessment Unit, EPRS

In addition to internal revision, the study was subject to a double-blind external peer review organised by the Ex-Ante Impact Assessment Unit.

To contact the publisher, please e-mail EPRS-ExAnteImpactAssessment@ep.europa.eu

LINGUISTIC VERSIONS

Original: EN

Manuscript completed in April 2023.

DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

Brussels © European Union, 2023.

PE 740.248
ISBN: 978-92-848-0446-7
DOI: 10.2861/016876
CAT: QA-07-23-178-EN-N

eprs@ep.europa.eu
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)

Executive summary

On 11 May 2022, the European Commission presented a proposal for a regulation laying down rules to prevent and combat child sexual abuse (CSA proposal).[1] The proposal aims at replacing the Interim Regulation,[2] which provides a temporary legal basis enabling number-independent interpersonal communication services to continue their voluntary practices to detect, report and remove child sexual abuse material (CSAM) online. The Interim Regulation will remain in force until 3 August 2024 (or until an earlier date if the present proposal for a regulation is adopted by the EU legislator and repeals this temporary measure). With the present CSA proposal, the European Commission seeks to establish a longer-term legal framework. The general objective of the CSA proposal is to improve the functioning of the internal market by introducing clear, uniform, and balanced EU rules to prevent and combat child sexual abuse (CSA), notably through imposing detection, reporting, and removal obligations on certain relevant information society services (i.e., providers of interpersonal communication services and providers of hosting services). The proposal targets both traffic and location data,[3] as well as interpersonal communication content.[4] The European Commission prepared an impact assessment (IA), which accompanies the CSA proposal (CSA proposal IA).[5]

This study, requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), presents the findings of the complementary CSA proposal IA. The study answers the following research questions:

1. Are all dimensions and aspects of the problem covered and analysed adequately? How effective and efficient is the CSA proposal in addressing the problem?
2. What is the likely impact of the CSA proposal on the internet?
3. What is the likely impact of the CSA proposal on fundamental rights?
4. Are the measures envisaged in the CSA proposal necessary and proportionate, in particular regarding the new binding obligations for relevant service providers to detect, report, and remove from their services known and new child sexual abuse material or text-based threats such as grooming, having regard for Court of Justice of the EU (CJEU) case law and notably the judgment of 6 October 2020 in *La Quadrature du Net and Others* v *Premier ministre and Others*?
5. How would the detection of new CSAM or grooming respect the prohibition of general monitoring obligations? Are the new obligations and requirements envisaged in the CSA proposal sufficiently precise to avoid violating the prohibition of general monitoring obligations?
6. What would be the preferred option among the three retained options for the creation of an EU centre to prevent and counter child sexual abuse?

---

1 Proposal for a regulation laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, European Commission, May 2022.

2 Regulation (EU) 2021/1232 of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC.

3 Data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing (traffic) and data processed in an electronic communications network or by a service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service (location).

4 Information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service.

5 Impact Assessment Report accompanying the proposal for a regulation laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, European Commission, May 2022.

The need to protect children against CSA is undisputed, and this study does not question this principle. At the core of this study lies the achievement of a balance between protecting children and safeguarding the fundamental rights of users of covered online services under the EU Charter of Fundamental Rights (CFR). The study was conducted between December 2022 and March 2023 and is based on desk research, a literature review, case law analysis and interviews. The European Commission's Better Regulation Guidelines guided the study, in particular in regard to the fundamental rights test[6] and the cost-benefit analysis.[7]

The text box below summarises the answers to the research questions and, thereby assesses the effectiveness and efficiency of the CSA proposal (i.e., part of research question 1). These findings are further detailed in the text following the textbox.

[6] Better regulation toolbox, European Commission, p. 243-244.

[7] Ibid., p. 554-557.

Overall summarising conclusions

Effectiveness

This study concludes that the overall effectiveness of the CSA proposal is expected to be limited. This is due to a variety of factors that, when taken together, make it difficult to conclude that the CSA proposal will be effective. The main factors include:

(1) Weaknesses in the argumentation (problem definition) underpinning the CSA proposal;

(2) The fact that the proposal targets known content, new content, and grooming, while the technologies to detect new content and grooming are of low accuracy (compared to the technologies to detect known CSAM). A majority of experts consulted consider that deploying the technologies to detect new CSAM and grooming will result in an increase in reported content and a reduction in accuracy, thereby substantially impacting law enforcement agencies' (LEAs) workload. The feasibility of the role of an EU centre in filtering reported content specifically to alleviate the burden on LEAs is questioned;

(3) The fact that perpetrators that are keen to continue their activities and will likely resort to the dark and deep web where identification is more complicated to avoid being targeted by the measures introduced by the CSA proposal.

(4) The detection of CSAM in end-to-end encryption (E2EE) raises fundamental issues with regards to the secure nature of E2EE, as it creates vulnerabilities for users of E2EE communication channels;

(5) Weighing all the fundamental rights affected by the inclusion of the measures in the CSA proposal, it can be concluded that the CSA proposal would interfere with Articles 7 and 8 of the Charter of Fundamental Rights of the EU. This interference, by violating the prohibition on general data retention and the prohibition against general monitoring obligations, cannot be justified. While it would generally benefit the protection of children (i.e., enable the rapid identification and take-down of material, the reduction of risks of re-victimisation and better protection against grooming), the proposal would interfere with the fundamental rights of users of the services;

(6) Finally, the establishment of an EU centre would positively impact the combat against CSAM.

Efficiency

Given the expected limited effectiveness of the CSA proposal, it is difficult to draw solid conclusions with regards to its efficiency. Moreover, there is little insight on the ultimate results of the proposed legislation. Based on the material available, it can be concluded that the CSA proposal would result in efficiency gains in the fight against CSA.

In particular, a reduced reliance on United States databases and services for the detection of CSAM would benefit efficiency. In addition, this study concludes that the establishment of an EU centre as part of Europol (rather than as a decentralised agency as per the preferred option in the CSA proposal IA), would also allow for improved coordination and collaboration, and although such benefits could also be observed for an EU centre in other shapes (i.e. as a self-standing agency or as part of the EU Agency for Fundamental Rights (FRA)), this set-up is expected to become operational faster, meaning efficiency gains could be observed sooner.

Problem definition

Based on the European Commission's Better Regulation Guidelines, this study assesses the comprehensiveness and soundness of the problem definition in the CSA proposal IA. The problem definition serves as the foundation, based on which the CSA proposal has been developed by the European Commission. Following the Better Regulation Guidelines, this study identifies several weaknesses in the argumentation underlying the problem definition: the European Commission argues that fragmented legal frameworks across Member States negatively impact cooperation between public authorities and providers of information society services. However, the soundness of this logic may be questioned, as having national legal frameworks in place might actually improve cooperation between public authorities and providers of information society services on the national level, rather than hamper it. In addition, it is argued that the fragmentation of legal frameworks across Member States negatively impacts the internal market. The evidence to support this claim is found to be rather weak. Moreover, it can be questioned whether the fragmentation of legal frameworks across Member States can be considered as the driver that calls for the introduction of an EU-wide approach, or whether the actual problem driver is CSA.

The study also finds that the completeness of the problem assessment requires further strengthening. While end-to-end encrypted (E2EE) communication substantially impacts the detection of CSAM, the problem definition only addresses this element briefly. It does not mention this challenge in the problem tree and no measure is designed to address this challenge directly.

Impact of the CSA proposal on the internet

The impact of the CSA proposal on the internet can be broken down into three types of impact, namely (1) the impact on technology, (2) the impact on the quantity and quality of detection and (3) the impact on the behaviour of providers of information society services, children, and users of online services. As the CSA proposal lays down that providers of information society services should detect known content, new content and grooming, this distinction will be referred to below, where relevant.

First, in regard to the impact of the CSA proposal on technology, the study finds that only the detection of known CSAM **on open communication channels** can, at this point in time, be done with relatively high accuracy levels. The detection of known content on open communication channels can be deemed feasible and realistic, although the risk of images being altered to avoid detection remains. The accuracy levels of technologies to detect new content is gradually improving, but they remain substantially lower than those detecting known content. This study finds that, at this point in time, deploying the currently available technologies to detect new content on a large scale would result in high error rates and a very large number of false positives. As for the detection of grooming, the current accuracy levels of these technologies means that they cannot be deployed on a large scale without causing high error rates. The detection would, moreover, require language, cultural and context sensitive technologies to, for instance, assess messages in languages other than English and across various cultural contexts. These are currently not sufficiently developed.

Detecting known CSAM, new CSAM and grooming **in E2EE** communications presents substantial challenges. The study concludes that the currently available solutions are not sufficiently transparent. The complexity and lack of transparency of the technologies does not allow for independent evaluation by external experts and, therefore, quality control. Moreover, the detection of CSAM on E2EE interpersonal communications is disputed because it would impact a user's private life, with increased vulnerability to attack and abuse.

Second, the views on the expected impact of the CSA proposal on the quantity of reported content vary. The majority of experts consulted expect a steep increase in reported content, as the CSA

proposal obliges providers of information society services to detect and report known content, as well as new content and grooming. This prediction is fuelled by the expectation that some providers of information society services might resort to over-reporting to avoid liability claims. However, an increase in the quantity of reported content may not necessarily result in an equivalent increase in investigation and prosecution, and, thus, better protection of children. Furthermore, the feasibility of the role envisaged for an EU centre in filtering the expected vast amount of (false positive) reports before they are shared with LEAs is questioned.

The quality of detection is expected to deteriorate, due to the compulsory detection of new content and grooming. Technologies to detect new content and grooming have low accuracy levels, in comparison with the accuracy levels of technologies to detect known CSAM (with technologies to detect grooming being less accurate than those to detect new content). Application of these technologies would result in high error rates.

As long as law enforcement capacity remains limited, the increased error rates in conjunction with the rise in detected content are expected to negatively impact the ability of law enforcement authorities to investigate CSAM. Considerable effort would be required to sift through the large sets of data to verify which content is worthwhile investigating further. While an EU centre to prevent and combat CSA is envisaged to act as a central hub for hashes (the values returned by a hash function, used to map data – a type of digital fingerprinting) and would help standardise approaches, it is unlikely that the proposed EU centre would substantially improve the quality of detection, considering that decades of research and development have, to date, not resulted in high accuracy levels for detecting new CSAM and grooming.

Finally, behavioural impacts are expected for providers of information society services, child and adult users of online communication services. The workload of providers of information society services is generally expected to increase substantially due to the obligations that the CSA proposal introduces. The ambition to innovate in detection and E2EE is expected to be impacted in two ways. On the one hand, the innovation of technologies that can accurately detect CSAM in E2EE communications could be stimulated, because the CSA proposal illustrates a need for such technologies. On the other hand, the experts consulted point out that the CSA proposal requires the deployment of technologies that are inherently in conflict with what E2EE communications stand for – namely private communication. Hence the incentive to invest and develop E2EE communication could stagnate as the essence of this type of communication is affected by the CSA proposal.

The proposal would help online communication services to become more child-friendly, and it would lead to a more rapid identification and take-down of CSAM, a minimised risk of re-victimisation, and better protection against grooming. With regards to adult users without malicious intent, it can be expected that chilling effects would occur when the CSA proposal enters into force. Adult users without malicious intentions are expected to change behaviour to avoid false accusations of disseminating or consuming CSAM. Some users with malicious intent are expected to resort to the dark web, where detection is highly complex. Others are expected to continue their illegal activities on 'regular' communication channels and a part of this group is expected to be disincentivised to continue or start activities as a result of the CSA proposal.

Impact of the CSA proposal on the protection of fundamental rights

The CSA proposal is expected to impact the fundamental rights of the three main affected stakeholder groups differently. In aiming to prevent children falling victim to CSA, the proposal impacts several fundamental rights positively. It creates positive obligations for public authorities to act to protect: Articles 3 (the right to integrity of the person) and 4 (prohibition of torture) of the Charter of Fundamental Rights and Freedoms of the European Union (CFR) require that children's physical and mental integrity are being ensured; Article 7 CFR (right to privacy) mandates that children's private and family lives are protected, and Article 24 CFR demands that children are

protected from any form of violence. On the other hand, the measures, including CSAM detection orders, provided in the CSA proposal, can also negatively impact the fundamental rights of children as users of online services. More specifically, the right to privacy (Article 7 CFR), the right to data protection (Article 8 CFR), and the right to freedom of expression and information (Article 11 CFR) are affected. Limiting these rights may impact the personal development of children and their space to develop.

The proposal interferes with several fundamental rights of users of services by allowing for detection orders to be issued that oblige service providers to screen their services for the dissemination of CSAM, both known and new, or grooming. Firstly, this would interfere with the right to private life and communications (Article 7 CFR), as the CJEU has already acknowledged in respect of instances where traffic and location data are monitored, and would likely trigger a particularly serious infringement in cases where content of interpersonal communications is concerned. Secondly, it would interfere with the right to protection of personal data (Article 8 CFR), as screening by service providers constitutes a form of data processing. Thirdly, the freedom of expression and information (Article 11 CFR) would be seriously impacted, as screening of users' communications might deter people from openly expressing their views.

The proposal interferes with one of the fundamental rights of providers of information society services. Article 16 CFR (freedom to conduct a business) aims at safeguarding the right to each individual in the EU to operate a business without being subject to either discrimination or disproportionate restrictions. Imposing an obligation on service providers to install and maintain a costly computer system to monitor all electronic communications made through its network interferes with this right.

Prohibition of general data retention and general monitoring obligations
As part of the fundamental rights test carried out, this study analysed whether the negative impact on, Articles 7 and 8 CFR in particular, is justifiable (following the criteria established in Article 52 CFR and CJEU case law). In these considerations, the study looks at the criteria the CJEU has established on the prohibitions of general data retention and general monitoring obligations.

The prohibition of general data retention and general monitoring obligations are assessed for the detection, reporting and removing of known CSAM, new CSAM and grooming. The parameters to detect known CSAM can be set with a high degree of specificity, as the content has already been categorised as CSAM. However, as the CSA proposal does not require a detection order to target a specific group of users, the detection orders would violate the prohibition of general data retention and the prohibition of general monitoring obligations. In theory, the CSA proposal could be amended to require detection orders to specify targeting a certain group of users in line with the requirements of CJEU case law, to prevent detection orders from violating the prohibitions of general data retention and general monitoring. However, certain classifiers, such as geographic location, age, or gender, would not be appropriate features for specifying the groups of users subject to detection orders, because they cast the net too wide.

With respect to new CSAM and grooming, the parameters for detection cannot be set with high specificity, as compared with the detection of known CSAM, which exact content a technology ought to identify is not predetermined. With regard to new CSAM, the technologies can only be applied indiscriminately to all users of both hosting services and interpersonal communication services. The proposed rules regarding obligations to detect new CSAM, imposed both on hosting providers and (all the more) on interpersonal communications providers, disproportionately affect the right to privacy in terms of the group of users affected, which would amount to unlawful generalised monitoring and unlawful generalised surveillance. The requirements to detect grooming would not be sufficiently targeted and would, thus, amount to generalised and

indiscriminate automated analysis of all communications transmitted through interpersonal communication services by default.

Indeed, with regard to obligations on the scanning of the content of interpersonal communications (which includes grooming, new CSAM and likely known CSAM), this study concludes that the CSA proposal would compromise the essence of the fundamental right to privacy. Scanning content on users' personal devices in E2EE communications violates the essence of the right to data protection. In the case of E2EE communications, even should it not be accepted that the essence of the right to data protection is compromised, the device-side scanning of interpersonal communications is disproportionate to the aims pursued. It creates vulnerabilities and exposes users to a particularly increased risk of unlawful access.

Necessity and proportionality

The study also analysed the necessity and proportionality of the measures laid down by the CSA proposal. This examination would only apply in the case that, in the case of interpersonal communications, the argument that the CSA proposal measures impact the very essence of the Article 7 and 8 CFR were to be rejected.

The assessment of the necessity of the measures requires an analysis of whether the measures would be effective in achieving their goal and, if so, whether less intrusive means could achieve the same goal. With respect to effectiveness, there are two main concerns: (i) the current state of play of the technology to detect new CSAM and grooming is not sufficiently accurate for effective determination of CSAM, and (ii) the extent to which LEAs would be able to assess the potentially high number of reports in a timely manner. The evidence collected in the CSA proposal IA is too limited with respect to both concerns. Turning to the question of whether less intrusive ways could achieve the same goal as the detection order; article 4 of the CSA proposal presents the possibility of mitigation measures for providers of information society services, to reduce the risk of abuse of their service. Should the provider fail to adopt such measures voluntarily, the coordinating authority can issue a detection order. However, it does not provide the coordinating authority with a legal basis to take other, less intrusive, measures and, as such, the CSA proposal does not allow the coordinating authority to opt for less-intrusive measures to achieve the same objectives.

In considering proportionality of the measures, the study followed the case of *La Quadrature du Net*, where the CJEU set out that, for serious crime, as is the case for CSAM, the options for data retention are more restricted and should be more targeted (compared with issues of national security).

The proposed rules regarding the issuance of detection orders in the CSA proposal do not rule out detection orders that would provide a generalised data retention obligation on service providers. Therefore, with regard to the detection of known material, the CSA proposal raises proportionality concerns because of a lack of requirement as to how specific the detection order will be with respect to the targeted individuals. It is feasible for detection orders to specify a certain group of users to be targeted in line with CJEU case law. However, with regard to known material, proportionality concerns are raised in relation to the technologies used in detection in E2EE communications, the procedural safeguards regarding the issuance of detection orders and the duration of the detection order.

Furthermore, due to the nature of new CSAM and grooming, detection orders to detect these types of CSAM would require a general data retention duty for service providers. For the detection of new CSAM and grooming in E2EE communications, the same concerns arise as those raised in relation to the detection of known material. Therefore, new binding obligations stemming from detection orders for relevant service providers to detect, report, and remove new material and grooming from their services would likely fail the proportionality test. In addition, in relation to the technology used regarding the detection of CSAM in E2EE communications, the device side scanning of interpersonal communications is disproportionate to the aims pursued.

The proposed safeguards regarding the technologies used, the procedural aspects, such as the involvement of an EU centre, the conditions of issuance of a detection order and the duration of a detection order, cannot compensate for the lack of substantive safeguards in relation to all three types of content.

The proposed EU centre to prevent and counter child sexual abuse

The option of establishing an EU centre with some functions hosted by Europol and others in an independent organisation under Member State law is found to be most efficient. This differs from the conclusion reached in the CSA proposal IA, in which the option for a decentralised agency was found to be the preferred option. The main reason for this difference is that this study expects an EU centre with some functions hosted by Europol and others in an independent organisation under Member State law, to have a shorter timeframe for implementation. The benefits, therefore, are expected to materialise earlier than in other options.

However, it should be noted that it is difficult to conduct a cost-benefit analysis of an EU centre in this study, especially because such an EU centre would act in close collaboration with many other stakeholders and, therefore, the effectiveness of the EU centre would substantially depend on the action of others. The differences in costs and benefits between options are also small. Moreover, certain aspects could not be quantified and expressed in monetary terms. It should be noted that factors associated with independence, institutional culture and the proposed EU centre's signalling function (i.e., that the EU takes the matter seriously) can hardly be captured in a cost-benefit analysis.

Table of contents

1. Background, Objectives, and Methodology ____ 1

1.1. Background ____ 1

1.2. Outline of the CSA proposal ____ 2

1.3. Objectives of this study ____ 3

1.4. Methodology and limitations ____ 5

2. Analysis of the problem definition as expounded in the CSA proposal IA ____ 6

2.1. Description of problem definition in the CSA proposal IA ____ 6

2.2. Assessment of comprehensiveness of the problem definition in the CSA proposal IA ____ 7

2.3. Assessment of soundness of the problem definition ____ 8

2.4. How the CSA proposal covers the identified problems and drivers ____ 10

3. Impact of the CSA proposal on the internet ____ 11

3.1. Impact on technology ____ 13

3.2. Impact on quantity and quality of detected and reported content ____ 25

3.3. Impact on behaviour ____ 29

4. Impact of the CSA proposal on fundamental rights ____ 33

4.1. The fundamental rights checklist ____ 34

4.2. Fundamental rights impacted by the CSA proposal ____ 35

4.3. Nature of the (negatively) impacted fundamental rights ____ 41

4.4. CSA proposal in light of the prohibition of generalised data retention and general monitoring obligations in EU law ____ 42

5. Assessment of the necessity and proportionality of the proposed measures obliging providers to detect, report and remove CSAM ____ 50

5.1. Assessment of the legal basis for the interference ____ 52

5.2. Assessment of the objectives pursued by the CSA proposal ____ 53

5.3. Assessment of respect for the essence of the fundamental rights ____ 54

5.4. Assessment of necessity and proportionality 55

6. Review of the cost-benefit analysis for the creation of the EU Centre to prevent and counter child sexual abuse 64

6.1. Introduction 65

6.2. Objectives and activities of the EU Centre 66

6.3. Retained implementation options 67

6.4. Review of costs 68

6.5. Review of benefits 71

6.6. Review of the cost-benefit analysis 76

7. Conclusions 81

References 87

ANNEX I – Stakeholder consultation 93

ANNEX II – Problem definition as in CSA proposal IA 94

ANNEX III – Elaboration on technical solutions reflected upon in CSA proposal IA 95

ANNEX IV – Elaborated analysis of impact of the CSA proposal on fundamental rights 97

ANNEX V - CBA calculations and reflections 111

Table of tables

Table 1: Overview of research questions and corresponding chapters 4

Table 2: Assessed fundamental rights 35

Table 3: Overview of differences between regimes of prohibition on general data retention and prohibition of general monitoring obligations 43

Table 4: Overview of limitations for general data retention and general monitoring obligations provided for in CSA proposal 48

Table 5: Comparison of legislative options for the EU Centre 68

Table 6: Overview of total initial investment costs per option in million Euro (year 1) 69

Table 7: Overview of annual cost per option in million Euro (year 6) 69

Table 8: Overview of annual cost per option in million Euro (year 6) 70

Table 9: Development of staff of five existing agencies 71

Table 10: Overview of the benefits per option as estimated in the CSA proposal IA (year 6) 73

Table 11: Overview of the benefits per option as estimated by researchers (year 6) 76

Table 12: Overview of total costs per option in million Euro based on the estimates in the CSA proposal IA (in present value year 1 – year 10) 77

Table 13: Overview of total costs per option in million Euro based on estimates from the researchers (in present value year 1 – year 10) 77

Table 14: Overview of the benefits per option in million Euro based on the estimates in the CSA proposal IA (present value year 1 – year 10) 77

Table 15: Overview of total benefits per option in million Euro based on estimates from the researchers (in present value year 1 – year 10) 78

Table 16: Overview per option in million Euro based on the estimates in the CSA proposal (in present value year 1 – year 10) 78

Table 17: Overview per option in million Euro based on estimates from the researchers (in present value year 1 – year 10) 79

Table 18: Overview of consulted stakeholders 93

Table 19: Problem definition as presented in CSA proposal IA 94

Table 20: Identified solutions for detecting CSAM in E2EE 96

Table 21: Evaluated fundamental rights 97

Table 22: Relative difference in costs between Option C and Option B 113

Table 23: Relative difference in costs between Option C and Option D 114

Table 24: Overview of existing agencies and their ramp-up in staffing 115

Table 25: Overview of EU Centre costs per option and year, including corrections in million Euro 116

Table 26: Overview of EU Centre benefits per option and year, in million Euro _____ 116
Table 27: Discounted costs per option and year, including corrections in million Euro _____ 117
Table 28: Discounted benefits per option and year, in million Euro _____ 117
Table 29: Overview of EU Centre costs per option and year, in million Euro, SA1 _____ 117
Table 30: Discounted costs per option and year, in million Euro, SA1 _____ 118
Table 31: Overview of EU Centre benefits per option and year, in million Euro, SA1 _____ 118
Table 32: Discounted benefits per option and year, in million Euro, SA1 _____ 118
Table 33: Overview per option in million Euro (in present value year 1 – year 10), SA1 _____ 118
Table 34: Overview of EU Centre costs per option and year, in million Euro, SA2 _____ 118
Table 35: Discounted costs per option and year, in million Euro, SA2 _____ 118
Table 36: Overview of EU Centre benefits per option and year, in million Euro, SA2 _____ 119
Table 37: Discounted benefits per option and year, in million Euro, SA2 _____ 119
Table 38: Overview per option in million Euro (in present value year 1 – year 10), SA2 _____ 119
Table 39: Overview of EU Centre costs per option and year, in million Euro, SA3 _____ 119
Table 40: Discounted costs per option and year, in million Euro, SA3 _____ 119
Table 41: Overview of EU Centre benefits per option and year, in million Euro, SA3 _____ 120
Table 42: Discounted benefits per option and year, in million Euro, SA3 _____ 120
Table 43: Overview per option in million Euro (in present value year 1 – year 20), SA3 _____ 120

List of abbreviations

AI	Artificial Intelligence
API	Application Programming Interface
CBA	Cost-benefit analysis
CEPOL	European Police College
CJEU	Court of Justice of the European Union
CNIL	Commission Nationale de l'Informatique et des Libertés
CFR	Charter of Fundamental Rights and Freedoms of the European Union
CRC	UN Convention on the Rights of the Child
CSA	Child sexual abuse
CSAM	Child sexual abuse material
DSA	Digital Services Act
E2EE	End-to-end-encryption
EC	European Commission
ECHR	European Convention on Human Rights
ECPAT	End Child Prostitution and Trafficking
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EDRi	European Digital Rights
EECC	European Electronic Communications Code
ENISA	The European Union Agency for Cybersecurity
EPRS	European Parliamentary Research Service
ESP	Electronic Stability Program
FRA	European Union Agency for Fundamental Rights
GDPR	General Data Protection Regulation
HSI	US Department of Homeland Security Investigations
ICMEC	International Center for Missing and Exploited Children
IMEI address	International Mobile Equipment Identity address
INHOPE	International Association of Internet Hotlines
IP address	Internet Protocol address
LEA	Law Enforcement Authority
LIBE	European Parliament's Committee on Civil Liberties, Justice and Home Affairs
MAC address	Media Access Control address
NCMEC	US National Center for Missing and Exploited Children
NI-ICS	Number-Independent Interpersonal Communications Services
OPC	Open Public Consultation
RSB	European Commission Regulatory Scrutiny Board
SME	Small and medium-sized enterprises
URL	Uniform Resource Locator
US	United States
VPN	Virtual Private Network

Key terminology

Artificial Intelligence (AI): a software that is developed and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments it interacts with.[8]

Accuracy: number of correct predictions; it takes into account both the false positive rate and the false negative rate.[9]

Child sexual abuse material (CSAM): material constituting child pornography or pornographic performance.[10]

Children: natural persons under the age of 18.[11]

Deep web: the set of web pages on the World Wide Web that cannot be indexed by search engines, are not viewable in a standard Web browser, require specific means (such as specialised software or network configuration) in order to access, and use encryption to provide anonymity and privacy for users.[12]

Dark web: a section of the deep web primarily used for illegal purposes.

End-to-end encryption (E2EE): a secure communication process that prevents third parties from accessing data transferred from one endpoint to another.[13]

Error rates: false positives and false negatives. In this study this is content wrongfully labelled as CSAM when it is not, and to content not being labelled as CSAM while it actually is.

False negative rate: in the case of CSAM, this refers to content that has not been labelled as CSAM when it actually is CSAM.

False positive rate: in the case of CSAM, this refers to content that has been labelled as CSAM when it is actually not.

Grooming (solicitation of children): when an adult seeks to meet a minor for the purpose of engaging in sexual activities with the child, or the production of child pornography.[14]

Hashing technology is a type of digital fingerprinting.[15]

Perceptual hashing is a type of digital fingerprinting in which small modifications to the picture (or video) such as rotation, cropping, changing colours that do not change the visual appearance, result in small changes to the digital fingerprint.

---

8 Proposal for a Regulation laying down harmonised rules on artificial intelligence, COM(2021) 206 final, European Commission, April 2021, Article 3.

9 Confusion matrix, accuracy, recall, precision, false positive rate and F-scores explained, NillsFblog, accessed 8 March 2023.

10 Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, European Commission, May 2022, Article 2(l).

11 Ibid., Article 2(i).

12 Dark web, Merriam-Webster, accessed 1 March 2023.

13 What is end-to-end-encryption, IBM, accessed 28 February 2023.

14 Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, European Commission, May 2022, Article 2(o).

15 Impact Assessment Report Accompanying the document Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, European Commission, May 2022, p. 279.

Hosting service: an intermediary service consisting of the storage of information provided by, and at the request of, a recipient of the service;[16]

Internet access service: a publicly available electronic communications service that provides access to the internet, and thereby connectivity to virtually all end points of the internet, irrespective of the network technology and terminal equipment used.[17]

Interpersonal communication content means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information.[18]

Interpersonal communications service: a service that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s);[19]

Known CSAM refers to content that has previously detected and identified as constituting child sexual abuse material.[20]

Machine learning: a subfield of artificial intelligence that gives computers the ability to learn without explicitly being programmed.[21]

New CSAM: content that has not previously detected and identified as constituting child sexual abuse material.[22]

Number-independent interpersonal communications service is an interpersonal communications service which does not connect with publicly assigned numbering resources, namely, a number or numbers in national or international numbering plans, or which does not enable communication with a number or numbers in national or international numbering plans.[23]

Online child sexual abuse: the online dissemination of child sexual abuse material and the solicitation of children.[24]

S*ensitivity*: this is the probability of a positive test, conditioned on truly being positive. In the case of CSAM, this refers to the probability that CSAM is actually being detected as such.

---

16 Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services.

17 Regulation (EU) 2015/2120 of 25 November 2015 laying down measures concerning open internet access, Article 2(2).

18 Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Article 2 (d).

19 Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code, Article 2(e).

20 Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, European Commission, May 2022, Article 2(m).

21 Machine learning, explained, MIT Management, accessed 8 March 2023.

22 Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, European Commission, May 2022, Article 2 (7).

23 Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code, Article 2(e).

24 Ibid., Article 2(p).

Software application store: a type of online intermediation services, which is focused on software applications as the intermediated product or service;[25]

Software application: any digital product or service that runs on an operating system;[26]

Specificity: the probability of a negative test, conditioned on truly being negative. In the case of CSAM, this refers to the probability that content that is not CSAM is actually not being detected as such.

Traffic and location data refers to any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof (traffic data) and any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service (location data).[27]

[25] Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector, Article 2(15).

[26] Ibid.

[27] Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Article 2 (b – c).

1. Background, Objectives, and Methodology

1.1. Background

The European Commission identified the fight against child sexual abuse (CSA) as one of its key priorities.[28] The EU strategy for a more effective fight against CSA aims to provide an effective response to fight CSA at the EU level. It sets out eight initiatives to implement and develop a legal framework, strengthen the law enforcement response, and catalyse coordinated multi-stakeholder action in relation to prevention, investigation, and assistance to victims, to be implemented by 2025. Alongside a series of other policy and legislative initiatives, this strategy will guide EU action in this domain.

One of the components of this strategy is the temporary derogation to the e-Privacy Directive[29], commonly referred to as the Interim Regulation[30], which provides a temporary legal basis enabling Number-Independent Interpersonal Communication Services (NI-ICS) to continue their voluntary practices for detection, reporting, and removal of CSA material (CSAM) online. The Interim Regulation aims to bridge the gap created by the entry into force of the extended scope of the e-Privacy Directive[31], which prevents certain companies from continuing their own measures on voluntarily detecting, removing and reporting online CSAM. The proposal for an Interim Regulation was submitted to the European Parliament and the Council of the EU in the autumn of 2020. This proposal was not accompanied by an impact assessment (IA), and therefore, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) requested the EPRS to conduct a targeted substitute IA.[32]

The Interim Regulation entered into force in July 2021 and will remain in force until 3 August 2024, (or until an earlier date if the current proposal for a regulation is adopted by the EU legislators and repeals this temporary measure) until which providers of information society services may continue their activities. Against this background, on 11 May 2022, the European Commission adopted a proposal for a Regulation to prevent and combat child sexual abuse (CSA proposal), which aims to establish a long-term framework.

The CSA proposal builds on the Interim Regulation. It would further advance the EU's and Member States' activities in the fight against CSA. Its general objective is to improve the functioning of the internal market by introducing EU rules to prevent and combat CSA, particularly by imposing detection, reporting, and removal obligations on certain relevant information society services.[33]

The CSA proposal is accompanied by a European Commission impact assessment (CSA proposal IA).[34] The draft impact assessment initially received a negative opinion from the European

---

[28] Communication on EU strategy for a more effective fight against child sexual abuse, COM/2020/607 final, European Commission, July 2020.

[29] Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

[30] Regulation (EU) 2021/1232 of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC.

[31] Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

[32] Commission proposal on the temporary derogation of the e-Privacy Directive for the purpose of fighting online child sexual abuse, targeted substitute impact assessment, EPRS, February 2021.

[33] Impact Assessment Report Accompanying the document Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, European Commission, May 2022, p. 43.

[34] Ibid.

Commission's Regulatory Scrutiny Board, which is the European Commission's internal body scrutinising the quality of all draft impact assessments.[35] As a response, the Commission services revised the draft IA and shared a second draft version with the Regulatory Scrutiny Board in January 2022. This time the Board issued a positive opinion with reservations.[36]

1.2. Outline of the CSA proposal

The CSA proposal aims to address the misuse of information society services for online CSA.[37] The proposal primarily affects three stakeholder groups: children, users, and providers of information society services. The obligations laid down in the proposal are addressed primarily to providers of information society services, but national authorities would play a substantial role in implementing the CSA proposal.

In a nutshell, the CSA proposal introduces a two-step approach requiring providers of information society services first to conduct risk assessments to identify whether their services are misused for disseminating CSAM.[38] Providers of information society services are obliged to take appropriate measures based on the risk assessment outcome. As a second step, the proposal introduces the possibility for judicial authorities or independent administrative authorities at the national level to issue detection, removal, or blocking orders to providers of information society services if the risk assessment provides reasons to do so.[39]

Providers of information society services comprise of broadly two groups: (1) providers of interpersonal communication services; and (2) those that provide hosting services. Each group plays a slightly different role in the fight against CSAM, as the services they provide involve different categories of personal data, namely content of communications during transmission, device-side scanning of content of communications before transmission, content retrieved via internet access, content on hosting services, app stores, traffic and location data.

The CSA proposal prescribes procedural guidelines and safeguards concerning the scope of the detection order, the timeline, the application, the protection of personal data, and quality management. Additionally, the proposal envisages the establishment of an EU Centre (in the form of an EU agency) to prevent and combat child sexual abuse.[40]

Furthermore, the proposal differentiates between three different types of CSAM: known CSAM (content that has already been categorised as CSAM), new CSAM (content that has not been categorised as CSAM before) and the solicitation or grooming of children.[41]

The proposed rules are to be applied to all types of interpersonal communication, including encrypted and non-encrypted communications. While the legislative proposal does not make this

---

35 European Commission Regulatory Scrutiny Board, Regulatory Scrutiny Board Opinion Regulation on detection, removal and reporting of child sexual abuse online, and establishing the EU centre to prevent and counter child sexual abuse SEC (2022) 209, 2022.

36 Ibid.

37 Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, European Commission, May 2022, Article 1.

38 Ibid., Article 3 – 5.

39 Ibid., Article 7 – 18.

40 Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, European Commission, May 2022, Article 40.

41 Ibid., Article 2.

distinction explicitly, end-to-end encryption (E2EE)[42] is referred to in recital 26 and the IA.[43] Including E2EE communications in the scope of application of the CSA proposal constitutes a change compared to the Interim Regulation, which only provides a legal framework for providers of information society services to detect, report, and remove identified CSAM in non-E2EE communications.

1.3. Objectives of this study

This study presents the findings of the complementary IA[44] of the CSA proposal[45] and adds to the substitute IA of the Interim Regulation[46] by the EPRS, published in February 2021.[47] First and foremost, this study does not question the importance and the need to fight CSA(M).

The LIBE committee formulated six research questions for the EPRS to answer and they constitute the core of this study. The following table presents these research questions and indicates the different chapters of this study in which they are addressed.

[42] E2EE is a form of encryption where data is encrypted on the sender's device and can only be decrypted by the recipient's device. This means that the data is protected from anyone who might try to intercept it, including internet service providers, government, and hackers.

[43] Impact Assessment Report Accompanying the document Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, European Commission, May 2022, p. 279.

[44] Ibid.

[45] Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, European Commission, May 2022.

[46] Proposal for a Regulation on a temporary derogation from certain provisions of Directive 2002/58/EC, COM(2020) 568 final, European Commission, September 2020.

[47] Commission proposal on the temporary derogation of the e-Privacy Directive for the purpose of fighting online child sexual abuse, targeted substitute impact assessment, EPRS, February 2021.

Table 1: Overview of research questions and corresponding chapters

Chapter	Research question
2	Considering the problem definition in the CSA proposal IA, are all dimensions and aspects of the problem covered and adequately analysed?
3	What is the likely impact of the CSA proposal on the internet? In particular: a. What would be the technological implications?[48] b. Would mandating the use of CSAM-detection technology disrupt end-to-end encryption and decrease the level of security? c. What would be the behavioural implications? d. Would users change their behaviour if it becomes common knowledge that companies are scanning their private messages (possible chilling effects)? e. What is the likely impact, both in terms of quantity and quality of detected and reported content, of the move away from voluntary measures, subject to the conditions specified in the Interim Regulation, to the system of mandatory measures proposed in the draft Regulation? f. What are the technological parameters, possibilities and limitations to further improve the accuracy to detect CSA material and grooming in particular?
4	What is the likely impact of the CSA proposal on fundamental rights, in particular, the right of the child, the right of the victim, the right to liberty and security, the right to data protection and the right to privacy, which includes the protection of private communications? [49]
5	Are the measures foreseen in the CSA proposal necessary and proportionate, in particular regarding the new binding obligations for relevant service providers to detect, report and remove from their services known and new CSAM or text-based threats such as grooming, having regard to the CJEU case law and notably the judgment *La Quadrature du Net*?
5	How would the detection of new CSAM or grooming respect the prohibition of general monitoring obligations? Are the new obligations and requirements foreseen in the CSA proposal precise enough as to not violate the prohibition of general monitoring obligations?
6	Reviewing the cost-benefit analysis of the European Commission and complementing it, if necessary, what would be the preferred option among the three retained options for an EU Centre to prevent and counter CSA: a stand-alone agency, a Centre attached to Europol or a Centre attached to the Fundamental Rights Agency?
7	How effective and efficient is the CSA proposal in addressing the problem?

Source: Ecorys

[48] The research question answered in Chapter 3 is comprised of six sub-questions. All questions are answered as part of the same chapter. Given the overlap between the sub-questions, not all of them are answered under separate headings. Instead, sub-question a, b, and f, as well as c and d, are grouped.

[49] The research questions answered in Chapter 4 and 5 are closely linked. Therefore, Chapter 4 provides a theoretical framework for the analysis, which is done in Chapter 5.

1.4. Methodology and limitations

This complementary IA was conducted between December 2022 and March 2023. Different data collection methods were used.

(1) Desk research and literature review included academic and applied research publications[50] relevant case law, and policy documentation. The goal was to establish a knowledge basis of existing research and outline the legal framework within which the CSA proposal operates. An overview of the consulted documentation is available at the end of this study;

(2) Semi-structured expert interviews (n=16)[51] included public and private sector experts in privacy and data protection, fundamental rights, child protection, law enforcement, and ICT. The goal was to complement the findings from the desk research and to obtain a balanced understanding of the broad implications of the CSA proposal. Annex I presents an overview of the consulted stakeholders;

(3) Ad-hoc consultation included stakeholders who, on their own initiative, shared information via the EPRS with the researchers.

This study is guided by the European Commission's Better Regulation Guidelines.[52] Specifically, Chapters 4 and 5 form the fundamental rights test whereby proposed measures that negatively impact fundamental rights are tested against article 52 of the Charter of Fundamental Rights of the European Union (CFR).[53] [54] In addition, tool # 63 of the Better Regulation Toolbox guided the cost-benefit analysis of the creation of the EU Centre to prevent and counter CSA.[55]

This study has three key methodological limitations. First, the study is narrow in scope. By nature, a complementary IA focuses on specific aspects and omits others. While this study was developed to be as comprehensive as possible, some elements of the CSA proposal and its impact received less attention as the researchers were primarily guided by the six research questions submitted by the LIBE committee.

Second, while ample documentation and written input from various organisations on the CSA proposal is available, the amount of evidence-based academic research on the impact of the proposal is limited. This is particularly the case for the impact of the proposal on technology, the quantity and quality of detection, and on behaviour. For this reason, the study sometimes relies predominantly on expert input.

Third, the researchers had limited access to documentation supporting the cost-benefit analysis by the European Commission of the EU Centre to prevent and counter CSA. Therefore, the cost-benefit in this study is, at times, developed based on expert assumptions.

[50] The researchers focused on studies published in the past five years.

[51] This includes two stakeholders that provided written feedback.

[52] Better Regulation Guidelines, European Commission.

[53] Charter of Fundamental Rights of the European Union, December 2017.

[54] Better regulation toolbox, European Commission, p. 243-244.

[55] Better regulation toolbox, European Commission, p. 554-557.

2. Analysis of the problem definition as expounded in the CSA proposal IA

Answer to the corresponding research question in brief

Considering the problem definition in the Commission's IA, are all dimensions and aspects of the problem covered and adequately analysed?

(1) In the problem definition it is argued that fragmentation of legal frameworks across Member States to urge providers of information society services to detect, report, and remove CSAM would negatively affect cooperation between national authorities and providers of information society services. It is questioned whether this would actually be the case, as national legal frameworks are likely contributing to creating an equal level playing field within a Member State, thereby positively impacting cooperation.

(2) In the problem definition it is argued that the fragmentation of legal frameworks across Member States also negatively impacts the internal market. The evidence to support this claim is found to be rather weak. In addition, it can be questioned whether the fragmentation of legal frameworks across Member States can be considered as the driver that calls for the introduction of an EU-wide approach or whether the actual problem driver is CSA.

(3) While the impact of E2EE communication on the detection of CSAM is substantial, the problem definition only addresses this element briefly. No measure in the CSA proposal is designed to address this element directly.

(4) The problem definition is weakened by limited contextualisation of quantitative data, by providing insufficient evidence for the persistence of the problem and by presenting stakeholder views to a limited extent.

2.1. Description of problem definition in the CSA proposal IA

This section assesses the problem definition as presented in the CSA proposal IA. This assessment has been made based on the Better Regulation Guidelines and Toolbox (2021).[56] These guidelines guide how the European Commission should assess a problem, how the problem analysis should be built up, which argumentation should be used, and how it should be used. The most relevant sections are Tools #7 to #17 on how to perform an IA and Tools #51 to #55 on stakeholder consultation.

To analyse a problem, the European Commission ought to describe the problem first. A problem consists of several drivers, each with several underlying drivers. Chapter 2 of the CSA proposal IA describes the problem, the three problems drivers, and the underlying drivers.[57] Annex II provides an overview of the problem definition (including problem drivers and underlying drivers), as presented in the CSA proposal IA. The table also includes, for each of the problem drivers, the corresponding measures proposed.[58]

---

[56] Better Regulation Guidelines, European Commission.

[57] Impact Assessment Report Accompanying the document Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, European Commission, May 2022, p. 16.

[58] Ibid., p. 53.

2.2. Assessment of comprehensiveness of the problem definition in the CSA proposal IA

As highlighted throughout the CSA proposal IA, the problem that the European Commission aims to address with the proposal is the role providers of information society services play in the detection, reporting and removal of CSAM. When assessing the comprehensiveness of the problem definition, this aim should be kept in mind. According to the Better Regulation Guidelines (2021), the problem, problem drivers and underlying drivers need to form a coherent and logical framework. For this IA, this means that the problem, problem drivers and underlying drivers should form a coherent framework explaining why EU action on the role of the providers of information society services in combatting CSA is required. Several key observations can be made when assessing the problem in relation to the problem drivers. These are presented in more detail in the two sections below.

2.2.1. Unclear link between legal fragmentation, inefficient cooperation, and the internal market

One of the problem drivers (#2) identified by the European Commission relates to inefficient cooperation between providers of information society services, public authorities, and civil society (see the table in Annex II). The accompanying analysis provided in the CSA proposal IA on this driver lacks clarity.

First, in the problem definition the fragmented legal framework and its impact on the internal market is highlighted. A link is made to the cooperation between public authorities and providers of information society services (underlying driver #2.1). The European Commission states that some Member States have adopted national legislation to urge providers of information society services to detect, report, and remove CSAM.[59] This is because with a voluntary regime in place, providers of information society services are not obliged to detect, report, and remove CSAM and, as a result, not all providers do so. Arguably, if this is the underlying reason for Member States to adopt legislation, the legal fragmentation is an argument that relates more to the first problem driver (#1. voluntary action by providers of information society services to detect online CSA has proven insufficient) rather than to the second.

Moreover, the argument that legal fragmentation would negatively affect cooperation between public authorities and providers of information society services, thereby negatively impacting the internal market, is not further detailed in the problem definition. In fact, it is debatable whether this argument is solid. From a legal perspective, national legislation would create an equal level playing field between providers of information society services in that Member State, thereby likely improving the cooperation between public authorities and providers of information society services.

Finally, the European Commission reasons that adopting EU-wide rules to create a more harmonised approach to detecting, reporting, and removing CSAM would help address the legal fragmentation.[60] The CSA proposal IA argues that such a harmonised approach would benefit children, but it would also reduce the discrepancies between providers of information society services' responses.[61] However, it can be questioned whether the varying national legal frameworks should be the primary reason for adopting EU-wide measures or whether the primary reason should

[59] Ibid., p. 31.

[60] Ibid., p. 24.

[61] Ibid.

be the protection of children against sexual abuse. The national legislation can be understood as a consequence of the absence of EU law and not necessarily the reason for adopting EU law.

2.2.2. Unclear how Member State efforts relate to the role of information society services

The problem, as identified by the European Commission, also refers to the need for prevention and assistance to victims, which is further detailed in the third problem driver (#3). While the prevention of CSA and assistance to victims can be considered pivotal issues in the fight against CSA, it can be questioned whether these components are best addressed through the proposed legislation. As confirmed by the European Commission during an interview for this study, prevention and assistance provided by Member States is also part of other legal initiatives related to CSA.

By including the prevention and assistance to victims in the problem definition of the CSA proposal, the focus of the CSA proposal on providers of information society services is diluted. The role of providers of information society services in solving issues related to inadequate prevention of CSA and assistance to victims is limited, as it is the Member States' responsibility is to ensure adequate prevention and assistance. As a result, the clear link between the problem, the problem drivers and the underlying drivers weakens.

2.3. Assessment of soundness of the problem definition

2.3.1. Soundness of the presented argumentation

Certain observations regarding the problem definition can be made, specifically regarding the technical implications of E2EE communications and its benefits.

In the problem definition, the shift towards E2EE communication is briefly mentioned as one of the underlying drivers of the first problem driver (i.e. voluntary action by providers of information society services to detect online CSA has proven insufficient).[62] Although the CSA proposal IA signals this trend, it pays little attention to that driver in relation to the fight against CSA. The increased use of E2EE communication hampers the sufficient detection, reporting and removal of CSAM. The issue could have been considered as a separate problem driver, which would have required a targeted solution.[63]

2.3.2. Soundness of the used evidence

The problem definition presents several problem drivers, each with a set of underlying drivers. Evidence is presented for each. Observations can be made regarding (i) the limited contextualisation of quantitative data, (ii) the insufficient evidence for the persistence of the problem and (iii) limited presentation of stakeholder views in the problem definition.

Limited contextualisation of quantitative data

It is difficult to obtain a clear and comprehensive picture of the magnitude of CSA. This is partially due to the lack of available data on the Member State level and underreporting or dark figures of CSA.[64] In the CSA proposal IA, the European Commission has to present the available quantitative

62 Ibid., p. 27.

63 See Better regulation toolbox, European Commission, tool #16, p. 114.

64 Ibid. 259.

data to support the problem definition. However, in various instances, the quantitative data that is presented is insufficiently contextualised.[65] For example, some of the data presented[66] shows an increase in the detection of CSAM by providers of information society services. In the problem definition, however, this information is mainly used to show that CSA is a serious problem. The reason why the number of reports has increased and whether this is related to more online material or more detection is not discussed.

Insufficient evidence for the persistence of the problem

The CSA proposal IA provides an analysis of the persistence of the overall problem, i.e., the problem of CSA.[67] However, this analysis is qualitative, high-level and lacks quantification and concretisation. As the analysis of the persistence of the overall problem forms input for the baseline needed for further analysis in the IA, an attempt at quantification should have been made, according to the Better Regulation Toolbox.[68] As this is lacking, the evidence for the persistence of the problem is rather weak.

In addition, the European Commission does not explain how the problem drivers would evolve without any EU action. The European Commission merely states that: "it is unrealistic to expect that, in the absence of incentives or obligations, the relevant service providers would implement sufficient voluntary measures, given that many have failed to do so to date despite the evident proliferation of CSA online".[69] The evidence underpinning this statement is not clarified, which constitutes a weakness in the analysis of the persistence of the problem.

Limited presentation of stakeholder views in the problem definition

In any policy process, stakeholder views need to be taken into account. In the Better Regulation Guidelines and Toolbox, guidance is provided on how to involve stakeholders in the policymaking process. The European Commission has consulted various stakeholders[70] on the CSA proposal (including the problem definition) as part of the legislative process. In the problem assessment, some stakeholder views from the consultations conducted for the CSA proposal IA are included.[71] In this regard, several observations are made.

Various arguments in the problem definition fall short of supporting evidence from stakeholder consultations conducted for the CSA proposal IA. Underlying drivers and problem drivers are predominantly based on information resulting from written sources. Whether the stakeholders consulted identify with the problems described generally remains unclear.

When stakeholder views are included in the analysis, it mainly covers the views of only a few groups instead of all stakeholders affected by the problem. The views of EU citizens[72] and public authorities[73] are presented. In contrast, views from, for example fundamental rights organisations,

---

65 Kesteren et al., 'CSAM Data Factcheck of recent European Commission statements', 2023, p. 9.

66 Such as the one on page 22 or the ones included in Annex 6 of the CSA proposal IA.

67 Section 2.3.

68 Better regulation toolbox, European Commission, tool #60, p. 538.

69 Impact Assessment Report Accompanying the document Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, European Commission, May 2022, p. 38.

70 Stakeholder groups consulted include: citizens, service providers, public authorities, practitioners, NGOs, IGOs, EU institutions, and academia.

71 Impact Assessment Report Accompanying the document Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, European Commission, May 2022, p. 18, 23, 30, 35, 38.

72 Ibid., p. 23.

73 Ibid., p. 35.

providers of information society services, and civil society organisations seem to be underrepresented in the analysis.

2.4. How the CSA proposal covers the identified problems and drivers

In the CSA proposal IA, the core problem and problem drivers identified are linked to the proposed measures. The table in Annex II presents the link between the three problem drivers and the proposed measures. As the table shows, most measures proposed in the CSA proposal (seven out of the eight) aim to tackle the first problem driver (i.e., voluntary action by providers of information society services to detect online CSA has proven insufficient). Not only will providers of information society services be obliged to detect, report, and remove different forms of CSAM (such as known, new, and grooming), an EU Centre that supports combatting CSA as well as provides assistance to victims will be established. Whether the measures proposed are indeed the most effective is assessed throughout the remainder of this study.

For problem drivers 2 and 3, only one measure has been developed, i.e., the EU Centre on prevention and assistance to victims. The proposed EU Centre is further assessed in Chapter 6, which presents the cost and benefit analysis.

3. Impact of the CSA proposal on the internet

Answer to the corresponding research question in brief

What is the likely impact of the CSA proposal on the internet? In particular:

a. What would be the technological implications?
b. Would mandating the use of CSAM-detection technology disrupt end-to-end encryption and decrease the level of security?
f. What are the technological parameters, possibilities, and limitations to further improve the accuracy to detect CSA material, and child solicitation in particular?

(1) On open communication channels, known material can be detected with relatively high accuracy. Nevertheless, risk for abuse (i.e., changing content so that it is not detected) remains. Thus, the detection of known material on open communication channels can be deemed feasible and realistic when a certain risk of abuse is accepted. The envisaged EU Centre to prevent and combat CSA is foreseen to provide a database of hashes, standardisation and norm-setting, thereby aiding the detection of known material.

(2) Technology to detect new material is increasingly accurate. Nevertheless, accuracy levels remain substantially lower than those of the technologies aimed at detecting known material. This raises the question as to which accuracy levels are deemed sufficient to deploy such technologies on a large scale, also when taking into account the impact that false positives have on people's lives and the capacity at LEA and the EU Centre required to sift through reported content.

(3) At this point in time, detecting new material and grooming results in substantial amounts of false positives and false negatives and, in particular, the accuracy levels of the tools used to detect grooming can be considered insufficiently accurate to be deployed on a large scale. The detection would, moreover, require cultural and context-sensitive technologies to identify grooming accurately, which are currently not sufficiently developed.

(4) Technologically, the detection of CSAM in E2EE communications is possible but the solutions available are not sufficiently transparent and secure, and known detection mechanisms undermine the end-to-end protection offered by the encryption.

(5) Detection of CSAM in E2EE communications would also impact the user's private life and their shared (semi-)public sphere and enhance the vulnerabilities to attacks and abuse and would raise practical issues related to trust, accountability, and transparency.

(6) It is unlikely that technologies to detect CSAM in E2EE communications develop rapidly to reach high accuracy levels in the upcoming two to five years, without undermining the secure nature of E2EE communications and the security at the end devices. The same conclusion can be drawn with regard to the technologies that could identify new CSAM or grooming (in open communication channels and/or E2EE communications). Solutions that have more potential include analyses of user behaviour and metadata such as network signals. Improving user empowerment (of children and adults) to allow them to report CSAM more easily is identified as a more feasible solution at this point in time.

e. What is the likely impact, both in terms of quantity and quality of detected and reported content, of the move away from voluntary measures, subject to the conditions specified in the Interim Regulation, to the system of mandatory measures proposed in the draft Regulation?

(1) Expert views on the expected impact on the quantity of reported content differ. They range from an expectation that reported content will decrease (resulting from the absence of a legal basis for voluntary monitoring, use of restricted classifiers and the 'disincentivising' effect that the CSA proposal will have) to an expected sharp increase due to the obligatory nature of the CSA proposal. The majority of consulted experts expect a steep increase in reported content as providers of information society services would be obliged to detect and report more, and the CSA proposal covers known material, new material and grooming. This prediction is fuelled by the expectation that some providers of information society services might resort to overreporting in order to avoid liability claims.

(2) An increase in the quantity of reported content may not necessarily result in an equivalent increase in investigations and prosecutions, and, thus, better protection of children. As long as the capacity of LEAs is limited to its current size, an increase in reporting will make effective investigation of CSAM more difficult. Furthermore, the feasibility of the foreseen role of the EU Centre in filtering the expected vast amount of (false positive) reports before they are shared with LEA is questioned.

(3) It is expected that the overall quality of detection is likely to deteriorate due to the compulsory detection of new CSAM and grooming. These types of CSAM require the application of technologies that have relatively low accuracy levels compared to the technologies that can detect known material. This would thus result in higher error rates (both false positive and false negatives).

(4) An increase of reported content could be beneficial to LEAs as it would allow for better training of the LEA systems that can help investigate and prioritise CSAM cases. Nevertheless, this benefit would only materialise when ample resources and priority to detect CSA are granted by Member States.

c. What would be the behavioural implications?

d. Would users change their behaviour if it becomes common knowledge that companies are scanning their private messages (possible chilling effects)?

(1) It is expected that the CSA proposal would impact the workload of providers of information society services substantially, which could incentivise such providers to consider moving their services outside the EU. The impact on the incentive of providers of information society services to innovate is expected to be twofold. On the one hand, the CSA proposal might negatively impact the desire to innovate in E2EE as the CSA proposal directly interferes with the core principle of E2EE. On the other hand, the need to develop technologies that can accurately detect known material, new material and grooming might accelerate innovation in CSAM detection mechanisms (although reaching high accuracy levels in the near future remains unlikely).

(2) The CSA proposal might impact children that use online communication services in two ways. The safety by design principle fostered by the CSA proposal would create safer and more secure environments for children. In addition, the CSA proposal is expected to allow for more rapid identification of images, reduce re-victimisation and more protection against grooming. Simultaneously, children (teenage minors) might feel uncomfortable when consensually shared images could be classified as CSAM.

(3) With regards to adult users with no malicious intentions, chilling effects are likely to occur. This group is expected to alter some types of behaviour in order to avoid mistakenly being identified as a perpetrator. Furthermore, a part of the group of users who do consume CSAM is not expected to change behaviour by any type of legislation or intervention. A part of this group might shift their activities to illegal platforms such as the dark web or deep web, thereby further thwarting detection. However, for a variety of reasons, a part of the users who consume CSAM are likely to remain active on 'regular' communication channels (E2EE or not).

(4) Generally, it can be concluded that the level of accuracy of the detection technologies also impacts the ways in which behaviour by users would change. The greater the accuracy with which technologies can detect CSAM, the less negative impact the proposal would have on the behaviour of its users of online communication services (both children and adults).

3.1. Impact on technology

In this section, the impact of the CSA proposal on the technologies to be implemented to detect, remove and block CSAM will be assessed. First, the current state of play with regards to the detection and reporting of CSAM (in non-E2EE) communications) will be presented. Second, potential avenues for detecting CSAM in E2EE communications will be discussed as this requires an additional layer of technology (namely, to 'intercept' the messages before their encryption).

3.1.1. Current state of play in detection of CSAM

This section introduces the most frequently applied methods for detecting known and new CSAM, and grooming. The potential for detecting CSAM differs per type of material, however, some general observations are relevant to all types. Namely, detecting CSAM is geared towards identifying whether content could potentially be CSAM. It does not seek to identify what the content is displaying exactly.[74] In addition, detecting CSAM is often a combination between technology and human verification. This combination is required both to reduce the error rates and to train machine learning used to detect CSAM.

Detection of known material

The detection of known material is primarily done through the application of so-called hashing technology and perceptual hashing technology, both types of digital fingerprinting also used in the

[74] Impact Assessment Report Accompanying the document Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, European Commission, May 2022, p. 279.

identification of malware or copyright infringements.[75] This approach allows one to compare the fingerprints of images more efficiently, as opposed to the comparison of entire images. Also, the technology allows for the storing of a targeted list of fingerprints, which means providers do not need to store and process images.[76] There are different software solutions used to detect CSAM via hashing. Microsoft's PhotoDNA is one of the most widespread tools used for hashing photos and videos.[77] Other examples are HashKeeper[78] and MediaDNA[79], but also Photo Detection of Child Sexual Abuse Material and SmartID respectively developed by the US National Center for Missing and Exploited Children (NCMEC) and the International Centre for Missing and Exploited Children (ICMEC).

Hashing is a critical tool used in the fight against CSAM. It creates unique digital fingerprints of images and videos containing CSAM, stores information in databases and use it to identify and track the spread of content on the internet. It also is used to identify content on online platforms, such as social media and file-sharing networks. It can quickly scan large volumes of data to identify images and videos that match known CSAM fingerprints. Hashing can also be used to automatically remove content from online platforms and prevent further spreading. For example, online platforms can use the technology to scan user-generated content for CSAM before it is even uploaded.

Hashing takes place in several steps.[80] First, when potential CSAM is detected, the tool identifies the specific images involved. Second, it creates a unique fingerprint (a hash) of the image by changing the colour of the image, filtering salient image features, and parting the image into quadrants based on which the hash is developed. The hash is irreversible, meaning that the original image cannot be recreated from the hash. In a third step, the created hash is compared against a database of hashes of known CSAM. This is filled with hashes that fulfil certain criteria (i.e., that depict a form of CSA) and all included hashes in the database are reviewed for by human verification. When the attempt to match the hash with the database does not yield a positive result (i.e., no match is found), the hash is not kept. When it does result in a match, additional steps can be taken to report and remove the content (see below). Currently, such matching generally is done against the NCMEC database. The CSA proposal foresees the creation of an EU Centre to prevent and counter CSA which would create and maintain a database of hashes. By doing so, the EU Centre could play a central role, also in the light of technical standardisation and norm-setting.[81]

The reliability of PhotoDNA is claimed by Microsoft to be high: it has a claimed false positive rate of 1 in 50 billion images.[82] However, experts' views on the accuracy of technologies vary, and some highlight the vulnerability of the technology for purposeful false negatives (CSAM not being detected as such) and false positives (non-CSAM being detected as such).[83] These can be created

---

75 How PhotoDNA for Video is being used to fight online child exploitation, Microsoft, accessed 23 December 2022; Impact Assessment Report Accompanying the document Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, European Commission, May 2022, p. 280.

76 Abelson et al. 'Bugs in our Pockets: The Risks of Client-Side Scanning', 2021, p. 7.

77 How PhotoDNA for Video is being used to fight online child exploitation, Microsoft, accessed 23 December 2022; Please note that PhotoDNA is a tool used for hashing, not for perceptual hashing.

78 HashKeeper, accessed 27 March 2023.

79 Technologies to stop CSAM: Binary Hashing, NetClean, accessed 27 March 2023.

80 Impact Assessment Report Accompanying the document Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, European Commission, May 2022, p. 279.

81 Expert input by academics.

82 Farid, H. 'Fostering a Healthier Internet to Protect Consumers', accessed 1 March 2023, p. 2.

83 Hintersdorf et al., 'Investigating the Risks of Client-Side Scanning for the Use Case NeuralHash', 2022, p. 1.

when images are slightly altered (i.e. in colour or by tilting)[84], and this can potentially happen on large-scale to create an overload of images to be sifted through (i.e. a false-positive attack).[85] While some attacks require knowledge of the description[86], others can be applied to a broad class of schemes[87], the details of which may not be known. While no independent review of PhotoDNA is available, the tool could, in theory be subject to an independent expert review as it is relatively transparent (in comparison to the tools used to detect new CSAM, grooming and those that detect CSAM in E2EE communications).

The use of perceptual hashing to match hash values rather than images and videos is more privacy-friendly than a solution in which the matching happens on the data itself (i.e. hashing).[88] However, the flip side of this is a reduced accuracy of detection and the need to keep the description of the perceptual hash function secret.[89] The required secrecy of the perceptual hash function impacts the suitability of this solution to be deployed on a wide scale.

Detection of new material

New CSAM cannot be identified based on hashing because the detected images (and their unique hashes) will not result in any matches in the hash database. Therefore, new material can only be detected through the use of classifiers and artificial intelligence. Classifiers are algorithms that sort data into classes or categories based on machine learning.[90] Classifiers can, for instance, be trained to detect nudity, shapes, colours, or faces of a set of people. The more often classifiers come across a certain pattern, the more accurate their assessment becomes.[91]

One particular challenge in the detection of new CSAM is that one needs to be able to reliably estimate the age of the person displayed in the content by analysing the content itself. This is known to be a very difficult problem, in particular for persons with an age close to the age of consent (as they might be wrongly classified as an adult or as a child).[92] One can expect very high error rates for CSAM content with victims in this age range.

One of the most frequently used tools is the machine learning component of Thorn's Safer tool.[93] This tool is made available to providers of information society services who can apply the tool to detect new material, based on machine learning. Thorn reports that if it sets the accuracy (sensitivity and specificity) of the tool to 99.9% (i.e., "only" 0.1% of the cases is a false positive), the tool is able to identify 80% of the total CSAM in the dataset (when testing the tool).[94] An independent expert

---

84 Ibid., p. 5; Struppek et al., 'Learning to break deep perceptual hashing: The use case neuralhash', 2022, p. 12.

85 Abelson et al. 'Bugs in our Pockets: The Risks of Client-Side Scanning', 2021, p. 28; Hao et al., 'It's Not What It Looks Like: Manipulating Perceptual Hashing based Applications', 2021, p. 1.

86 Weng, L and Preneel, B., 'Attacking some perceptual image hash algorithms', 2007, p. 880.

87 Jain et al., 'Adversarial Detection Avoidance Attacks: Evaluating the robustness of perceptual hashing-based client-side scanning', 2023, p. 2318.

88 Commission proposal on the temporary derogation of the e-Privacy Directive for the purpose of fighting online child sexual abuse, targeted substitute impact assessment, EPRS, February 2021, p. 15.

89 Expert input by academics.

90 Impact Assessment Report Accompanying the document Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, European Commission, May 2022, p. 280.

91 Ibid., p. 280.

92 Peersman et al., 'REPHRAIN: Towards a Framework for Evaluating CSAM Prevention and Detection Tools in the Context of End-to-end encryption Environments: a Case Study', 2023, p. 23.

93 How Safer's detection technology stops the spread of CSAM, Thorn, accessed 23 December 2022.

94 Benchmarking, Perception, accessed 27 March 2023.

assessment of these accuracy levels is difficult given the specific hash function (methodology) used in this benchmarking.

Similar to PhotoDNA, the accuracy claim of Thorn Safer tool has not been verified by independent experts.[95] Experts consulted for this study note that machine learning is growing increasingly accurate, but that human verification remains essential in order to contextualise and add nuance; something that machine learning is incapable of.[96]

Furthermore, the accuracy levels must be interpreted taking into account the amount of CSAM exchanged. With an accuracy rate of detecting 80% of all CSAM exchanged, it is likely that human verification is often required to determine whether detected images actually concern CSAM. Given the large numbers of messages and images exchanged daily, this would require ample resources. To illustrate, if the Safer Tool is applied to a messaging system in which one billion messages are sent per day, of which 10,000 are messages with CSAM, the tool would report one million false positives each day, with 8,000 true positives and 2,000 false negatives.[97] Sorting out the true positives from the false positives would require a huge manual effort.

Moreover, if the design of this tool would be made public[98], it would be easy to modify the content to evade detection by this tool while still having a similar visual perception for the user.[99] A non-transparent tool could, in theory, be put in place to mitigate this weakness (i.e. when a tool is kept secret, it is more complicated to evade detection). Such a tool could be verified independently, but experts would not be able to provide details underpinning their analysis (as the tool is secret). This means that the broader academic community would not be able to evaluate the quality and depth of the analysis and thus the security of the tool.[100]

Finally, experts raise concerns with regards to transparency, fairness and politicisation in light of the application of algorithms for content moderation.[101] Experts point to the challenges with regards to determining which body would design and maintain the algorithm, as well as the risk of discrimination against certain groups by the algorithm, among other things. Given the complexity of these machine learning algorithms, they are less transparent compared to the algorithms used in tools such as PhotoDNA (which is based on a less complex technology which is, therefore, more transparent). As a result, independent expert evaluation of the machine learning algorithms for content moderation is more complicated and cannot be done as thoroughly as an independent expert review of tools such as PhotoDNA.[102]

Detection of grooming

The detection of grooming requires the analysis of text-based communications. This is more complex than the identification of images. Grooming can be detected (with a certain degree of accuracy) by applying machine learning to conduct a risk assessment of texts and behaviour on messaging platforms.[103] Based on a series of assigned indicators, tools (in theory) can assess which

95 Expert input by academics and service providers.

96 Expert input by academics and EU independent body.

97 Expert input by academics.

98 Consulted experts note that it is likely that a tool, if deployed on a wide scale, would have to be made public.

99 i.e. images can be slightly tilted to avoid detection.

100 Expert input by academics.

101 Gorwa, R., Binns, R. and Katzenbach, C., 'Algorithmic content moderation: Technical and political challenges in the automation of platform governance', 2020, p. 10.

102 Expert input by academics.

103 How WhatsApp Helps Fight Child Exploitation, WhatsApp, accessed 23 December 2022.

texts can probably be assessed as grooming. The tools can flag such conversations, and thereby alert providers of information society services to conduct an additional (human) assessment.[104]

Tools developed to detect grooming include Project Artemis (by Microsoft, The Meet Group, Roblox, Kik, and Thorn).[105] Microsoft reported that the accuracy (sensitivity) of this tool is 88%.[106] An independent review of this accuracy level is not available. Moreover, expert views on the accuracy levels of tools that can detect grooming vary. Some note that for these technologies, it is difficult to achieve error rates significantly below 5 – 10%, depending on the nature of the material being searched for.[107] Such accuracy rates would amount to such high rates of false positives and false negatives that substantial resources are required to verify whether those alerts actually constitute CSAM.[108]

An additional problem is that it may be difficult to determine the age of the persons in the conversation. A study by the Commission Nationale de l'Informatique et des Libertés (CNIL) concludes that the current methods for age verification are "circumventable and intrusive".[109] It notes that less intrusive methods could be deployed based on attribute-based authentication, but this would require rolling out an EU-wide standard implemented both by service providers and by Member States. Even then, some of these solutions still allow to link official identity with private information, thereby impacting the privacy of users.

Furthermore, experts argue that the technologies to detect grooming are easily circumvented. They can be manipulated, data can be trained, labelled or batched, which would further impact the accuracy levels of the technology.[110] Additionally, experts highlight that text does not necessarily have to be captured in written text; they point to the usage of 'memes' that also serve to convey text while not being flagged as written content.[111] Also, as grooming is primarily text-based, it is essential for such technologies to be adapted to the local languages of the Member State[112] and to be free of bias.[113] Currently, the tools mentioned above are primarily available and tested in English.[114] Similarly, for the technologies deployed to detect grooming to be effective across the EU, they ought also to be sensitive to cultural differences (in communication).[115] In any case, detected potential instances of grooming would require a human check to verify whether the identified text actually concerns grooming, thereby increasing such tools' intrusiveness.[116]

---

104 Impact Assessment Report Accompanying the document Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, European Commission, May 2022, p. 282.

105 Ibid.

106 Ibid., p. 283. Micosoft recommended against using this figure in EU Policy discussions: Position Paper on the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, Microsoft, September 2022, p. 5.

107 Vu et al., 'ExtremeBB: Enabling Large-Scale Research into Extremism, the Manosphere and Their Correlation by Online Forum Data', 2021, p. 4; Abelson et al. 'Bugs in our Pockets: The Risks of Client-Side Scanning', 2021, p. 4.

108 Abelson et al. 'Bugs in our Pockets: The Risks of Client-Side Scanning', 2021, p. 5

109 Online age verification: balancing privacy and the protection of minors, CNIL, accessed 20 April 2023.

110 Ibid, Shumailov et al., 'Manipulating SGD with Data Ordering Attacks', 2021, p. 5.

111 Expert input by service provider.

112 Expert input by service provider, academic and NGO.

113 Bias in Algorithms – Artificial Intelligence and Discrimination, European Agency for Fundamental Rights, 2022, p. 11.

114 Expert input by service provider, academic and NGO.

115 Report presented at expert workshop on EU's proposed regulation on preventing and combatting child sexual abuse, Leiden University, February 2023, p. 31.

116 Commission proposal on the temporary derogation of the e-Privacy Directive for the purpose of fighting online child sexual abuse, targeted substitute impact assessment, EPRS, February 2021, p. 16.

Finally, it should be noted that, contrary to the Interim Regulation, the CSA proposal does not exclude audio communications from its scope. In the light of CSAM, audio communications can be primarily regarded as a form of grooming. Currently, this type of communications cannot be monitored by providers of information society services to detect CSAM. However, the CSA proposal does not explicitly refer to detecting, removing and blocking audio communications. The CSA proposal fails to specify how this type of communication would be monitored and how CSAM would, in the future, be detected in spoken messages.[117] Therefore, this type of content is disregarded in this analysis.

Key challenges in detection of CSAM

The detection of CSAM in online communications is faced by two key challenges, namely (a) the shift to E2EE communication and (b) the risk of spill-over effects to other domains.

End-to-end-encryption of communications

Data encryption is a way to scramble data (files and information) when they are shared with others. As a result of this, the original data becomes unreadable to those who do not have the key to decrypt the information.[118] In some systems, data encryption is only provided for on the links between a user device and the server of a service provider.[119] In this case, the information is fully accessible to the service provider. Moreover, in the case of a security breach or hack of the server, all user data would be exposed. Because of this risk, there is an increased deployment of encryption in E2EE communication: now content is encrypted before it is sent and only decrypted by the intended recipient. With this, the service provider facilitating the communication cannot access the exchanges.[120]

Encryption can safeguard stored data (i.e., encrypting a stored space) or data 'in motion' (often through E2EE). Encryption has become widespread to safeguard privacy, confidentiality of communications, and personal data. Encrypted messaging allows users (such as journalists, dissidents, and vulnerable groups) to communicate privately. Hence, encrypted communication can be understood as a pivotal element of digital security.[121]

Nevertheless, encryption hampers the detection of CSAM by allowing perpetrators to hide themselves, the content they exchange, and their stored content from law enforcement agencies (LEA).[122] This impacts the ability of LEA to detect and prosecute those who possess and exchange CSAM because they simply cannot access the E2EE communications easily.[123] A substantial share of the online communications is currently already E2EE. In addition, some key providers of information society services are also moving towards E2EE (i.e., Facebook Messenger and Instagram personal messages and calls are foreseen to be E2EE by the end of 2023).[124] This is likely to further impact the ability of LEA to detect CSAM.

---

117 Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, The EDPB and the EDPS, July 2021, p. 26.

118 What is Encryption?, Microsoft, accessed 23 December 2022.

119 This is for example the case for all mobile data sent over the basic 3G/4G/5G data services: only the wireless part of the link is encrypted between mobile phone and the base station controller.

120 Use end-to-end encryption for one-to-one Microsoft Teams calls, Microsoft, accessed 23 December 2022.

121 Impact Assessment Report Accompanying the document Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, European Commission, May 2022, p. 284.

122 Turning The Tide Against Online Child Sexual Abuse, The Police Foundation, July 2022, p. 39.

123 Thank you very much, your mail is perfectly fine", Verfassungsblog, accessed 9 March 2023.

124 Testing End-to-End Encrypted Backups and More on Messenger, Messenger News, accessed 26 March 2023.

In summary, encryption (particularly E2EE) precludes the methods that some providers of information society services currently use to detect CSAM. Simultaneously, encryption also plays an essential role in ensuring privacy and confidentiality of communications and personal data. Therefore, striking the balance between privacy and data protection of users and enabling detection of CSAM is a delicate task. As part of this process, the technological capabilities to detect CSAM play a critical role; the detection must be technically feasible. This element will be explored further in the following section.

Spill-over effects to other domains

One of the main risks foreseen by experts includes the risk of application of the CSA proposal to adjacent domains (such as the fight against terrorism or political opponents).[125] If monitoring and detection is allowed within the framework of CSAM, there might be a chance that similar activities will, in the future, also be allowed in the fight against other issues (i.e. function creep).[126] As described above, it is not complex to amend the parameters of a moderations system to include new material.[127] The application of the CSA proposal to adjacent domains can, in the future, occur in a legitimate way (when legislation is amended to include other types of threats as well, for instance) but it can also illegally take place, when actors amend the moderation systems without a legal basis. Hence, the function creep also relates to the potential to abuse the legal framework and technologies required to detect content.[128] As pointed out above, several technical mechanisms require secrecy and work based on fingerprinted data, which impedes oversight and transparency, and facilitates the stealthy modification and/or the abuse of these mechanisms.

Similarly, experts warn against the spill-over effect of the CSA proposal to other jurisdictions with lower human rights standards and which might use the legal framework and technologies to detect CSAM and other types of content (as described in the previous paragraph).[129] Experts argue that, while the EU seeks to be at the forefront of the fight against CSAM, it ought to be wary of the potential and way in which other jurisdictions might copy the CSA legislation. A similar observation can be made in the light of non-state actors who might be interested in the technologies that would be deployed to detect CSAM.[130]

3.1.2. Current state of play in reporting CSAM

While the previous section has outlined the current state of play regarding the detection of known material, new material and grooming, the section at hand focuses on the current state of play in reporting of CSAM by providers of information society services, users, and LEA.

By information society services

At the moment, the Interim Regulation allows certain online communication services, such as instant messaging and email, to detect and report CSAM voluntarily, on the premise that their

---

125 Koops, B., 'The concept of function creep', 2021, p. 35; Three new committees on Pegasus spyware, foreign interference and COVID-19, press release, European Parliament, 10 March 2022.

126 Abelson et al. 'Bugs in our Pockets: The Risks of Client-Side Scanning', 2021, p. 3 and 20; A practical example can be observed in the UK where the changes to the Online Safety Bill were tabled to also cover the identification of terrorist content and specific migration-related content, see: Donelan confirms stiffer online safety measures after backbench pressure, The Guardian, accessed 9 March, 2023; Koops, B., 'The concept of function creep', 2021, p. 35; Peersman et al., 'REPHRAIN: Towards a Framework for Evaluating CSAM Prevention and Detection Tools in the Context of End-to-end encryption Environments: a Case Study', 2023, p. 2.

127 Bartusek et al., 'End-to-End Secure Messaging with Traceability Only for Illegal Content', 2022, p. 9.

128 Koops, B., 'The concept of function creep', 2021, p. 35.

129 Expert input by academics and NGO.

130 Abelson et al. 'Bugs in our Pockets: The Risks of Client-Side Scanning', 2021, p. 13.

activities are lawful and, in particular, meet a set of specific conditions for the voluntary detection of CSAM by providers of information society services (see below for more details).[131] The process of detecting and reporting CSAM material by providers of information society services in the EU consists of several steps. These steps are outlined in this section, primarily based on the description included in the CSA proposal IA.[132]

First, when providers of information society services in the EU detect (potential) CSAM, they report this to the respective national authorities and/or NCMEC.[133] The majority of the detected CSAM within the EU is reported with NCMEC. NCMEC then determines the location from where materials were uploaded. When uploads relate to an EU Member State, the report is handed over to the US Department of Homeland Security Investigations (HSI) which, in turn, can hand over the report directly to the respective Member State LEA or to Europol. Currently, the ability for Europol to receive reports directly from providers of information society services or NCMEC is restricted.[134] Hence, the HSI is intermediate in transferring relevant reports from NCMEC to Europol. Europol receives reports that are checked and forwarded to the respective Member State authorities (often LEA). The LEA then have the mandate to act upon the received reports. The CSA proposal foresees that the EU Centre would create a database of reports and it would also grant Europol access to this database, thereby reducing the reliance on NCMEC and HSI.[135]

By users

A second avenue for detecting and reporting CSAM is through users who accidentally come across such content. Many EU Member States have a national hotline, part of the INHOPE network.[136] These hotlines, in turn, forward the reports to LEA and liaise with the respective service provider to have the content removed. Important to note is that neither victims nor hotlines can search for CSAM proactively. In addition, the INHOPE hotlines support the removal of CSAM hosted outside the territory of the country where the material has been reported. They do so by facilitating the identification of the country where material is hosted, then share the information with the hotline in the respective country to allow the latter to contact the public authorities. When no hotline exists in the country identified as hosting the material, the INHOPE hotline may contact the provider directly.

By law enforcement agencies

In addition, LEA may search for content based on metadata. While this data type is less likely to identify individuals, it can help LEA identify networks of users exchanging CSAM.[137] Identifying groups might, in turn, enable LEA to identify individual users of such group.

---

131 The overviews by NCMEC provide a clear overview on the number of providers reporting to them annually, see: 2021 CyberTipline Reports by Electronic Service Providers (ESP), National Center for Missing & Exploited Children, 2022.

132 Impact Assessment Report Accompanying the document Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, European Commission, May 2022, p. 21

133 The National Center for Missing & Exploited Children is a US, private, non-profit organisation.

134 Expert input by service providers.

135 Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, COM (2022) 209 final, European Commission, May 2022, Article 46.

136 INHOPE is a global network of national hotlines that facilitate the reporting of CSAM by users.

137 Expert input by academics and law enforcement.

3.1.3. Detection of CSAM in E2EE

The previous sections have presented the current state of play regarding the detection and reporting of CSAM. As pointed out above, one of the key challenges in detecting CSAM is that interpersonal communications are increasingly taking place on E2EE channels. As noted, detecting CSAM on E2EE channels would require additional technology to 'intercept' communications at some point during the encryption process. Therefore, this section explores the potential avenues for detecting CSAM in E2EE channels.

One potential avenue to detect CSAM in E2EE communications is through the use of metadata: this includes mobile telephone number, IMEI address[138], IP address, MAC address[139], location of device, device model, or operating system. Based on this data, one can identify communication patterns, social networks and physical networks of users starting from one person in the network. This method is currently applied by LEA but they usually find it to provide insufficient basis to initiate an investigation, due to the lack of information on the level of individual users.[140] It should be pointed out that there are no independent studies on the effectiveness or limitations of the current uses of metadata by LEA to detect CSAM. This lack of usability of metadata is one of the reasons for the European Commission to extend the legal basis for the detection of CSAM to include the actual content of communications as well.[141] Therefore, this study focuses on possible solutions that could potentially have a better usability in detecting CSAM. The use of metadata to detect CSAM in E2EE is not further considered in this study. Nevertheless, further intensifying the application of metadata in the detection of CSAM could be an interesting avenue that would welcome further research.[142]

As part of the CSA proposal IA, the European Commission invited technical experts to reflect on nine technological solutions that could potentially be applied to detect known and new material in an E2EE environment.[143] Annex III provides an elaborate description of this assessment. Ultimately, the technical experts consulted by the European Commission identified three solutions which can be understood to be most feasible in detecting CSAM in E2EE. These are the following and will be further explored below:

(4) On-device full hashing (with matching at server);

(5) On-device partial hashing (with matching at server);

(6) Secure enclaves in Electronic Service Provider (ESP) server.

It should be noted that even if these solutions could be feasible, the experts consulted by the European Commission as well as those consulted as part of this study did not identify them as ready for deployment.

Potential solution 1: On-device full hashing (with matching at server)

As the hashing in E2EE communications cannot occur on the server after the communication has been encrypted, this solution converts the content into hashes before it is encrypted. After the hashes have been created the device sends both the hashes and the encrypted message to the server. The server then compares whether the sent hashes match with the hashes in the database.

---

138 A unique number for identifying a device on a mobile network.

139 A unique identifier assigned to a network interface controller.

140 Global Threat Assessment, WeProtect Global Alliance, 2021, p. 34.

141 Impact Assessment Report Accompanying the document Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, European Commission, May 2022, p. 28.

142 Based on the limited scope of this study, no further conclusions with regards to the use of metadata in detecting CSAM can be drawn.

143 Ibid., pp. 284 – 314.

This solution would require installing an application on the device of the user to facilitate the matching at the server.

The experts consulted by the European Commission consider this solution promising, as it allows for the detection of known CSAM. To the knowledge of the researchers, this potential solution has not been successfully applied on a wide scale in practice to detect CSAM.

However, academia and experts consulted for this study note several concerns regarding the application of client-side scanning technologies. Some concerns are similar to those raised in light of monitoring on non-E2EE communications, namely that providers of information society services can access all hashes, leading to privacy and security concerns.[144] Furthermore, there is an absence of consistent monitoring of an enforcement agency, which affects the transparency of the technology.[145]

Other concerns raised are specific to the monitoring of E2EE communications. First, client-side scanning substantially impacts the boundaries between a user's private and shared (semi-)public spheres.[146] Through the application of this technological solution, content that was formerly private to a user can become accessible to LEA and intelligence services, without the need of a warrant.

Second, client-side scanning poses substantial vulnerabilities to attacks and abuse.[147] By extending the technology from server-side scanning to client-side scanning, new vulnerabilities for on-device attacks are created.[148] Despite constant patching, such vulnerabilities likely continue to exist.[149] Attacks can be launched from a variety of points, including from governments, non-state actors and local adversaries.[150] Such vulnerabilities weaken the information infrastructure as a whole. Furthermore, client-side scanning poses a risk for abuse.[151] While scanning applications would, in the case of the detection of CSAM, be programmed to detect only CSAM on a number of applications installed on the device (i.e. only WhatsApp or Facebook Messenger communication), there is a risk that these parameters are changed to monitor other applications on the device as well.[152]

Furthermore, experts in various publications have flagged practical issues that will likely surface when the client-side scanning is to be deployed in real life. These mainly concern which body would be trusted to write the code for the client-side scanning applications[153], how the maintenance and updating of such codes would be organised[154] and where devices would report targeted content.[155]

---

144 Ibid., p. 289.; Towards a principled level playing field for an open and secure online environment, Centre for European Policy Studies, October 2022, p. 46.

145 Ibid.

146 Abelson et al. 'Bugs in our Pockets: The Risks of Client-Side Scanning', 2021, p. 11.

147 Jain et al., 'Adversarial Detection Avoidance Attacks: Evaluating the robustness of perceptual hashing-based client-side scanning', 2023, p. 2318; Hao et al., 'It's Not What It Looks Like: Manipulating Perceptual Hashing based Applications', 2021, 81.

148 Abelson et al. 'Bugs in our Pockets: The Risks of Client-Side Scanning', 2021, p. 12; Expert input by academics.

149 Prokos et al., 'Squint hard enough: Evaluating perceptual hashing with machine learning', 2021, p. 19.

150 Levy, I. and Robinson, C., 'Thoughts on Child Safety on Commodity Platforms', 2022, p. 35.

151 Abelson et al. 'Bugs in our Pockets: The Risks of Client-Side Scanning', 2021, p. 22; Expert input by academics.

152 Abelson et al., Bugs in our Pockets: The Risks of Client-Side Scanning, 2021, p. 22; Client-Side Scanning And Winnie-The-Pooh Redux (Plus Some Thoughts On Zoom), The Center for Internet and Society, accessed 9 March 2023.

153 Ibid., p. 25; Bartusek et al., 'End-to-End Secure Messaging with Traceability Only for Illegal Content', 2022, p. 7.

154 Abelson et al. 'Bugs in our Pockets: The Risks of Client-Side Scanning', 2021, p. 25.

155 Ibid., p. 26.

Also, it would be difficult to restrict any measures regarding encryption to users of services only in the EU.[156] These more practical issues mainly revolve around trust, accountability and transparency.

Moreover, experts warn that technology develops rapidly. While this means that solutions to detect CSAM are improving, it also means that perpetrators are becoming better at circumventing the solutions. The deployment of solutions such as the one at hand risk contributing to a 'technology arms race' whereby solutions and workarounds are chasing one another.[157] One of the key challenges is developing a sufficiently robust perceptual hash technology even if it were to be decided, for transparency purposes, to make its technical description available to the public. After two decades of work on this technology, this has not been achieved and it is unlikely that this will be the case soon.[158]

Finally, experts pointed to practical implications such as the need for solutions to be deployed in a high connectivity environment.[159] In practice, this means that the solutions would be less effective when deployed with older devices. Recently some technical improvements have been proposed that strengthen the solutions[160] : users are now only reported after multiple matches, and one can certify that external groups have approved the set of hash values. However, none of these improvements overcome the key challenges mentioned above.

Potential solution 2: On-device partial hashing (with matching at server-level)

This solution concerns an advancement of the previous tool and would be able to detect known material. The difference is that in this solution the (perceptual) hashing is performed in two stages: a first step happens on the user device. For this part the design of the hash function is likely to become public,[161] allowing for users to verify the computation, thereby positively impacting the transparency of this solution. A second step happens in the server, where the partial hash is hashed again with a second function and the result is matched against a database with known CSAM content. The advantage of this approach is that the second part of the hashing operation is performed on the servers and can thus be kept secret. There is increased transparency as the user can verify the computation of the partial hash that leaves the device unencrypted. Additional protection is needed to ensure the partial hash matches the encrypted content.

Experts contributing to the CSA proposal IA and those consulted for this study are cautious regarding the feasibility of this tool because it is much newer than the on-device full hashing.[162] They argue that the tool is still in development and that the accuracy levels for this technology are not high and, therefore cannot be applied in practice.[163] In addition, all concerns raised regarding the above presented solution (on-device full hashing) are also valid for this solution. For example, if tools would become available to break the first partial hash, they could be used to evade detection or to frame someone with a false positive.

---

156 Private and secure communications attacked by European Commission's latest proposal, European Digital Rights, accessed 3 March 2023.

157 Expert input by academic.

158 Ibid.

159 Ibid.

160 Bhowmick et al., 'The Apple PSI System', Apple Technical Report, July 2021; Scheffler, S., Kulshrestha, A. and Mayer, J., 'Public Verification for Private Hash Matching', 2023.

161 I.e., through reverse engineering (if it the function not made public from the start.

162 Expert input by academics.

163 Ibid.

Potential solution 3: Secure enclaves in Electronic Service Provider server

This solution consists of 'secure enclave' on the Electronic Service Provider (ESP) server that decrypts E2EE communication. In this case, content would be encrypted and sent to a server to decrypt in a secure setting. Once communication has been decrypted, it is possible to carry out all operations in communications that are not E2EE. Providers can monitor content in the secure enclave, encrypt it, and send it onward when deemed safe.[164] To date, no companies have implemented this solution to detect CSAM.

The experts consulted by the European Commission for their IA view this solution as promising, as it can detect both known and new material. However, at the current stage there are substantial concerns with respect to the feasibility of this solution as the hardware and software required for this solution is operationally complex. As a result, only few companies can currently implement this solution (for purposes other than the detection of CSAM). The implementation of this solution by smaller providers is likely to be cumbersome or even unrealistic.[165]

Concerning privacy, security, and transparency, the concerns are similar to the ones about the on-device hashing solutions. In addition, an expert consulted for this study noted that while this method is more difficult to bypass, the service offered is not E2EE but a somewhat more secure version than point-to-point encryption. Providers of information society services may put modified secure enclaves (which are impossible to detect for the clients, particularly if they get help from a device manufacturer or a government agency). They can then fully access the exchanged communication after it is decrypted. Addressing (i.e., solving) such weaknesses in the solution, subsequently, may take months. In addition, providers can also use the technology for other purposes than detecting and reporting CSAM and, equally, it cannot be ruled out that they will provide access to other entities.[166]

Future developments regarding the detection of CSAM in E2EE communications

The above sections have outlined the current state of play of detection and reporting and the possibilities currently to detect CSAM in E2EE. Providers of information society services consulted for this study shared that, despite (joint) efforts in combatting CSA in E2EE communications (see for example the Project Protect by amongst others Microsoft, Facebook, Google and Apple)[167] they deem it unlikely that the above-presented technologies will rapidly develop in the next two to five years, without undermining the secure nature of E2EE communications.[168]

They make a similar observation regarding the developments of technologies that could potentially identify new material or grooming (in open communication channels and / or E2EE communications).[169] While such technologies are developing rapidly, achieving accuracy rates (and minimal error rates) similar to those of the technologies to detect known CSAM is a vast challenge that is not expected to be overcome soon.[170]

---

164 Impact Assessment Report Accompanying the document Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, European Commission, May 2022, p. 289.

165 Expert input by service providers and academics.

166 Expert input by academics and NGO.

167 Working together to end online child sexual exploitation and abuse, TechCoalition, accessed 28 March 2023.

168 Expert input by academics and service providers.

169 Ibid.

170 Ibid.

The EU Centre that the CSA proposal foresees to establish could, potentially, play a role in advancing such technological developments. Nevertheless, to add value to the existing research and development activities undertaken, sufficient funding would be required for the technology-related activities of the EU Centre.[171]

The providers of information society services consulted believe solutions based on non-E2EE technology have a bigger potential for innovation. Examples of such solutions include the analysis of behaviour, network signals, and other available data.[172] Moreover, most consulted experts stressed that the best solution would be to empower users (both children and adults) of online communication services in reporting potential CSAM when they come across it.[173] Communication services would benefit from intensifying the application of 'safety by design'[174], providing users of communication services with more opportunities to act when needed.[175] Despite its limitations, subsequent LEA investigations could rely on metadata to link one or more reports to a network.

3.2. Impact on quantity and quality of detected and reported content

In this section, the expected impact on the quantity (i.e., the amount of detected CSAM) as well as on the quality of the detection (i.e., the accuracy levels) will be described. This section builds upon the analysis above, where it was concluded that the detection of known material can occur at relatively high accuracy levels. The detection of new material and grooming cannot be deemed accurate at this point, although the detection of new material is growing increasingly accurate. For the reasons outlined above, whether known material, new material or grooming is detected in non-E2EE communications or in E2EE is less relevant in the section at hand.

3.2.1. Expected impact on quantity

The impact of the CSA proposal on the amount of reported CSAM is highly relevant as it impacts the workload of LEA directly. Reported CSAM ought to be investigated by national LEA and as this task would require substantial (additional) capacity.[176] The available literature is limited on the topic of the expected impact on the quantity of reported CSAM. Hence, this analysis primarily relies on stakeholder expert opinions. The views of the consulted experts differ: some expect the quantity of reported CSAM to remain the same or decrease. In contrast, others anticipate that the reported CSAM would sharply increase.

Experts who expect the amount of reported content to decrease, point to several larger providers of information society services who, at this moment, are actively reporting CSAM voluntarily. As the CSA proposal would not provide a legal basis for voluntary monitoring, these providers of information society services would be restricted in their ability to detect and report because they would not have the legal basis to continue their voluntary efforts (which are more advanced than the obligations laid down in the CSA proposal). In addition, the detection would have to be done

---

171 Expert input by academics, service providers and NGO.

172 Ibid.

173 Ibid.

174 Safety by Design Principles and Background, eSafety Commissioner of the Australian government, accessed 6 February 2022.

175 Research for CULT Committee – The influence of social media on the development of children and young people, Policy Department for Structural and Cohesion Policies, European Parliament, February 2023, p. 8.

176 Europese Verordening ter voorkoming en bestrijding van seksueel kindermisbruik, Tweede Kamer, accessed 9 March 2023.

based on the EU centre's set of EU classifiers. These experts argue that both developments would lead some larger providers of information society services to be able to detect and report less than they currently do, thereby countering the CSA proposal's intended effect.

In addition, some experts note that the CSA proposal would disincentivise perpetrators to exchange CSAM in the first place, thereby leading to a drop of reported content.[177] These experts highlight that detection orders should be regarded as the 'last resort' and that the CSA proposal prioritises preventive measures over compulsory reporting. As a result, these experts expect a part of the group of perpetrators to stop sharing and consuming CSAM and, therefore, the amount of exchanged CSAM will drop and so will the reports.

Other experts argue that the reported CSAM will likely increase substantially after the CSA proposal enters into force.[178] However, they reference the fact that much known CSAM is often reported repeatedly.[179] Once the CSA proposal enters into force, the content can be taken down more swiftly, these experts argue. This would, after a while, result in fewer incoming reports because the known material being reported repeatedly will have been taken down and only new material will be reported.[180]

Finally, a group of consulted experts warns that the CSA proposal will result in a significant increase of reports as providers of information society services who had not been (or only very limited) reporting CSAM before are now required to do so. According to those experts, this would naturally result in a sharp increase, simply because a larger set of providers will report.[181]

Some consulted experts note that providers of information society services might even start overreporting content (i.e., reporting content which might constitute CSAM) to avoid liability for not sharing. These experts argue that providers of information society services might be keen on receiving detection orders because this would provide them with legal certainty for deploying technologies to detect CSAM (see also Chapter 4).[182]

Notwithstanding the experts' expectation on the impact of the CSA proposal on the quantity of the reported content, it can be concluded that the obligation to detect new material and grooming will likely result in more false positive reports (see also above).[183] The technologies that allow new material detection and grooming are not accurate enough to avoid false positives. Therefore, it is realistic to assume that the reported CSAM will increase sharply because less accurate tools will have to be deployed to detect new material and grooming.

Another factor likely to impact the quantity of detected content is the expectation that some perpetrators might shift their activities towards the dark web (see Section 3.3). Detection of CSAM on the dark web is more complex and a shift to such platforms would likely lead to decreased

177 Expert input by NGO.

178 Why an increase in reports of CSAM is actually a good thing, Thorn, accessed 9 March 2023.

179 Impact Assessment Report Accompanying the document Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, European Commission, May 2022, p. 265.

180 Expert input by NGO.

181 Expert input by academics and law enforcement.

182 Expert input by NGO.

183 Vu et al., 'ExtremeBB: Enabling Large-Scale Research into Extremism, the Manosphere and Their Correlation by Online Forum Data', 2021, p. 5; Anderson, R., 'Chat Control or Child Protection?', 2022, p. 4.

reported CSAM content. While detecting CSAM on the dark web is possible, identifying individual users is more cumbersome.[184]

Importantly, the quantity of reports does not equal the quantity of investigations and/or prosecutions. Therefore, it is incorrect to assume a direct causal relation between increased reporting and reduced harm for children. To translate an increase in reported CSAM into an increase in investigations and prosecutions, this requires sufficient capacity at LEAs. When capacity at LEAs is lacking, the reported CSAM can increase, but it would not necessarily translate to more perpetrators being identified and halted. Some experts note that an increased quantity of reported CSAM would give authorities a better picture of the size and scope of the issue. Simultaneously, it would (with the current capacity at LEA) become more difficult to effectively investigate reported CSAM.[185]

However, some consulted experts shed a different light on the expected increased workload of LEA when the CSA proposal would enter into force. These experts underline that LEAs depend on reports of CSAM by providers of information society services, as the latter have access to information that LEAs do not necessarily have. To detect and investigate CSAM effectively, LEA would need to collaborate closely with providers of information society services. These experts note that the way LEA currently investigate cases of CSA(M) does not allow them to keep up with the large amounts of reports issued to them. More data-driven investigations and AI-based prioritisation of reports and cases could be a solution to increase investigation capacity at LEAs. Such systems would need to be trained by large sets of data. In this regard, experts argue that an increased number of reports (as likely to result from the entry into force of the CSA proposal) would benefit the development of such LEA solutions. Nevertheless, these experts note that ample resources, will, and priority are required to develop and fund such LEA systems.[186] Moreover, these kinds of tools present an elevated risk of abuse for discrimination and predictive policing.[187]

The EU Centre is foreseen to play a role in filtering reports received by providers, in an effort to alleviate the burden on LEA. It is questionable whether such a filtering exercise is feasible, given the number of messages exchanged each day. To illustrate, if 0.1%[188] of all messages would be falsely flagged as CSAM (i.e., a false positive) and this percentage is applied to one billion messages exchanged each day, it results in 1 million false positives per day. It takes one person approximately 10 seconds to classify whether reported content is indeed CSAM or whether it is a false positive. This means that one person could classify about 2500 messages per day. Per 1 billion messages, this would require 400 people on a permanent basis to classify those images. Taking into account training, holidays and weekends, it is more likely that a team of 800 people would be required to classify those images. This workload is deemed not feasible, regardless of whether it is the responsibility of the EU Centre or LEA.

184 Expert input by academics.

185 Expert input by law enforcement, academics, NGOs.

186 Ibid.

187 Expert input by academics, NGOs.

188 Expert input by academic. This is an optimistic estimate for the false positive rate for the detection of new CSAM and grooming – in practice the false positive rate may well be higher.

3.2.2. Expected impact on quality

An assessment of the impact of the CSA proposal on the expected quality of the detection of CSAM is relevant as this has a direct impact on the burden of LEA, which are tasked with the investigation of reported content. Essential in the assessment of the expected quality of detection is the accuracy threshold that will be applied for the technologies implemented to detect CSAM. If a higher evidence threshold is adopted by the developers of technologies to detect CSAM, a higher percentage of detected content also truly constitutes CSAM.[189] Simultaneously, when lowering the accuracy threshold, these effects would be reversed. Hence, the impact on the quality of the detection is heavily impacted by the accuracy thresholds of the technologies applied. As described in the sections above, the accuracy levels of the technologies used to detect new material[190] and grooming[191] are low (compared to accuracy levels of technology used to detect known material).[192]

Hence, when also requiring providers of information society services to detect new material and grooming, the number of false positives and false negatives would be high. While the EU Centre that the CSA proposal foresees to establish could potentially play a role in advancing technologies to enhance their accuracy levels, it is not likely that the EU Centre will substantially contribute to increasing the accuracy of these technologies, as decades of research and development efforts by the tech industry have not resulted in high accuracy levels for technologies to detect new CSAM and grooming yet.[193]

Expert views on the impact of the CSA proposal on the quality of detection vary. Some expect the quality to increase because the CSA proposal would create a common standard across the Union.[194] This would improve the quality because it addresses discrepancies in the detection of known material between EU Member States (and the US). Children across the EU will, as a result of the CSA proposal, enjoy the same level of protection, regardless of their location.[195]

Other experts argue that the quality of detection will decrease as the detection of new material and grooming would require the application of technologies that have low accuracy rates and would therefore result in large amounts of false positives and false negatives.[196] They argue that the amount of identified potential CSAM will increase but that this does not necessarily mean that the amount of detected CSAM would increase, too.

Finally, some experts note that while the accuracy of detecting new material and grooming would indeed be lower than the accuracy levels for the detection of known material, it would still be worthwhile to aim also towards detecting new material and grooming because such content is likely

---

189 Impact Assessment Report Accompanying the document Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, European Commission, May 2022, p. 79.

190 Thorn reports that if it sets the accuracy (sensitivity and specificity) of the tool on 99.9% (i.e., "only" 0.1% of the cases is a false positive), the tool is able to identify 80% of the total CSAM in the dataset.

191 Microsoft reported that the accuracy (sensitivity) of this tool is 88%.

192 Farid, H. 'Fostering a Healthier Internet to Protect Consumers', accessed 1 March 2023, p. 2.

193 Expert input by academic.

194 Impact Assessment Report Accompanying the document Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, European Commission, May 2022, p. 33.

195 Expert input by European Commission and NGO.

196 Internal documents revealed the worst for private communications in the EU; how will the Commissioners respond?, European Digital Rights, accessed 9 March 2023.

produced more recently, which means that chances of protecting a child from (further) harm are higher (in comparison to known material).[197]

3.3. Impact on behaviour

The analysis of the expected impact of the CSA proposal on behaviour can be divided into three components, namely in relation to providers of information society services, children, and adult users. As evidence to support the assessment is relatively limited, much of the analysis is based on inputs from consulted experts. In addition, evidence persistent to adjacent domains has been applied to the extent possible to the domain of the fight against CSAM. [198]

3.3.1. Behavioural effects for providers of information society services

The identified potential behavioural effects on providers of information society services cover a number of different aspects. These include their incentive to do business in the EU, their incentive to innovate, and legal safeguards.

First of all, the CSA proposal would create additional responsibilities, workload, and legislation for the providers of information society services to adhere to (i.e., the development of risk assessment reports).

Secondly, the CSA proposal is expected to have an impact on the incentive of providers of information society services (and industry players) to innovate. On the one hand, the incentive to accelerate innovation in the domain of technologies that can accurately detect CSAM in E2EE communications would increase. The analysis shows that currently, in particularly with regards to the detection of new material and grooming, technologies are substantially less accurate than the technologies that detect known CSAM. This gap provides a direct area for research and development of industry players, contributing to the development of technologies that would be able to detect new material and grooming accurately.[199] Consulted experts note that it is unlikely that such technologies would reach high accuracy levels in the near future. In addition, it is unclear to what extent providers of information society services are interested to invest in this domain.[200]

In addition, it is also argued that the CSA proposal would impact E2EE communications to such an extent that it might be less interesting for providers of information society services to invest, research and develop this type of communications. The CSA proposal would require the deployment of technologies that can monitor E2EE communications to a certain extent. Such technologies are inherently in conflict with what E2EE communications stand for, namely private communication. Hence, with providers of information society services being obliged to allow for the partial monitoring of E2EE communications, their incentive to invest and develop E2EE communication could stagnate as the essence of this type of communication is touched by the CSA proposal (and potentially future, adjacent legislation).[201]

With regards to providers of software application stores, particular challenges arise. The CSA proposal lays down that providers of software application stores are held accountable for the

---

197 Expert input by European Commission and NGO.

198 See for instance: Frosio, G,. 'Reforming intermediary liability in the platform economy: A European digital single market strategy', 2017 and Buiten, M. et al., 'Rethinking Liability for online hosting platforms', 2019.

199 Expert input by academics, service providers and NGO.

200 Ibid.

201 Expert input by academics and service providers.

services that the developers of applications provide on their platform.[202] However, the providers of software application stores are not involved in the risk assessment procedures for the applications that are offered on their services. This puts app store providers in a difficult position where they have to vouch for an app developer without knowing exactly how the app developer assessed its risks. A similar observation can be made with regards to providers of hosting services. In its draft opinion, the European Parliament Internal Market and Consumer Protection committee has also requested for providers of software application stores to be removed from Article 6 of the CSA proposal.[203]

Finally, providers of information society services would need sufficient legal certainty to implement the CSA proposal. At this point in time, this legal certainty is not sufficiently provided for as some elements of the CSA proposal lack clear wording and specification (see Chapter 5). Hence, it can be expected that providers of information society services alter their behaviour in order to avoid liability when monitoring CSAM. In this regard, two avenues for behavioural adaptations were mentioned by experts. Providers of information society services could start to overreport potential CSAM in order to avoid false negatives.[204] Similarly, providers of information society services might be keen to be more pessimistic in their risk assessments in order to receive a detection order because such order would provide them with sufficient legal coverage.[205] It is difficult to assess the likelihood of these avenues as such behaviour would also directly impact the 'customers' of the providers of information society services.

3.3.2. Behavioural effects for children

The expected impact of the introduction of the CSA proposal on children varies across experts consulted. Generally, experts representing the children's protection perspective expect the CSA proposal to benefit children who are making use of online communication services. These benefits have also been elaborately in the CSA proposal IA and include, amongst others, more rapid identification and take-down of images, the reduction of a risk to re-victimisation and better protection against grooming.[206]

Other stakeholders, such as privacy and data protection experts, expect some negative impacts of the CSA proposal on this group. Both arguments are presented below.

The CSA proposal, some stakeholders argue, requires providers of information society services to apply security by design.[207] This entails that products are designed in such a way that they incorporate service provider responsibility, user empowerment, autonomy, transparency, and accountability. Through this requirement, communication services would become safer and more secure for children by default, positively impacting their behaviour and sense of freedom online.[208]

---

202 Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, European Commission, May 2022, Article 6, 2022.

203 Draft opinion on the proposal for a regulation laying down rules to prevent and combat child sexual abuse, IMCO committee, European Parliament, 8 February 2023, p. 51.

204 Urban et al., 'Takedown in Two Worlds: an empirical analysis', 2017, p. 516. And 516.; Urban et al., 'Notice and Takedown: Online Service Providers and Rightsholders Accounts of Everyday Practice', 2017, p. 390.

205 Expert input by academics and NGO.

206 Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, European Commission, May 2022, Article 6, 2022, p. 89.

207 Safety by Design Principles and Background, eSafety Commissioner of the Australian government, accessed 6 February 2022.

208 Expert input by European Commission and NGO.

Furthermore, some stakeholders argue that the fact that the CSA proposal would make it easier for coordinating authorities and providers of information society services to take down CSAM, which would benefit the sense of safety of children using online services.[209] When children know they can safely make use of these services, with a limited risk of encountering illegal content that might upset them, they would be able to enjoy those services more freely and confidently. This also applies to the notion that the CSA proposal would, in the view of these stakeholders, reduce the number of perpetrators online, thereby increasing the safety of children.

Nevertheless, other stakeholders are concerned about the impact of the potential for monitoring on the behaviour of children. They highlight that teenage minors who are consensually sharing sexual content might be impacted when they know that this content could be monitored by providers of information society services, as it could potentially be labelled as CSAM.[210] This scenario is particularly evident when providers of information society services are also required to monitor for new material as this would be primarily done through the application of AI, which might not be able to contextualise the images it detects.[211] From the perspective of these stakeholders, the CSA proposal would impact the ability of teenage minors to express themselves sexually online. Some more vulnerable groups, such as queer children, might be impacted substantially, these experts argue.[212]

3.3.3. Behavioural effects for adult users

This paragraph covers two groups of adult users, namely, adult users who make use of online communication services without having the intention to produce or disseminate CSAM, and those who do. It is essential to stress that, while those users are addressed together in this section, they are vastly different from one another. With regards to adult users without malicious intents, based on studies focusing on adjacent domains, it can be expected that chilling effects would occur when the CSA proposal would enter into force.[213] Chilling effects refer to the notion that government surveillance may chill or deter people from engaging in certain legal (or even desirable) online activities because they fear legal punishment or criminal sanction, and do not trust the legal system to protect their innocence.[214]

In the case of the CSA proposal, some stakeholders expect the legislation to impact the behaviour of adult users who do not (seek to) engage in sharing or consuming CSAM in a way that they alter their current behaviour so as not to be deemed suspicious by authorities.[215] Such change in behaviour might, for instance, occur across parents who consult a general practitioner online about an issue that their child experiences. These parents might usually share images of their child with the general practitioner for advice, however, when the CSA proposal would enter into force, such images might be categorised as CSAM, as already has happened in practice.[216] This group of users

---

209 Ibid.

210 Kardefelt Winther et al., 'Encryption, Privacy and Children's Right to Protection from Harm', 2020, p. 8; Report presented at expert workshop on EU's proposed regulation on preventing and combatting child sexual abuse, Leiden University, February 2023, p. 19.

211 Expert input by academics, service providers and NGO.

212 Expert input by service provider and NGO.

213 Penney, J., 'Chilling Effects: Online Surveillance and Wikipedia Use', 2016, p. 119; The Chilling Effect of Student Monitoring: Disproportionate Impacts and Mental Health Risks, Center for Democracy & Technology, 2022, p. 2.

214 Schauer, F., 'Fear, Risk and the First Amendment: Unravelling the "Chilling Effect"', 1978, p. 687.

215 Expert input academics and NGOs.

216 A Dad Took Photos of His Naked Toddler for a Doctor. Google Flagged Him as a Criminal, The New York Times, accessed 9 March 2023; Reactionary Authoritarianism, Encryption, and You!, Electronic Frontier Foundation, March 2023.

might be inclined to change their behaviour in order to avoid suspicion and/or monitoring. While there is little evidence to quantify this expectation, several experts highlighted this as a to-be-expected adaptation by users of communication services.

With regards to the users who do consume CSAM through online communication channels, experts highlighted a number of elements. First of all, all experts agreed that within the group of people that produce, share and/or consume CSAM, there is a part which is determined to continue doing so and which will spend substantial efforts to circumvent any barrier that authorities put up. It is deemed extremely difficult to identify, let alone prevent this group from producing, sharing and/or consuming CSAM, consulted experts agree. There is likely a chase without ending between LEA and these types of perpetrators.[217] The CSA proposal is not expected to impact the behaviour of this group as they will resort to (and likely already have) other channels such as the deep web or dark web.[218] These platforms offer the privacy and security that these users seek in order to continue their activities.[219] It is, however, difficult to estimate the share of users who consume CSAM that would resort to the use of such illegal platforms to continue their activities.

Nevertheless, there are a number of elements that ought to be taken into account when assessing the expected shift to platforms such as the dark web. First, it should be noted that shifting activities to such platforms requires a certain degree of determination from the side of the user.[220] Not all consumers of CSAM might be determined to such a degree that they are willing to make the step and start using such platforms. Secondly, consulted experts argue that a certain level of understanding of technology is required to be able to make use of the dark web or deep web.[221] They note that a large share of the consumers of CSAM is not sufficiently tech-savvy to understand how to shift from using open communication channels or E2EE communication channels to the dark web or deep web. Finally, experts mention that there is an incentive for adult users that seek to groom children to remain active on 'regular' communication channels (i.e. not the dark web and deep web) because children (i.e. potential victims) are mostly active on the 'regular' communication channels.[222] Therefore, it can be expected that a part of the users that do have malicious intentions will not resort to the deep web or dark web for CSAM, because they do not have the means or capacity to do so.[223]

---

217 Expert input by law enforcement and service providers.

218 Expert input by academics, civil society and law enforcement; A similar trend was observed in the light of Wikipedia: Penney, J., 'Chilling Effects: Online Surveillance and Wikipedia Use', 2016, pp. 119, 174.

219 The sale and exploitation of children: digital technology, Unicef Office of Research-Innocenti, 2020, p. 2.

220 Expert input by NGO.

221 Expert input by NGO.

222 Van der Hof, et al. 'Sweetie 2.0, Using Artificial Intelligence to Fight Webcam Child Sex Tourism', 2019, p. 3.

223 Expert input by NGO.

4. Impact of the CSA proposal on fundamental rights

Answer to the corresponding research question in brief

What is the likely impact of the CSA proposal on fundamental rights, in particular the rights of the child, the rights of the victim, the right to liberty and security, the right to data protection, and the right to privacy, which includes the protection of private communications?

The impacted fundamental rights, laid down in CFR, are distinguished per affected group.

Children

(1) In aiming to prevent children falling victim to CSA, the proposal impacts several fundamental rights positively. It creates positive obligations for public authorities to act in protecting: Articles 3 CFR (the right to integrity of the person) and 4 CFR (prohibition of torture) require that children's physical and mental integrity are being ensured; Article 7 CFR (right to privacy) mandates that children's private and family lives are protected, and Article 24 CFR demands that children are protected from any form of violence.

(2) The measures, including detection orders of CSAM, provided in the CSA proposal can also negatively impact the fundamental rights of children as users of online services. More specifically, Articles 7 CFR (right to privacy), 8 CFR (right to data protection) and 11 CFR (right to freedom of expression and information) are affected. Limiting these rights may impact the personal development of children and their space to develop.

Users of services

(1) The proposal negatively impacts several fundamental rights of users of services by allowing for the issuing of detection orders that oblige service providers to screen their services for the dissemination of CSAM, known or new, or grooming. Firstly, the right to private life and communications (Article 7 CFR) would be negatively impacted to a serious extent, as the CJEU already acknowledged in respect of instances where traffic and location data are monitored, and would likely trigger a particularly serious infringement in cases where the content of interpersonal communications is concerned. Secondly, the right to protection of personal data (Article 8 CFR) would be impacted as screening by service providers constitutes a form of data processing. Thirdly, the freedom of expression and information (Article 11 CFR) would be seriously impacted as screening users' communications might deter people from openly expressing their views and receiving the views of others.

Providers of information society services

(1) The proposal interferes with one of the fundamental rights of providers of information society services. Article 16 CFR (freedom to conduct a business) aims at safeguarding the right to each individual in the EU to operate a business without being subject to either discrimination or disproportionate restrictions. Imposing an obligation on service providers to install and maintain a costly computer system to monitor all electronic communications made through its network interferes with this right.

In addition to the analysis of the impact of the CSA proposal on fundamental rights, this Chapter also provides the theoretical framework for the assessment of the necessity and proportionality of the obligations for service providers laid down by the CSA proposal.

Two principles under EU law ought to be considered when assessing the CSA proposal: the prohibitions against general data retention, and the prohibition on general monitoring obligations. These principles, in conjunction with relevant CJEU case law outline the limitations for general data retention, namely: the categories of data to be retained, the means of communication affected, the persons concerned, the retention period adopted and the need for objective evidence revealing at least an indirect link with serious criminal offences. The limitations for general monitoring obligations are: limits to the content identified in an order issued by a Court or Member State law, focused on specific (ready-known) types of content, they must be effective and proportionate, to not involve almost all information stored or transmitted by the users, to not be used as a preventive measure, to include sufficient fundamental rights safeguards and to not require an independent assessment.

In answering the research question on the impact of the CSA proposal on fundamental rights, this chapter follows the fundamental rights checklist specified in the Better Regulation Toolbox.[224] This checklist is designed to help understand whether the proposed measures that negatively impact fundamental rights can be justified under article 52 CFR.[225] The checklist consists of a four-step approach. The first two steps of this approach are addressed in this chapter and the necessity and proportionality test, which are part of step three and four of the fundamental rights checklist, will be addressed in the next chapter.

Next, this section introduces the EU law prohibition against generalised data retention and general monitoring obligations. These two principles define under which condition interpersonal communication services, internet access services and hosting services are allowed to retain and monitor content and data on their services in a way that aligns with key fundamental rights under the CFR. A theoretical overview of how these two principles ought to be applied in practice thus serves as a useful building block for assessing the necessity and proportionality test of the measures advocated for in the proposal.

Prior to doing so, it is useful to repeat briefly that the CSA proposal provides for the issuing of detection orders with respect to both hosting and interpersonal communication services. These different services monitor different categories of data, namely: content of communications during transmission, device-side scanning of content of communications before transmission, content retrieved via internet access, content on hosting services, app stores, traffic and location data.

4.1. The fundamental rights checklist

The fundamental rights checklist involves answering questions distributed over four steps:

1. How does the proposal impact different fundamental rights?

   The first step involves answering whether the measures advocated in the CSA proposal would impact fundamental rights, either positively or negatively. When some fundamental rights would be impacted negatively, the following three steps need to be taken to understand whether the proposal would nevertheless be compatible with the CFR.

2. Are the negatively impacted fundamental rights absolute or relative fundamental rights?

---

224 Better regulation toolbox, European Commission, p. 243-244.

225 Charter of Fundamental Rights of the European Union, December 2017.

The second step involves an analysis that investigates whether the negatively impacted fundamental rights are relative or absolute in nature. Where the fundamental rights are relative in nature, this step will further identify the applicable legal framework and interpretation given of these rights by the CJEU. Interference with relative fundamental right can be allowed if the conditions in steps 3 and 4 are met.

3. Are the negatively impacted fundamental rights provided for by law in a clear and predictable manner?

   Article 52(1) of the CFR prescribes that any limitation on the exercise of a fundamental right must be provided for by law in a way that is understandable and foreseeable for the average person.

4. Would the measure (a) genuinely meet an objective of general interest or protect the rights and freedoms of others? (b) preserve the essence of the negatively impacted fundamental rights? and (c) be necessary and proportionate to achieve the desired aim or objective?

   These sub-questions also follow from article 52(1) of the CFR. This article prescribes that measures that have a negative impact on (relative) fundamental rights can be considered as compatible with the CFR if the answers to these questions are 'yes'. The second and third bullet involve the so-called '*essence*' and '*proportionality and necessity*' tests.

4.2. Fundamental rights impacted by the CSA proposal

Step 1 of the fundamental rights checklist involves an analysis of the impact on the fundamental rights specified in the CFR. Similar as in the CSA proposal IA, the analysis carried out in this report is structured along the main groups whose fundamental rights are being impacted by the CSA proposal: children, users of services, and providers of information society services.

The following table shows which fundamental rights have been identified as being impacted by the proposal, including whether the fundamental rights have been impacted in a positive or in a negative way. As will be explained in more detail below, the identified fundamental rights of children are expected to be impacted in a positive way while the ones of users of services and providers of information society services are likely to be affected negatively. The full analysis of how each different fundamental right is being impacted by the proposal can be found in Annex IV.

Table 2: Assessed fundamental rights[226]

Rights of children (positively)	Rights of users of services (negatively)	Rights of information society services (negatively)
Article 3 – Right to integrity of the person Article 4 – Prohibition of torture and inhumane or degrading treatment Article 7 – Right of private and family life, home, and communications Article 24 – Rights of the Child	Article 7 – Right of private and family life, home, and communications Article 8 – Protection of personal data Article 11 – Freedom of expression and information Article 24 – Rights of the Child	Article 16 – Freedom to conduct a business

Source: Ecorys

[226] The research question also mentions the right of victims. As this is not a standalone right per the CFR and as the right to an effective remedy and fair trial is not directly related to the CSA proposal, this right has not been explicitly included in the analysis. In a way, the right of the victim has been addressed as part of the analysis of the rights of children.

4.2.1. Rights of children

The fundamental rights of children are expected to be positively influenced by the CSA proposal. This section presents an analysis of the expected impacts per right.

Articles 3 CFR (Right to integrity of the person) and 4 CFR (Prohibition of torture)[227]

Article 3 CFR states that 'everyone has the right to respect for his or her physical and mental integrity.' Article 4 CFR establishes that 'no one shall be subjected to torture or to inhuman or degrading treatment or punishment.' This right sets out an indispensable condition to protection of the right to human dignity (Article 1 CFR) and should be interpreted in its light.

In the case of the *La Quadrature du Net*, the CJEU ruled that public authorities face a positive obligation to protect children's physical and mental integrity and prevent them from inhumane or degrading treatment. [228] When producing CSAM, the inhumane or degrading treatment of children is taking place (live) or has taken place in the past. The circulation of the material continues and perpetuates the victimisation of the child involved. As the CSA proposal aims to prevent children falling victim to CSA and the further spreading of CSAM, it contributes to protecting their physical and mental integrity. These rights can thus be expected to be positively impacted by the CSA proposal.

Article 7 CFR (Right of private and family life, home, and communications)

Following Article 7 CFR 'everyone has the right to respect for his or her private and family life, home, and communications'. The rights guaranteed under Article 7 CFR involve that in principle there shall be no interference by a public authority with the exercise of this right.[229] Importantly, as emphasised in the case *La Quadrature du Net*, Article 7 also creates an active obligation for the public authorities to adopt legal measures that effectively protect private and family life.[230]

It can be expected that the CSA proposal would impact this right positively. The proposal aims to contribute towards reducing the chances of children falling victim to CSA and indirectly also protects children's private lives. Yet the same measures may have a potential risk for children's privacy rights: children have the right to private communications and that CSA proposal can interfere with their ability to build their own identity online and express themselves freely.

In addition, the CSA proposal does not explain the role of victims' personal data in criminal procedures if prosecutors decide to prosecute perpetrators after a positive hit. The use of images or content involving children as evidence in the prosecution of a case can have a negative impact on the child's right to private life, especially where the child's social and sexual life, sexual orientation, and similarly sensitive information are referred to by LEA in the investigation. The Law Enforcement Directive[231] may offer the appropriate legal framework to limit the impact of the private life of

---

227 Articles 3 and 4 are discussed together as the case law, more specifically the case *La Quadrature du Net,* treats them together in the context of data retention issues.

228 Judgment in Joined Cases C-511/18, C-512/18 and C-520/18 – *La Quadrature du Net and Others* v *Premier ministre and Others*, paragraph 126. (Hereafter: Judgment in Joined Cases C-511/18, C-512/18 and C-520/18 – *La Quadrature du Net).*

229 EU Charter of Fundamental Rights: Article 7 – Respect for private and family life, European Union Agency for Fundamental Rights, December 2007.

230 Judgment in Joined Cases C-511/18, C-512/18 and C-520/18 – *La Quadrature du Net*, paragraph 126. See also: Judgement in Case C-78/18 – *European Commission* v *Hungary (Transparency Associations)*, European Court of Justice, June 2020, paragraph 123. (Hereafter Judgement in Case C-78/18 – *European Commission* v *Hungary).*

231 Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

victims. The impact on this right when considering children as users of services is explored in the next section.

Article 24 CFR (Rights of the child)

Article 24 CFR establishes that "children shall have the right to such protection and care as is necessary for their well-being. They may express their views freely. Such views shall be taken into consideration on matters which concern them in accordance with their age and maturity. In all action relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration." The right to protection and care entails protecting children from any forms of violence.

Overall, in light of the analysis above and conditional on the effectiveness of detection and subsequent law enforcement, the expected impact of the CSA proposal on the rights of the children should be assessed as positive. The expected positive impact is closely related to the expected positive impacts as specified under Articles 3, 4, and 7 CFR. Article 24 CFR may also be negatively impacted if children's right to private communications is reduced through the measures laid down by the CSA proposal. Their ability to develop their identity and freedom of expression may be negatively impacted. In addition, the feeling of being watched (through technical measures) may lead the children to self-censor based on concerns over sexual content and solicitation.[232]

Article 6 CFR (Right of liberty and security)

The research question also requires an analysis of whether the proposal impacts the right of liberty and security. Article 6 states that 'everyone has the right to liberty and security of the person.' It corresponds to the right established by Article 5 ECHR, which is primarily focused on physical liberty and the prohibition of unlawful detention.[233] The proposal does not directly impact the physical liberty or unlawfully detains people.

Potentially, it can however be argued that a failure of the public authorities to prevent and punish CSA results in interference with children's liberty and security (under Article 6). This claim is, as specified in the case *La Quadrature du Net*, not consistent with the CJEU's interpretation of Article 6 CFR. In that case, the Court states that "Article 6 of the Charter cannot be interpreted as imposing an obligation on public authorities to take specific measures to prevent and punish certain criminal offences".[234]

4.2.2. Rights of users of services

The fundamental rights of users of services (including users who are children) are expected to be negatively influenced by the CSA proposal. With respect to users of services, the CSA proposal IA identified that the CSA proposal potentially impacts the fundamental rights laid down in Articles 7, 8, and 11 CFR. This also aligns with relevant case law of the CJEU.[235]

Article 7 CFR (Right of private and family life, home, and communications)

---

232 Powell et al. 'Child Protection and Freedom of Expression Online', 2010, p. 3.

233 Peers et al. 'The EU Charter of Fundamental Rights: A Commentary', 2021, p. 115.

234 Judgment in Joined Cases C-511/18, C-512/18 and C-520/18 – *La Quadrature du Net,* paragraph 125.

235 Judgment in Joined Cases C-293/12 and C-594/12 – *Digital Rights Ireland Ltd* v *Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others,* paragraphs 25 and 70. (Hereafter: Judgment in Joined Cases C-293/12 and C-594/12 – *Digital Rights Ireland)*; Judgment in Joined Cases C-203/15 and C-698/15 – *Tele2 Sverige AB* v *Post- och telestyrelsen and Secretary of State for the Home Department* v *Tom Watson and Others*, paragraphs 76 and 91 – 92. (Hereafter: Judgment in Joined Cases C-203/15 and C-698/15 – *Tele2 Sverige)*; Judgment in Joined Cases C-511/18, C-512/18 and C-520/18 – *La Quadrature du Net*, paragraphs 126 and 113.

Confidentiality of communications forms an integral part of the right to respect for private life. Article 7 CFR on the right to having a private life includes people's right to have private communications. This involves a general prohibition for state authorities against interference with one's personal communications.[236]

For CSAM to be detected as per the measures laid down by the CSA proposal, the communications of users need to be monitored for the types of content identified in the proposal. Hence the proposed detection orders will significantly affect the confidentiality of communications. The monitoring can also reveal a significant amount of personal information on the individuals affected, regarding their personal relationships and associations of family, friends, or their professional nature. The impact is on the totality of their lives and not limited to one particular aspect. In addition, these measures would interfere with the rights of a large group of users who are not complicit or implicated with using or distributing online CSAM.

Depending which type of information society services are addressed, detection orders will monitor traffic and location data and interpersonal communications content. The CJEU has in different cases considered that retention and analysis with respect to both traffic and location data (metadata) (in the cases *Digital Rights Ireland*[237] and *Tele2 Sverige*[238]) and content data (in the case *Schrems*[239]) by state authorities fall within the scope of Article 7 CFR. The rationale is that, as established in *Digital Rights Ireland,* the retention of even traffic and location data provides very precise conclusions on the private lives of the individuals whose data has been retained.[240] Collecting metadata (traffic and location data) constitutes a serious interference with Article 7 CFR. Arguably, the CSA proposal measures addressed to information society services (such as interpersonal communication services) monitoring the content of the communications would constitute an even more serious interference with Article 7 CFR and very likely also infringe the essence of the right.

Article 8 CFR (Protection of personal data)

The purpose of personal data protection is to offer protection to individuals with respect to the processing of their personal data. Two important definitions are 'personal data' and 'processing'. According to the GDPR[241], personal data refers to any information related to an identified or identifiable person. Processing involves any operation performed on this personal data. Any operation is defined broadly and comprises, among other things, the collection, storage, alteration and dissemination of personal data.[242] All activities that providers of information society services need to pursue according to the CSA proposal (i.e. retaining, analysing and, in the case of a positive hit, forwarding communication data to the public authorities) qualify as processing of personal data and fall thus within the scope of Article 8 CFR.

---

236 Handbook on European Data Protection Law, European Union Agency for Fundamental Rights and Council of Europe, April 2018, p. 19.

237 Judgment in Joined Cases C-293/12 and C-594/12 – *Digital Rights Ireland,* paragraphs 32-37.

238 Judgment in Joined Cases C-203/15 and C-698/15 – *Tele2 Sverige*, paragraph 93.

239 Judgment in Case C-362/14 – *Maximillian Schrems* v *Data Protection Commissioner*, paragraph 94. (Hereafter: Judgment in Case C-362/14 – *Maximillian Schrems).*

240 Judgment in Joined Cases C-293/12 and C-594/12 – *Digital Rights Ireland,* paragraph 27.

241 Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

242 Ibid., Article 4.

Article 11 CFR (Freedom of expression and information)

The fundamental right to freedom of expression and information entails a prohibition for public authorities to restrict people's ability to both send and receive information and ideas.[243] As expressed in the *La Quadrature du Net* case, the fact that providers of information society services retain traffic and location data for policing purposes already infringes on Article 11 CFR as it might potentially deter people from openly expressing their views as well as from freely receiving information.[244] This aligns with the 'chilling effect' as described in Chapter 3. This view has also been shared by the European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS).[245] Following on the reasoning of the CJEU, if the retention of traffic and location data already infringes Article 11 CFR, the monitoring and retention of interpersonal communications content would presumably have an even more serious impact on Article 11 CFR. The 'chilling effect' would be greater when users know that the content of their communication or a message on the device of the user is being is scanned for online CSAM.

In addition, screening of all content accessed via internet access services interferes with the freedom to freely receive information. This interference impacts the rights of potentially a large group of users that is covered by a detection order.

Another potential avenue along which the proposal impacts the freedom of expression includes the increased potential of erroneous over-removal of content in efforts by providers to avoid liability (assumption that it concerns CSAM). This restricts the ability of individuals to exchange ideas.

Children as internet users

So far, the analysis has shown that the proposal impacts the fundamental rights of children in a positive way and the fundamental rights of internet users in a negative way. However, it is important to bring some nuance to this sharp distinction. The reason is that children are not necessarily only potential victims that are being protected by this proposal. Children can also be internet users and, as such, the proposal also has a negative impact on children's right to privacy (Art. 7 CFR), data protection (Art. 8 CFR) and freedom of expression (Art. 11 CFR). In turn, Article 24 CFR will also be negatively impacted if children's right to private communications is reduced through the CSA measures. Their ability to develop their identity and freedom of expression may be negatively impacted. In addition, the feeling of being watched (through technical measures) may lead the children to self-censor based on concerns over sexual content and solicitation.[246] Indeed, some interviewees have put forward that the CSA proposal can also hinder children's sexual development because they become hesitant sharing messages, photos, and videos with each other if they know that they are being monitored.[247]

It is not disputed that children need protection from becoming victims of CSA and online CSAM (as identified in the earlier positive impact on rights of children), but they also need to be able to enjoy the protection of fundamental rights as a basis of their development and transition into adulthood.

---

243 Peers et al., 'The EU Charter of Fundamental Rights: A Commentary', 2021, p. 348.

244 Judgment in Joined Cases C-511/18, C-512/18 and C-520/18 – *La Quadrature du Net*, paragraph 118; Judgment in Joined Cases C-293/12 and C-594/12 – *Digital Rights Ireland*, paragraph 28.

245 Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, The EDPB and the EDPS, July 2021, p. 20 and 23.

246 Powell et al. 'Child Protection and Freedom of Expression Online', 2010, p. 3.

247 Expert input by service provider and NGO.

4.2.3. Right of information society services

The fundamental rights of information society services are expected to be negatively influenced by the proposal.

Article 16 CFR (Freedom to conduct a business)

The main aim of the right to conduct a business is to safeguard the right of each individual in the EU to operate a business without being subject to either discrimination or disproportionate restrictions. Following the CJEU's case law, the CSA proposal would interfere with Article 16 CFR. In the cases *Scarlet Extended* and *Netlog,* the Court held that imposing an obligation on providers of information society services to install and maintain a costly computer system to monitor all electronic communications made through its network infringes upon their freedom to conduct a business.[248]

As the proposal provides an obligation for providers of information society services to screen its networks on the dissemination of CSAM, which involves the maintenance of costly systems, this can also be understood as negative interference with Article 16 CFR.

4.2.4. Key determinants of the severity of the interference

The CSA proposal specifies that a detection order will only be issued if 'the reasons for issuing the order outweigh negative consequences for the rights and legitimate interests of all parties affected'.[249] In this context, it is important to highlight three particular factors that influence the degree of interference that a detection order causes, namely: whether the technology is being installed on private or public communications, the data types used by the technology to detect the exchange of CSAM or grooming, and the number of users of services affected by the detection order.

Installation on private or public communications

With regard to material that is accessible to the public, the measures in the CSA proposal would interfere with the users' enjoyment of Articles 7 and 8 CFR, as a provider of information society services will need to monitor what users post online and take decisions on whether CSAM is being disseminated or children are being groomed. This monitoring obligation may not be considered specific enough.[250] However, this impact is generally more limited as compared to the monitoring of private communications (which is not allowed in any generalised manner in EU law). The reason is that hosting services serve as 'virtual public spaces' for expression and economic transactions.[251] An additional issue is being presented with respect to the detection of the exchanging of CSAM and grooming in E2EE environments. In these environments, detection is only possible through client-side scanning (see Chapter 3). Although the CJEU did not take a decision on this, it can be argued that screening of content (including communications, photos, files etc.) on the device of the user is more privacy-invasive than service-side screening.[252]

---

248 Judgment in Case C-70/10 – *Scarlet Extended SA* v *Société belge des auteurs, compositeurs et éditerus SCRL (SABAM)*, paragraph 46. (Hereafter: Judgment in Case C-70/10 – *Scarlet Extended).*

249 Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, Article 7(4b).

250 Judgment in Case C-70/10 – *Scarlet Extended,* paragraph 51.

251 Ibid., p. 13.

252 Does monitoring your phone affect the essence of privacy?, European Law Blog, accessed 9 March 2023.

Monitoring according to data types

Turning to the data type used by the technology to detect the exchange of CSAM and grooming, it is important to distinguish between the use of traffic and location data (metadata) and the use of content data. As established in the case of *Digital Rights Ireland*, the use of the less infringing metadata already presents significant interference, as it can yield "very precise conclusions to be drawn concerning the lives of the persons whose data has been retained".[253] With respect to the use of technology that screens content of interpersonal communications, the CJEU found in various instances that this does not respect the essence of the considered fundamental rights if this is done on a generalised basis.[254]

Number of users

Finally, with respect to the number of users of services affected by the detection order, it is important to understand the current state of technology to detect CSAM and grooming. Key factors that impact the number of individual users affected by the detection order are the extent to which the technology is targeted upon a subset of users of the service, the number of users of the service, and the duration of the detection order. With respect to the latter, the CSA proposal specifies that detection orders regarding known or new material may have duration up to 24 months, whereas orders concerning grooming may last up to 12 months. Additionally, there is no limits regarding renewal of such orders, resulting in these interferences perpetuating.[255]

4.3. Nature of the (negatively) impacted fundamental rights

As per the fundamental rights checklist, for those rights that are found to be impacted negatively, it needs to be assessed whether the impacted rights are absolute or relative. Interference with absolute fundamental rights cannot be justified. It can be inferred from the explanatory memorandum of the CFR that interference with the rights in Article 7, 8 and 11 CFR can be allowed under certain conditions determined in Article 52 CFR. [256] The view that these three fundamental rights can be considered as relative rights is being supported in the case law of the CJEU.[257] In summary, the impacted fundamental rights of users of services qualify as relative rights.

Similarly, with regards to the rights of information society services, from the explanatory memorandum of the CFR, it can be inferred that interference with Article 16 CFR can be allowed under certain conditions (subject to the limitations provided in Article 52(1) CFR).[258] The freedom to conduct a business therefore qualifies as a relative right.[259]

As both the rights of users and information society services are identified as being relative, both are assessed as part of the necessity and proportionality test in Chapter 5.

---

253 Judgment in Joined Cases C-293/12 and C-594/12 – *Digital Rights Ireland,* paragraph 27.

254 Judgment in Case C-362/14 – *Maximillian Schrems*, paragraph 94. And Judgment in Joined Cases C-293/12 and C-594/12 – *Digital Rights Ireland.*

255 Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, Article 7(9).

256 Charter of Fundamental Rights of the European Union, December 2017, p. 21-22; Charter of Fundamental Rights of the European Union, December 2017, articles 8 and 10.

257 Judgment in Joined Cases C-511/18, C-512/18 and C-520/18 – *La Quadrature du Net,* paragraph 120; Judgment in Case C-362/14 – *Maximillian Schrems*, paragraph 172.

258 Charter of Fundamental Rights of the European Union, December 2017, p. 24.

259 Freedom to conduct a business: exploring the dimension of a fundamental right, European Agency for Fundamental Rights, 2015, p. 23.

4.4. CSA proposal in light of the prohibition of generalised data retention and general monitoring obligations in EU law

Two essential components to be addressed before assessing the necessity and proportionality of the obligations that the CSA proposal lays down on service providers. These are the following two principles under EU law: the prohibitions against general data retention, and the prohibition on general monitoring obligations. These principles provide, for the purpose of protecting the fundamental rights of users of services (and more specifically the ones laid down in Articles 7,8, and 11 CFR), boundaries on the extent to which providers of information society services can retain or monitor data on their network.[260] Therefore, both prohibitions are discussed in further detail in this section.

4.4.1. Introduction to the prohibition of general data retention and the prohibition of general monitoring obligations

The CSA proposal covers both traffic and location data (metadata) as well as content data. In addition, the CSA proposal applies to a range of providers of information society services, including both providers of interpersonal communication services as well as hosting providers. The following table provides a clear overview of the two sets of rules – for a prohibition of general data retention and prohibition of general monitoring obligations - and their application to different information society services and types of data monitored. It should be noted that in in practice, this distinction (between the two sets of prohibitions) is not always clear. In particular, certain services provided could be covered by several rules and, hence, careful analysis is needed.

[260] Wilman, F.G., 'Two emerging principles of EU internet law: A comparative analysis of the prohibitions of general data retention and general monitoring obligations', 2022., p. 10.

Table 3: Overview of differences between regimes of prohibition on general data retention and prohibition of general monitoring obligations

Rule	Prohibition of general data retention	Prohibition of general monitoring obligations
Relevant legislation	e-Privacy Directive[261]	Digital Services Act[262]
Relevant case law	Digital Rights Ireland[263] Digital Rights Ireland Tele2 Sverige[264] La Quadrature du Net and others[265]	L'Oréal v eBay[266] Scarlet Extended v SABAM[267] McFadden[268] Facebook Ireland Limited[269] Poland v European Parliament and Council[270]
Type of service providers	Internet access services and interpersonal communications services[271] In practice: internet voice calls, emails, messaging services or group chats (Interpersonal communication services)	Intermediary services ('mere conduit', 'caching' and 'hosting')[272] In practice: internet access services, publicly accessible Wi-Fi services, video-sharing platforms, social networks, and online marketplaces[273] (Hosting services)
Type of activity	Data retention	Monitoring of data
Type of content	Traffic and location data	Transmitted or stored data

Source: Ecorys

The following sections elaborate on the legislative framework and case law for both regimes.

261 Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

262 Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services.

263 Judgment in Joined Cases C-293/12 and C-594/12 – *Digital Rights Ireland.*

264 Judgment in Joined Cases C-203/15 and C-698/15 – *Tele2 Sverige.*

265 Judgment in Joined Cases C-511/18, C-512/18 and C-520/18 – *La Quadrature du Net*.

266 Judgment in Case C-324/09 – *L'Oréal* v *eBay International AG and Others*. (Hereafter: Judgment in Case C-324/09 – *L'Oréal* v *eBay).*

267 Judgment in Case C-70/10 – *Scarlet Extended.*

268 Judgment in Case C-484/14 – *Tobias Mc Fadden* v *Sony Music Entertainment Germany GmbH.* (Hereafter: Judgment in Case C-484/14 – *Tobias Mc Fadden* v *Sony).*

269 Judgment in Case C-18/18 – *Eva Glawischnig-Piesczek* v *Facebook Ireland Limited*.

270 Judgment in Case C-358/14 – *Republic of Poland* v *European Parliament and Council of the European Union*. (Hereafter: Judgment in Case C-358/14 – *Republic of Poland* v *European Parliament).*

271 Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code, article 2.

272 Ibid., Articles 12, 13 and 14.

273 Wilman, F.G., 'Two emerging principles of EU internet law: A comparative analysis of the prohibitions of general data retention and general monitoring obligations', 2022., p. 7.

4.4.2 The prohibition of general data retention

Legislative framework

The e-Privacy Directive lays down in Article 5 that "Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1)."[274]

This Directive also specifies (Article 15) that "Member States may adopt legislative measures to restrict the scope of the(se) rights and obligations […] when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection, and prosecution of criminal offences or of unauthorised use of the electronic communication system."[275] [276]

Case law

The CJEU has interpreted the e-Privacy Directive in various instances. On the basis of these interpretations, the CJEU determined the framework for the prohibition of general data retention. These interpretations do not specifically target the topic of CSAM; however, they do establish a basis of case law that is of relevance in the assessment of the CSA proposal.

Three cases in particular are of relevance here: *Digital Rights Ireland,*[277] *Tele2 Sverige*[278] and *La Quadrature du Net.*[279] In *Digital Rights Ireland*, the CJEU ruled that indiscriminate and general retention of traffic and location data (as provided for in the now invalidated Data Retention Directive[280]) was an infringement of the rights enshrined in Articles 7 and 8 CFR and could not be justified in the derogations of Article 15 of the e-Privacy Directive. Furthermore, this infringement could not be justified (in terms of Article 52 CFR) as it went beyond what is strictly necessary.[281] The CJEU held that even though from the retention of metadata, one would not necessarily also "acquire knowledge of the content of the electronic communications as such",[282] the retention of the metadata was enough to infringe the rights mentioned.

Tele2 Sverige[283] reiterated that the objective of fighting serious crime cannot justify the adoption of national legislation that provides for "the general and indiscriminate retention of all traffic and

---

274 Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Article 5.

275 Ibid., Article 15.

276 Following the revised European Electronic Communications Code Directive, online communication services such as instant messaging are now also subject to the e-Privacy Directive. Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code.

277 Judgment in Joined Cases C-293/12 and C-594/12 – *Digital Rights Ireland,* paragraph 37.

278 Judgment in Joined Cases C-203/15 and C-698/15 – *Tele2 Sverige.*

279 Judgment in Joined Cases C-511/18, C-512/18 and C-520/18 – *La Quadrature du Net.*

280 Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

281 Judgment in Joined Cases C-293/12 and C-594/12 – *Digital Rights Ireland,* paragraph 37.

282 Ibid., paragraph 39.

283 Judgment in Joined Cases C-203/15 and C-698/15 – *Tele2 Sverige.*

location data".[284] It then proceeded to introduce that the e-Privacy Directive would allow for the "targeted retention" of traffic and location data for the purpose of fighting serious crime. The targeted retention would have to be limited to what is strictly necessary, with respect to the categories of data to be retained, the means of communication affected, the persons concerned, and the retention period adopted. In addition to precise and clear rules and safeguards, the CJEU insisted on the presence of objective evidence revealing at least an indirect link with serious criminal offences".[285]

In *La Quadrature du Net*[286], the CJEU interpreted the term 'targeted surveillance' in the context of serious crime by introducing a number of conditions: the individuals affected must be identified in advance, on the basis of objective and non-discriminatory factors, as posing a threat to public or national security. The instruction for targeted surveillance may also be based on a geographical criterion.[287]

The CJEU referred specifically to 'particularly serious child pornography' offences, specifying that general and indiscriminate retention of IP addresses of all persons who own terminal equipment permitting access to the internet without, at first sight, any connection with the objectives pursued, and without being suspected of serious crimes is permissible, as the IP addresses might be the only means of investigation to identify the person to whom that address was assigned when the offence was committed. Nevertheless, the retention period must not exceed what is strictly necessary in light of the objective pursued, and substantive and procedural conditions regulating the use of that data must be foreseen.[288]

The CJEU further concluded that expedited retention of traffic and location data processed and stored by providers of information society services for a specified period of time is permissible for combatting serious crime and safeguarding national security. The retention of real-time traffic and location data must be considered as 'particularly sensitive', and, therefore, such retention may be justified for the purpose of the prevention of terrorism only in respect of persons for whom there is valid reason to suspect that they are involved in terrorist activities.[289]

Furthermore, the CJEU also reflected on automated analysis of all traffic and location data retained by providers carried out at the request of national authorities, which involved applying algorithms to detect suspicious patterns and behaviours in pursuance of safeguarding national security. The CJEU found that such processing would constitute general and indiscriminate processing and thus amount to a serious interference with the rights under Articles 7 and 8 CFR regardless of how that data is used subsequently.[290]

Thus, based on the above case law, it can be concluded that while data retention of traffic and location data are an interference with Articles 7 and 8 CFR, this interference can be justified if the surveillance is targeted (and not indiscriminate and general) and retention limited to:

(7) The categories of data to be retained;

(8) The means of communication affected;

(9) The persons concerned;

---

284 Ibid., paragraph 103.

285 Ibid., paragraphs 108 – 111.

286 Judgment in Joined Cases C-511/18, C-512/18 and C-520/18 – *La Quadrature du Net*.

287 Ibid., paras 149 - 150.

288 Ibid., paras 154 - 155.

289 Ibid., paras 164 – 165.

290 Ibid., paras 172-173.

(10) The retention period adopted;

(11) Objective evidence revealing at least an indirect link with serious criminal offences.

It is important to keep in mind that the CJEU found an infringement already on the retention of traffic and location data. Surveillance and retention of content data would hence be also an interference, possibly one that goes against the essence of the rights.

4.4.3. The prohibition of general monitoring obligations

Legislative framework

The origins for the prohibition of general monitoring obligations can be found in the e-Commerce Directive.[291] One of the main purposes is to exempt internet service providers from liability for the content they manage if they fulfil certain conditions. In 2022, the Digital Services Act (DSA)[292] entered into effect (with different dates for its application) amending (parts of) the e-Commerce Directive. Article 8 of the DSA lays down "no general obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers".

Specific orders can be issued. Article 9(1) of the DSA specifies that providers of intermediary services shall, upon receipt of an order to provide a specific item of information about one or more specific individual recipients of the service, inform the authority issuing the order of its receipt and the effect given to the order. Article 9(2) of the Digital Service Act then specifies criteria for orders to act against specific items of illegal content.

Voluntary actions by intermediary services to monitor for illegal content can be exempt from liability. Similar to the Interim Regulation, the DSA exempts intermediary services from liability if acting in good faith and in a diligent manner they carry out voluntary own initiative investigations and take down of illegal content, including CSAM.[293] Furthermore, intermediary services also have an obligation to assess systemic risks including the dissemination of illegal content through their services[294]; negative effects for the exercise of fundamental rights including respect for the rights of the child,[295] and the protection of minors.[296]

Case law

In various instances, the CJEU has interpreted the general monitoring obligation prohibition found in the e-Commerce Directive (in part the predecessor of the DSA). The case law is generally related to defamation and copyright. There is no case law that specifically addresses CSAM. This section presents how the CJEU distinguishes between general monitoring and specific monitoring obligations. In the *Eva Glawischnig-Piesczek v Facebook Ireland Limited*[297] case the CJEU set parameters for monitoring of specific content that has been held to be defamatory, content that is identical to defamatory comments and content that is equivalent. The CJEU ruled that a case can be classified as "specific" when the provider's search concerns already-known information that was declared illegal, and the name of the person concerned by the infringement. Furthermore, the CJEU

---

291 Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

292 Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services.

293 Ibid., article 7.

294 Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services, article 34(1)(a).

295 Ibid., article 34(1)(b).

296 Ibid., article 34(1)(d).

297 Judgment in Case C-18/18 – *Eva Glawischnig-Piesczek* v *Facebook Ireland Limited*.

ruled that an independent assessment concerning the content by the provider that requires automated search tools and technologies exceeds the sphere of a "specific case".[298]

While providers of information society services must not be obliged to monitor their users actively in order to identify illegality (e.g. in the case of infringement of intellectual property rights), effective and proportionate measures carried out by an providers of information society services are compatible with the prohibition of the obligation of general monitoring.[299] This was established in *L'Oreal and Others v Ebay*[300], in the context of copyright infringements.

In the context of what is effective and proportionate, one can look at *Scarlet Extended*,[301] and *McFadden v Sony Music Entertainment*[302]. The CJEU held in *Scarlet Extended*, that the installation of a (content) filtering system exceeds the sphere of 'specific' monitoring because it involves a systematic analysis of all content, and the gathering of identification details.[303] The CJEU concluded that such monitoring is generic, since it cannot distinguish between unlawful and lawful content.

In *McFadden v Sony Music Entertainment*,[304] the CJEU ruled that a wireless local area network operator could not be required to monitor 'all of the information transmitted' by means of that network, even if it were a question of blocking copies of a single musical work identified by the rightsholder.[305]

Furthermore, monitoring obligations (included in law) need to respect the right to freedom of expression and information of users of services. This was reiterated in *Poland v Parliament and Council*[306], where the CJEU was asked to consider the legality (in light of European Law) of Article 17 of the Directive on copyright in the Digital Single Market.[307] The CJEU ruled that the obligation on online content-sharing service providers to review, prior to its dissemination to the public, the content that users wish to upload to their platforms should be accompanied by the necessary safeguards to ensure that such obligation is compatible with freedom of expression and information. The CJEU underlined that providers of information society services should adopt measures which comply with the right to freedom of expression and information of users of services. These measures must be specific to ensure effective copyright protection without "affecting users who are lawfully using the services".[308]

In the case of illegal content such as copyright infringing content, an online platform provider cannot be liable for content uploaded by users on their platforms. In *Peterson v Google*,[309] the CJEU ruled that online platforms should not be liable for copyright infringing content posted by their users. The CJEU argued that services providers are not under a general obligation to monitor the information which they transmit or store or to a general obligation to look actively for facts or circumstances indicating illegal activity. Additionally, the Court clarified that even though the

298 Ibid., paras 45 - 46.

299 Judgment in Case C-324/09 – *L'Oréal* v *eBay*, paragraphs 141-143.

300 Ibid.

301 Judgment in Case C-70/10 – *Scarlet Extended.*

302 Judgment in Case C-484/14 – *Tobias Mc Fadden* v *Sony*.

303 Ibid., paragraph 51.

304 Judgment in Case C-484/14 – *Tobias Mc Fadden* v *Sony*.

305 Ibid., paragraph 7.

306 Judgment in Case C-358/14 – *Republic of Poland* v *European Parliament.*

307 Directive (EU) 2019/790 of 17 April 2019 on copyright and related rights in the Digital Single Market, Article 17.

308 Judgment in Case C-358/14 – *Republic of Poland* v *European Parliament*, paragraph 81.

309 Judgment in Joined Cases C-682/18 and C-683/18 – *Frank Peterson* v *Google LLC and Others and Elsevier Inc* v *Cyando AG*.

provider might have indexes with the uploaded material, provides a search function or suggests videos based on users' profiles, it cannot be concluded that the operator had "specific knowledge", unless they are informed or order to remove the content.

Thus, it can be concluded that imposing general monitoring obligations on providers of information society services is prohibited. Nevertheless, specific monitoring obligations can be mandated within certain parameter identified by the CJEU in its judgements. Specific monitoring ought:

(12) To be limited to content identified in an order issued by a Court or Member State law;[310]

(13) To be focused on specific (ready-known) types of content;[311]

(14) To be effective and proportionate;[312]

(15) Not involve almost all information stored or transmitted by the users;[313]

(16) Not be used as a preventive measure;[314]

(17) To include sufficient fundamental rights safeguards;[315]

(18) Not to require an independent assessment (i.e., for text-based communications).[316]

4.4.5. Summary of CSA proposal in the light of the prohibition of general data retention and the prohibition of general monitoring obligations

The above analysis is summarised in the following table. It indicates which limitations for general data retention and general monitoring obligations the CSA proposal provides for and where those are specified in the proposal. This table indicates *if* the CSA proposal indicates limitations. Whether these are *sufficient and specific* enough is assessed in Chapter 5.

Table 4: Overview of limitations for general data retention and general monitoring obligations provided for in CSA proposal

Limitation provided for	Main place in CSA proposal
Categories of data to be retained	Article 10 (3) – protection of personal data
Means of communication affected	Article 7 (8) – specification of part of component of service
Specification of period	Article 7 (8 - 9) – specification of start and end date of detection order
Specification of type(s) of content	Article 8 (1) – specification of type of content concerned
Proportionality	Article 7 (8) – to focus on what is strictly necessary
No preventive measure	Article 7 (4) – evidence of a significant risk
Fundamental rights safeguards	Article 7 (2 – 4) – safeguards before issuing a detection order Article 9 – options for redress

Source: Ecorys

310 Judgment in Case C-18/18 – *Eva Glawischnig-Piesczek* v *Facebook Ireland Limited*, paragraph 45; and Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services, article 9 (2).

311 Ibid.

312 Judgment in Case C-324/09 – *L'Oréal* v *eBay*, paragraphs 141-143.

313 Judgment in Case C-70/10 – *Scarlet Extended,* paragraph 51; and Judgment in Case C-484/14 – *Tobias Mc Fadden* v *Sony*, paragraph 7.

314 Judgment in Case C-324/09 – *L'Oréal* v *eBay*, paragraphs 141-143.

315 Judgment in Case C-358/14 – *Republic of Poland* v *European Parliament*, paragraph 81.

316 Judgment in Case C-18/18 – *Eva Glawischnig-Piesczek* v *Facebook Ireland Limited*, paragraph 46.

In the analysis presented in this chapter, several limitations were identified that are not covered in the CSA proposal. These concern limitations on the persons concerned, the need for objective evidence revealing at least an indirect link with serious criminal offences, monitoring cannot be required for all information stored or transmitted by the users and that monitoring must not require independent assessment. This observation is further explored in the next chapter.

5. Assessment of the necessity and proportionality of the proposed measures obliging providers to detect, report and remove CSAM

Answer to the corresponding research question in brief

How would the detection of new CSAM or grooming respect the prohibition of general monitoring obligations? Are the new obligations and requirements foreseen in the CSA proposal precise enough so to not violate the prohibition of general monitoring obligations?

(1) With regard to obligations on scanning the content of interpersonal communications by interpersonal communications providers, which includes grooming, new CSAM and likely known CSAM, the analysis shows that the proposed rules compromise the essence of the fundamental right to privacy in the form of confidentiality of communications. Scanning content on users' personal devices in the context of E2EE communications violates the essence of the right to data protection.

(2) The parameters to detect known material can be set with a high degree of specificity because these seek to identify content that has previously been categorised as CSAM. The CSA proposal does not require a detection order to be targeted at a specific group of users or content, and therefore the detection orders would violate the prohibition of general data retention (for interpersonal communication services) and the prohibition of general monitoring obligations (for hosting services). In theory, the CSA proposal could be amended to require detection orders to specify a certain group of users to be targeted in line with the requirements of the case law of the CJEU, in order to prevent detection orders from violating the prohibitions of general data retention and general monitoring. However, certain classifiers such as geographic location, age, or gender would not be appropriate features to be used for specifying the groups of users subject to detection orders because they cast the net too wide.

(3) For new CSAM and grooming, the parameters for detection cannot be set with high specificity as it is not predetermined which exact content a technology ought to identify. With regard to new material, the technologies can, therefore, only be applied indiscriminately to all users of both hosting services and interpersonal communication services. The proposed rules regarding obligations to detect new CSAM both to hosting providers and (all the more) to interpersonal communications providers disproportionately affect the right to privacy in terms of the group of users targeted by the detection orders, which would amount to unlawful generalised monitoring and unlawful generalised surveillance. The requirements to be set to detect grooming would not be targeted enough and thus amount to by default generalised and indiscriminate automated analysis of all communications transmitted through interpersonal communication services.

(4) In the case of E2EE communications, even if one would not accept that the essence of the right to data protection is compromised, the device side scanning of interpersonal communications is disproportionate to the aims pursued. It creates vulnerabilities and exposes users to a particularly increased risk of unlawful access.

Answer to the corresponding research question in brief

Are the measures foreseen in the CSA proposal necessary and proportionate, in particular regarding the new binding obligations for relevant service providers to detect, report, and remove from their services known and new child sexual abuse material or text-based threats such as grooming, having regard for CJEU case law and notably the Judgment of 6 October 2020, La Quadrature du Net and Others v Premier ministre and Others?

Necessity of the measures

(1) The assessment of the necessity of the measures requires an analysis on whether the measures will be effective in achieving their goal and, if so, whether less intrusive means could reach the same goal. With respect to the effectiveness, there are two main concerns. The first relates to the current state of play of the technology to detect new material, and grooming. The second concern involves the extent to which LEA officials will be able to assess detected CSAM or grooming and, if assessed positively, act upon it by prosecuting the suspects. The evidence collected in the CSA proposal IA is too limited with respect to both concerns.

(2) Turning to the question of whether less intrusive ways could reach the same goal as the detection order, it is important to have a look at the structure of the CSA proposal. Article 4 of the CSA proposal presents the possibility of mitigation measures for service providers to reduce the risk of abuse of their service. Should the provider fail to voluntarily adopt such measures, the competent coordinating authority can issue a detection order. However, it does not provide the coordinating authority with a legal basis to take other less intrusive measures and, as such, the CSA proposal does not allow the coordinating authority to opt for less intrusive measures to achieve the same objectives.

Proportionality of the measures

(1) In *La Quadrature du Net*, the CJEU has set out three different objectives for data retention, namely (a) national security (b) serious crime and (c) public security and combatting crime. It ruled that in the light of safeguarding national security, general data retention may be justified. As CSAM would not qualify as a matter of national security but rather as a serious crime, the options for data retention are more restricted and should be more targeted.

(2) The way in which the rules regarding the issuance of detection orders in the CSA proposal are currently phrased does not rule out detection orders that would provide a generalised data retention obligation to service providers. Therefore, with regard to the detection of known material, the CSA proposal raises proportionality concerns because of a lack of requirement on how specific the detection order will be with respect to the targeted individuals. It is feasible for detection orders to specify a certain group of users to be targeted in line with the case law of the CJEU.

(3) With regard to known material, proportionality concerns are raised in relation to the technologies used in detection in E2EE communications, the procedural safeguards regarding the issuance of detection orders and the duration of the detection order.

(4) With regard to new material and grooming, there are proportionality concerns with respect to specification of the group of users whose communication would need to be screened on the dissemination of CSAM due to the technology used.

(5) Therefore, new binding obligations stemming from detection orders for relevant service providers to detect, report, and remove new material and grooming from their services would likely fail the proportionality test.

At the heart of this complementary IA lies an analysis as to whether the CSA proposal is compatible with the protection of fundamental rights. For this purpose, the four steps of the fundamental rights checklist, as specified in the Better Regulation Toolbox, are being used. The first two steps have been discussed in the previous chapter.

5.1. Assessment of the legal basis for the interference

Step 3 of the fundamental rights checklist, which reiterates the requirements for a permissible limitation of fundamental rights under Article 52(1) CFR, concerns answering the question of 'whether the proposed measures that interfere with fundamental rights are provided for by law in a way that is understandable and foreseeable for the average person'. This will require a two-step approach where first it will have to be verified whether there is some sort of legal basis for the interference. Then, it needs to be established that the law is sufficiently accessible and precise for the average person.

In particular, the accessibility requirement means that the person concerned must be able to have an adequate indication of the legal rules applicable to a given case.[317] Sufficient precision is understood as providing the person concerned, if need be, with appropriate advice, to foresee the consequences a given action may entail to a reasonable degree depending on the circumstances.[318] However, absolute certainty is not required.[319] In the context of this proposal, foreseeability refers to two groups in particular: providers of information society services (with the aim that they understand how they ought to implement the proposal in practice) and users of these services (such that they understand to what extent their communications will be monitored).

The CSA proposal aims to establish a lawful basis for the interference. It imposes obligations on providers of information society services to act. This satisfies the first part of the approach. In the present case, whereas the adoption of a legal instrument would fulfil the accessibility requirement, the foreseeability of the obligations imposed on providers is more complicated.

Problems with respect to foreseeability arise especially due to the fact that some terms used in the proposal are rather vague. As a result, providers of information society services and the coordinating authorities will face uncertainty on how they ought to implement the CSA proposal and it will create de facto discretionary freedom for the providers of information society services and coordinating authority to interpret the norms. Users of the services will also have difficulties to foresee to what extent their communications will be monitored; the concrete measures, namely the detection orders will not be published and the foreseeability of how their communications will be monitored will solely be based on the wording of the proposed rules, which do not provide sufficient clarity.

With regard to the terminology used on the risk assessment and mitigation, Article 3 of the CSA proposal obliges providers of hosting services and providers of interpersonal communications services to identify, analyse, and assess the risk of use of the service for the purpose of online CSA and try to minimise the identified risk by applying 'reasonable mitigation measures'.[320] Article

---

317 Judgment in Case 6538/74 – *The Sunday Times* v *The United Kingdom*, European Court of Human Rights, April 1979, paragraph 49.

318 Ibid.

319 Ibid.

320 Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, European Commission, May 2022, Article 4(1).

3(2)(a)-(e) indicates which elements to take into account in the risk assessment. Here, in line with the joint opinion by the EDPB and the EDPS, the CSA proposal raises foreseeability concerns as some criteria leave a wide margin of discretion. In particular, the criterion on 'the manner in which users use the service and the impact thereof on that risk' is rather vague and the criterion concerning platforms 'enabling users to share images or videos with other users' is also widely applicable and will apply to a large number of online services.[321] The risk of lack of clarity with respect to the risk assessment and mitigation obligations entails that providers can interpret their duty in different manners. This is undesirable because the initial risk assessment is crucial for the decision on whether or not detection orders are issued.

With regards to detection orders and the choice of technology that is used for the detection of CSAM, there are similar concerns. Examples include the use of the term 'appreciable extent' in Article 7(4) – (6), which describes the acceptable amount of risk, and 'effective' in Article 10(3) referring to the deployment of effective technology to detect the exchange of CSAM. [322] The lack of clarity on a series of substantive norms related to detection orders constitutes a major challenge of the CSA proposal as the coordinating authority will have much discretionary freedom.[323] The risk of this arbitrariness in the issuance of detection orders must be highlighted as vague terms facilitate the problem that coordinating authorities can issue these orders in a wide manner, potentially resulting in a practice that de facto involves general and indiscriminate monitoring.[324]

5.2. Assessment of the objectives pursued by the CSA proposal

The first question of the fourth step of the fundamental rights checklist, and a requirement under Article 52(1) CFR, is whether the measures advocated in the CSA proposal genuinely meet an objective of general interest or protect the rights and freedoms of others.

The CSA proposal constitutes part of the European Commission's wider commitment to combat online CSA. This commitment is evident in the EU Strategy on the Rights of the Child[325], the EU strategy for a more effective fight against CSA[326], and the EU Better Internet for Kids Strategy.[327] In this light, it can be concluded that the CSA proposal meets the objectives of general interest recognised by the Union. At the same time, the measures in the CSA proposal aim to protect the rights and freedoms of others, namely of children, in particular their rights to human dignity and to the integrity of the person, the prohibition of inhuman or degrading treatment, as well as children's rights to respect for private and family life and to protection of personal data.

---

321 Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, The EDPB and the EDPS, July 2021, p. 14.

322 Ibid., p. 14; Report presented at expert workshop on EU's proposed regulation on preventing and combatting child sexual abuse, Leiden University, February 2023, pp. 14.

323 Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, The EDPB and the EDPS, July 2021, p. 16.

324 Ibid, p. 20.

325 Communication on EU strategy on the rights of the child, COM(2021) 142 final, European Commission, March 2021.

326 Communication on EU strategy for a more effective fight against child sexual abuse, COM/2020/607 final, European Commission, July 2020.

327 Communication on A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+), COM(2022) 212 final, European Commission, May 2022.

5.3. Assessment of respect for the essence of the fundamental rights

The second question of the fourth step of the fundamental rights checklist concerns whether the measures foreseen in the proposal preserve the essence of the fundamental rights in question.

Even though interference with relative rights can be justified in accordance with the principle of proportionality, their essence needs to be respected at all times.[328] The existing case law is not straightforward as to the exact conditions that lead to a measure not respecting the essence of a right. However, as described below, the CJEU has provided some guidance in its case law on factors that need to be taken into account for assessing whether the essence of fundamental rights.

In particular, based on a series of judgments, it can be deduced that interferences with the content of interpersonal electronic communications can affect the essence of the fundamental right to private life in Article 7 CFR. In *Digital Rights Ireland,* the CJEU sitting in Grand Chamber held that: "So far as concerns the essence of the fundamental right to privacy and the other rights laid down in Article 7 of the Charter, it must be held that, even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference with those rights, it is not such as to adversely affect the essence of those rights given that, as follows from Article 1(2) of the directive, the directive does not permit the acquisition of knowledge of the content of the electronic communications as such".[329] This was confirmed in *Tele2 Sverige* where the CJEU opined that the retention of the content of communications can adversely affect the essence of the rights to private life and data protection.[330] In *Schrems*, the Court held 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 […]'.[331]

In light of the above, measures permitting the public authorities to have access on a generalised basis to the content of a communication are more likely to affect the essence of the rights guaranteed in Articles 7, 8, and 11 CFR. In *Digital Rights Ireland,* the CJEU specified that Member States need to adopt the necessary safeguards that protect the essence of these fundamental rights.[332] In this context, the EDPS and EDPB have highlighted the importance of encrypted communications.[333]

In the present case, the CSA proposal entails obligations on interpersonal communication providers to target the content of interpersonal communications either on the device or on the communications being routed through servers (if any). A detection order on the content of interpersonal data either on the device or the server will compromise the essence of the right to

---

328 Brkan, M., 'The Concept of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core', 2018.; Lenaerts, K., 'Limits on Limitations: The Essence of Fundamental Rights in the EU', 2019; Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, European Data Protection Supervisor, December 2019, p. 8.

329 Judgment in Joined Cases C-293/12 and C-594/12 – *Digital Rights Ireland,* paragraph 39.

330 Judgment in Joined Cases C-203/15 and C-698/15 – *Tele2 Sverige*, paragraph 101.

331 Judgment in Case C-362/14 – *Maximillian Schrems*, paragraph 94.

332 Judgment in Joined Cases C-293/12 and C-594/12 – *Digital Rights Ireland,* paragraph 40.

333 Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, EDPB and EDPS, July 2021, pp. 27-28.

privacy under Article 7 CFR in the form of confidentiality of telecommunications. It constitutes a form of access on a generalised basis, pursuant to *Schrems*, where it involves an analysis of all communications going through the server. In the case of detection on the device the intrusiveness is even greater because the device is with their owner.[334] This involves new material but may also involve detecting known CSAM, because a dragnet approach is likely to be used and therefore all content of interpersonal communication would have to be scanned to sift out the known CSAM.

Furthermore, grooming on the networks of interpersonal communication services requires automated analysis of all videos, photos, text messages, and speech exchanged on such networks. Importantly, the technology is not yet ready to detect new material or grooming by targeting a specific group or geographical area. As a consequence, a detection order specifying the need for detecting new material or grooming will de facto imply generalised and indiscriminate surveillance of all content exchanged on the network of the interpersonal communication service that received the detection order. Therefore, in line with *Schrems,* such monitoring of the content of interpersonal electronic communications on a generalised basis violates the essence of Article 7 CFR.

Scanning content on users' personal devices in the context of E2EE communications poses additional concerns regarding the essence of the right to data protection under Article 8 CFR. In *Digital Rights Ireland*, the CJEU opined that the essence of that right was not compromised because in the Data Retention Directive certain principles of data protection and data security must be respected and Member States are to ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data.[335] Based on this, it could be argued that when a detection order entails client-side scanning whereby contents of messages will be scanned for CSAM before the message is sent to the intended recipient it would prevent taking appropriate security measures to protect personal data, and therefore the essence of the right to data protection will not be respected.[336]

In light of the above, the obligations imposed on interpersonal communications services violate the essence of the right to private life in the form of confidentiality of communications. This involves potentially known CSAM and certainly new CSAM and grooming. In addition, scanning content on users' personal devices in the framework of E2EE communications violates the essence of the right to data protection.

5.4. Assessment of necessity and proportionality

The final step of the fundamental rights check lists consists of the necessity and proportionality test. This involves answering the question of whether the measures foreseen by the proposal are necessary and proportionate to achieve the desired aim of the proposal.

5.4.1. Necessity test

Assessing the necessity of the proposed measures entails an assessment on the effectiveness of the envisaged measures for achieving the objective pursued and of whether it is less intrusive than other options for achieving the same goal.

---

334 Does monitoring your phone affect the essence of privacy?, European Law Blog, accessed 9 March 2023.

335 Judgment in Joined Cases C-293/12 and C-594/12 – *Digital Rights Ireland,* paragraph 40.

336 Does monitoring your phone affect the essence of privacy?, European Law Blog, accessed 9 March 2023.

Effectiveness of envisaged measures for achieving the objectives pursued

A first concern relates to the question whether the technology is effective in detecting known material, new material, and grooming. According to Article 10(1) of the CSA proposal, providers shall execute detection orders by installing and operating technologies to detect online CSAM, using the indicators provided for by the EU Centre. Providers can choose to develop their own technology or use technology made available by the EU Centre (provided that the technology meets a series of requirements laid down in Article 10(3) of the CSA proposal).

Assessing the accuracy of the to-be-used technology for the detection of known material, new material, and grooming requires taking into account a variety of sources. This implies that evidence coming from the developers of technology should be assessed with scrutiny and not be taken for granted.[337] The evidence on the accuracy of the technology presented in the CSA proposal is overly reliant on industry claims and uncritical.

As outlined in Chapter 3, the accuracy with which CSAM can currently be detected varies between known material, new material, and grooming. The accuracy of the detection of known material can be considered of high if an unaltered copy of the known CSAM is circulated, however if known CSAM has been altered in order to avoid detection then the technology will not be effective. As regards the technological tools for the detection of new material and grooming, these are of substantially lower accuracy and therefore due to the lack of maturity they are not reliable enough and will affect the effectiveness of envisaged measures. Also, there is no indication regarding the technologies to be used for monitoring of audio messages. Besides limited accuracy levels, the technologies to detect all three types of CSAM can be easily circumvented. E2EE and fingerprinting known CSAM are examples of technologies that can circumvented.[338]

A second concern, raised in the joint opinion of the EDPB and the EDPS, relates to how the CSA proposal envisages that LEA will take action as a follow up of the detection activities on a timely basis.[339] Cases of potential new material and grooming will most likely reveal recent or ongoing abuse, requiring a timely response from LEAs. The CSA proposal foresees a procedure in which providers first assess potential CSAM and then report it to the EU Centre.[340] The EU Centre must then 'expeditiously' assess the content, process the reports and if those are not deemed 'manifestly unfounded', it forwards them to Europol and to the LEAs with jurisdiction to investigate the case. After receiving the report, LEAs start their investigation.

While there is no clear timeframe specified regarding the identification of CSA cases,[341] the question arises how LEAs would assess a potentially high number of cases in a timely manner. The European Commission states that "significant investment of resources [is] required for LEAs to deal effectively

---

337 Report presented at expert workshop on EU's proposed regulation on preventing and combatting child sexual abuse, Leiden University, February 2023, p. 17.

338 Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, EDPB and EDPS, July 2021, p. 18.

339 Ibid., 18.

340 Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, European Commission, May 2022, Article 12 (1).

341 Report presented at expert workshop on EU's proposed regulation on preventing and combatting child sexual abuse, Leiden University, February 2023, p. 16.

with the volume of reports these authorities receive".[342] Potential prioritisation of urgent cases where there is evidence that a child may be in danger may be needed, but this raises questions as to which criteria to employ for such prioritisation or whether additional evidence would be required in addition to the material flagged by the provider.[343]

Finally, a concern related to the previous one is that the effectiveness of the proposed measures depends on to what extent law enforcement officials act upon detected CSAM or grooming (after it has been verified as truly constituting CSAM or grooming) in the form of prosecuting perpetrators. There is currently not sufficient evidence to assess the foreseen impact of the CSA proposal on the prosecution of suspects.

Existence of less intrusive measures to achieve the same objectives

The second part of the necessity test involves examining whether there exist less intrusive measures to achieve the same objective. Article 4 of the CSA proposal presents the possibility of mitigation measures for providers of information society services to reduce the risk of abuse of their service. Should the provider fail to adopt such measures voluntarily, the competent authority may require the implementation of mitigation measures to be mandatory and enforceable instead of issuing a detection order. The EDPB and EDPS note that this is not sufficient, as such a requirement would not be independently enforceable. [344] Moreover, the competent authority is not empowered to impose less intrusive mitigation measures prior to or instead of issuing a detection order.[345] Thus, the CSA proposal does not allow for less intrusive measures to achieve the same objectives.

Main findings on the necessity of the proposed measures

With respect to the first question of the necessity test on the effectiveness of the advocated measures, there are two main concerns. The first one relates to the current state of play of the technology to detect known material, new material, and grooming. The effectiveness of technologies to detect known CSAM if an unaltered copy of the known CASM is circulated are expected to be effective, but if known CSAM has been altered to avoid detection then the technology will fail. For new CSAM and grooming the technologies are not yet accurate enough to be considered effective. The second concern involves the extent to which law enforcement officials will be able to assess detected CSAM or grooming and, if assessed positively, act upon it by prosecuting the suspects. Depending on the number of cases, it is possible that the LEA may not have adequate resources to go through the flagged material, thus affecting the effectiveness of the proposed measures. Turning to the second question on whether less intrusive measures can be used reaching the same effect, the main concern is that the CSA proposal does not empower coordinating authorities to adopt mitigation measures that are less intrusive for fundamental rights than the issuance of detection orders.

5.4.2. Proportionality test

The proportionality test involves an analysis on the means used and the intended aim of the CSA proposal. If the means yield a negative impact that exceeds the positive impact of the intended aim, the proposed rules would be disproportionate. This analysis is performed by taking into account the

---

342 Impact Assessment Report Accompanying the document Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, European Commission, May 2022, p. 33.

343 Report presented at expert workshop on EU's proposed regulation on preventing and combatting child sexual abuse, Leiden University, February 2023, p. 16.

344 Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, EDPB and EDPS, July 2021, pp. 18-19.

345 Expert input by academics and service providers.

CJEU's case law on the prohibition of general data retention and the prohibition of general monitoring obligations outlined in Chapter 4.

From the outset with regard to obligations on scanning the content of interpersonal communications by interpersonal communications providers, which includes all cases of grooming, but will also involve new CSAM and it is likely to involve known CSAM too, the analysis above has shown that the proposed rules compromise the essence of the fundamental right to privacy in the form of confidentiality of communications. In fact, compromising the essence of privacy signifies that the measure in respect providers that target the content of interpersonal communications irreparably violates the fundamental right of privacy. Furthermore, scanning content on users' personal devices in the context of E2EE communications violates the essence of the right to data protection.

Proportionality and differentiation between the three types of CSAM

For the proportionality assessment, it is essential to differentiate between the three types of content that the CSA proposal covers: known CSAM, new CSAM, and grooming. As the nature of these types of content as well as the efforts required to detect, report, and remove it are inherently different, the analysis will continuously make this distinction. Where relevant, a distinction between the proportionality for detection on internet access services, hosting services, interpersonal communication services and device side scanning of E2EE communications is made.

Known material

By nature, known material can be detected, removed, and blocked relatively easily because it is clear which exact content ought to be identified. Thus, the detection of known CSAM content can be specified with regards to the content in the sense that the parameters for the to-be-detected content can be set with relatively high precision (see Chapter 3).[346] However, a specification of the exact content to be detected is not sufficient to pass the proportionality test, as it is necessary to ensure that the detection orders specify a certain group of users to be targeted. With regards to the detection of known material, the CSA proposal raises proportionality concerns because of a lack of requirement on how specific the detection order will be with respect to the targeted individuals. Furthermore, proportionality concerns are raised in relation to the technologies used in detection in E2EE communications, the procedural safeguards regarding the issuance of detection orders and the duration of the detection order.

Targeted group of users

With respect to the scope of the proposed measures for internet access services and hosting services, the CSA proposal does not contain a requirement that the detection orders specify a certain group of users to be targeted and therefore, the detection of known material could still require monitoring of all users of a given service. This is not specific enough, pursuant to the relevant CJEU case law.[347] In *G.D. v The Commissioner*, the CJEU ruled that monitoring ought to target persons whose traffic and location data are likely to reveal an (indirect) link with serious criminal offences, to contribute in one way or another to combatting serious crime or towards preventing a serious risk to public security, a risk to national security (which is not relevant to the present case) or persons

[346] The detection, removal, or blocking based on URLs is more complex when the full URL is end-to-end encrypted between the user's browser and the web server. Member States want internet service providers to do the impossible in the fight against child sexual abuse, European Digital Rights, accessed 9 March 2023.

[347] Does monitoring your phone affect the essence of privacy?, European Law Blog, European Law Blog, accessed 9 March 2023.

who have been identified beforehand as posing a threat to public or national security.[348] In the case of monitoring for known CSAM, this would not necessarily be the case.

With regards to detection of known CSAM on interpersonal communication services, similar observations can be made. A detection order would not specify the groups of individuals whose content of interpersonal electronic communications would be monitored. Therefore, in such cases the detection orders cannot be deemed as targeted surveillance with regards to the number of users that will be affected. In accordance with *La Quadrature du Net*, the proposed detection of known CSAM would be disproportionate to the aim pursued. Towards this direction points also the fact that according to Article 7(1), the conditions for issuing a detection order are rather vague and general and can be applied to an entire service and not just to selected communications.

It should be noted that if the CSA proposal would address the above observations and would require detection orders to also be specific with regards to the group of individuals to be monitored, the detection of known material could be considered specific enough so as not to violate the prohibition of general monitoring obligations (for internet access services and hosting services) and would comply with communications secrecy (for interpersonal communication). Technically, it could be feasible to program detection technologies for known material to monitor only the exchanges of a particular type of group, thereby, preventing overly wide detection orders in terms of affected users, in line with the CJEU case law. Such groups could for instance be members of a forum or chat group (where previously CSAM was exchanged). However, there needs to be caution as to which criteria are used to specify the group of users. Classifiers such as geographic location, age, or gender would not be appropriate features to be used for specifying the groups of users subject to detection orders because they cast the net too wide. Furthermore, users are not required to share such details before using services, therefore, providers of information society services do often not have access to such information.[349] Moreover, such classifiers can easily be falsified or circumvented (i.e., by the use of VPN). In any case, should technologies be set to detect CSAM in a particular group, there needs to be objective evidence revealing at least an indirect link with serious criminal offences and in particular with CSA. This evidence could be based on the risk assessment that the provider has produced before the issuance of a detection order, or other evidence (e.g., lists of existing offenders of CSA) to narrow down the group of affected users.

Technologies to detect CSAM in open communication and E2EE

With regard to the means used, Article 10 of the CSA proposal prescribes a series of requirements for the technologies to be used for detection purposes. These concern in particular their effectiveness, reliability and least intrusive nature in terms of impact on the users' rights. As stated in the joint opinion by the EDPB and the EDPS and discussed in Chapter 3, relying on hashes seems to be able to meet generally these standards, thus not raising proportionality challenges.[350]

However, in the case of detecting CSAM in E2EE communications, the device side scanning of interpersonal communications is disproportionate to the aims pursued, even if one would not accept that the essence of the right to data protection is compromised. Detecting CSAM in E2EE communications creates vulnerabilities and exposes users to a particularly increased risk of unlawful

---

348 Judgment in Case C-140/20 – *G. D.* v *The Commissioner of the Garda Síochána and Others*, paragraphs 76-78.

349 France recently announced that it would start age verification on pornography websites. France moves to block access to pornography sites for minors, Reuters, accessed 9 March 2023.

350 Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, The EDPB and the EDPS, July 2021, p 21.

access by other governments and criminal organisations.[351] It sets a precedent and poses a risk for potentially repurposing this functionality for other purposes aside CSAM resulting in mass surveillance.[352] There is also a danger of generalised surveillance of the content not only shared within that platform but on other parts of the device, if programmed to do so.

Procedural safeguards

The fact that detection orders must be issued by judicial authorities or by independent administrative authorities upon request of the coordinating authority is an important procedural safeguard. However, it is deemed insufficient because it allows for too much discretionary power with the national authorities, without imposing any limitations as to the scope of the detection orders. This may result in abuses, particularly in countries where rule of law challenges are observed. The vague wording of various terms on the conditions of issuing detection orders under Article 7(6), as discussed in Chapter 4, is relevant for the proportionality assessment as it perpetuates the risk that the detection orders will be particularly wide in scope.

Requesting an opinion by the EU Centre is an important safeguard. However, as mentioned in Article 43, the opinion is meant to facilitate the detection order and it is unclear whether the opinion will have any meaningful impact on a potential withdrawal or amendment of the detection order.

Duration of the detection order

Moreover, according to Article 7(9), the detection order for known CSAM can last for 24 months. This is already a particularly prolonged period without any requirement for reassessment of the necessity. Besides, it can be renewed without specific limitations. In practice, it hereby amounts to permanent surveillance of the affected individuals (which may or may not be sufficiently identified as mentioned above).

New material

The proposed rules regarding obligations to detect new CSAM both to hosting providers and (all the more) to interpersonal communications providers disproportionately affect the right to privacy in terms of the group of users affected, which will amount to unlawful generalised monitoring and unlawful generalised surveillance. The CSA proposal is deemed disproportionate with regards to the following elements: insufficient targeted content, insufficient targeted group of users, technologies used in detection, the procedural safeguards regarding the issuance of detection orders and the duration of the detection order.

Targeted content and targeted group of users

While the detection of known content can be made specific with regards to the content to be detected, this is not the case for the detection of new material because the latter has not been categorised as CSAM before and, therefore, there are no exact identifiers (i.e., URL or hashes) available (see Chapter 3). To identify new material, technologies would have to be able to scan in a targeted way and would need to operate based on a set of clear indicators. As Chapter 3 shows, with today's available technologies, the parameters to detect new material cannot be made sufficiently specific. Therefore, by default the intrusiveness of the measures would be particularly heightened. These technologies would be 'scanning' and can, therefore, only be applied indiscriminately to all

[351] Does monitoring your phone affect the essence of privacy?, European Law Blog, accessed 9 March 2023; Abelson et al. 'Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications', Massachusetts Institute of Technology, 2015.

[352] Fact Sheet: Client-Side Scanning, Internet Society, September 2022, accessed 30 March 2023.

users of both hosting services and interpersonal communication services.[353] The fact that the detection orders must be issued by judicial authorities or by independent authorities as a safeguard is irrelevant, because the technology in itself cannot be targeted enough.

Given the above-described lack of precision with which new material can be detected, removed, and blocked on both internet access services, hosting services (and all the more) on interpersonal communication services, they fail the proportionality test with regarding to the right to private life in the form of confidentiality of communications. Thus, based on the technologies currently available and CJEU case law, the detection of new material would violate the prohibition of general monitoring obligations (for internet access services). For interpersonal communication services it would amount to unlawful generalised surveillance without limitations, exceptions or restrictions and without regard to communications that are safeguarded by confidentiality and secrecy (lawyer/client, communications in the medical field).

Requirements by the CJEU about the need for objective evidence revealing at least an indirect link with serious criminal offences cannot be complied with. As CSAM, while being a heinous crime, does not constitute a threat to national security, such generalised and indiscriminate monitoring is not justified. The case law of the CJEU concerns the processing of metadata, which, arguably, does not fully reveal the private life of users. However, in the case of content of interpersonal communications the proportionality concerns are significantly heightened due to the importance of the content for development and fulfilment of one's own personality, development of personal relations and the overall enjoyment of normal daily activities without the unwanted attention by others.

The above analyse also holds for removal and blocking orders as, similarly, the order cannot be made sufficiently specific.

Technologies to detect CSAM in open communication and E2EE

Furthermore, based on the findings in Chapter 3, the technology available for detecting new CSAM (classifiers and AI) cannot meet the standards of effectiveness, reliability and least intrusive nature in terms of impact on the users' rights, as mentioned in Article 10. The technology is significantly more prone to errors, which would have particularly serious repercussions for flagged users who may be implicated for a particularly stigmatising criminal offence and have their personal data of their communications reported.[354] Therefore, the means used for detecting new CSAM are insufficient and affect the proportionality of the proposed rules in this respect. For the detection of new CSAM in E2EE communications, the same limitations as described for the detection of known CSAM in E2EE communications apply.

Procedural safeguards

As for the proposed procedural safeguards laid down in Article 7, the proportionality concerns mentioned in connection to known CSAM are equally relevant here.

Grooming

The proposed measures concerning the issuance of detection orders on grooming constitute disproportionate interferences with the right to private life. They are deemed disproportionate with regards to the following elements: insufficient targeted group of users, technologies used in

[353] Report presented at expert workshop on EU's proposed regulation on preventing and combatting child sexual abuse, Leiden University, February 2023, p. 12.

[354] Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, The EDPB and the EDPS, July 2021, p 21.

detection, the procedural safeguards regarding the issuance of detection orders and the duration of the detection order.

Targeted content and targeted group of users

The complex nature of grooming entailing text or audio messages or even memes makes it extremely difficult to apply a set of specific indicators to detect, remove and/or block content (see Chapter 3). Thus, detection would extend by definition to all text-based (and possibly audio) communications that fall within the scope of a detection order which will be subject to automated analysis.[355] By contrast to the other two types of CSAM, it cannot be limited to specific content.

Hence, the requirements to be set to detect grooming would not be targeted enough and, thus, amount to by default generalised and indiscriminate automated analysis of all communications transmitted through interpersonal communication services.[356] The findings mentioned before in relation to new CSAM with regard to the lack of proportionality in terms of the users affected are equally relevant for the case of grooming. As CSAM, while being a heinous crime, does not constitute a threat to national security, such general monitoring of text-based communications is excessive to the aim pursued and the interference with the right to private life cannot be justified. This also holds for removal and blocking orders as, similarly, the order cannot be made sufficiently specific.

Technologies to detect CSAM in open communication and E2EE communications

Given the lack of reliable technologies (Chapter 3) that can be instructed to identify grooming accurately, the technologies will not be able to meet the requirements of effectiveness, reliability and least intrusive nature in terms of impact on the users' rights, as mentioned in the proposed Article 10. Moreover, even if technologies would be able to detect grooming accurately, they would require access to entire conversations, thus process even more personal data of the individuals flagged and acquire additional information on the private lives of the individuals. Such processing would raise additional proportionality challenges with regards to both the right to privacy and protection of personal data at the stage of human review.[357] For the detection of grooming in E2EE communications, the same limitations as described for the detection of known CSAM in E2EE communications apply.

Procedural safeguards

Furthermore, Article 7(3) foresees that when the need for a data protection impact assessment and a prior consultation procedure in accordance with the GDPR when the detection order concerns grooming. This safeguard cannot compensate for the particularly excessive automated analysis of all text-based communications in a generalised manner. Besides, there may be implementation challenges in practice with the timely preparation of an impact assessment. As for the conditions for issuing a detection order on grooming the lack of sufficient legal clarity and certainty on the language used ('appreciable extent', 'comparable service') is even more problematic in the case of grooming as it may lead to potential widely divergent interpretations and practices.[358]

---

355 Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, The EDPB and the EDPS, July 2021, p 21.

356 Report presented at expert workshop on EU's proposed regulation on preventing and combatting child sexual abuse, Leiden University, February 2023, p. 12.

357 Expert input by academics.

358 Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, The EDPB and the EDPS, July 2021, p 21.

Duration of the detection order

In connection to grooming the proposed rules attempt to compensate by providing a substantially lower duration of detection order for 12 months. However, even this period is particularly prolonged given the wide applicability to a particularly increased number of users and can be renewed without restrictions.

Main findings on the proportionality of the proposed measures obliging providers to detect, report and remove CSAM

Based on the above presented analysis, it can be concluded that measures affecting the content of interpersonal communications compromise the essence of the right to private life, irrespective of whether they concern known CSAM, new CSAM or grooming.

With regard to the detection of known material, there are proportionality concerns with respect to specification of the group of users whose communication would need to be screened on the dissemination of CSAM. In particular, for the detection of known CSAM, the CSA does not sufficiently require detection orders to be targeted. And, therefore, they will violate the prohibition against general monitoring obligations (for hosting services) and the prohibition on general data retention (for interpersonal communication services). Furthermore, proportionality concerns are raised in relation to the technology used regarding the detection of CSAM in E2EE communications, the procedural safeguards regarding the issuance of detection orders, including due to lack of clarity in the language used on the conditions of issuing detection orders and the duration of the detection order.

With the current state of technology for the detection of new CSAM, technologies would need to be used that would indiscriminately monitor content, thereby disproportionately affecting the right to privacy in terms of the group of users affected. This would amount to unlawful generalised monitoring and unlawful generalised surveillance of the content of interpersonal communications. The other proportionality concerns that apply to the detection of known CSAM also apply to the detection of new CSAM.

Similarly, the requirements for detecting grooming would not be targeted enough and, thus, amount to generalised and indiscriminate automated analysis of all communications (including texts and potentially audio messages as well) transmitted through interpersonal communication services, which disproportionately affects the right to private life in the form of confidentiality of communications. The proposed procedural safeguards cannot compensate for the excessive interference with the right, as they are ill-worded and may be ineffective. The other proportionality concerns that apply to the detection of known CSAM also apply to the detection of grooming.

6. Review of the cost-benefit analysis for the creation of the EU Centre to prevent and counter child sexual abuse

Answer to the corresponding research question in brief

Reviewing the cost-benefit analysis of the European Commission, and complementing it if necessary, what would be the preferred option among the three retained options for an EU Centre to prevent and counter CSA: a stand-alone agency, a centre attached to Europol, or a centre attached to the Fundamental Rights Agency?

(1) This study concludes that the cost estimates in the CSA proposal IA are rather detailed and considered of high quality. The CSA proposal IA presents a detailed breakdown of the annual costs into components, allowing for a good understanding of the main driver(s) of costs and differences between options. When it comes to the assessments of the benefits, the provided explanations are deemed valid by the researchers. The drawn assumptions on the quantification of benefits are insufficiently explained, in particular where the CSA proposal IA considers the perceived difference in benefits per option.

(2) The researchers, therefore, are of the opinion that the cost-benefit analysis has some shortcomings. The main shortcoming identified lies within the (quantitative) estimation of benefits for the different options, as a justification for the adopted estimates is largely missing. A second shortcoming is identified within the cost estimates. Although the cost breakdown is detailed, the researchers are of the opinion that the CSA proposal IA overestimates some of the costs that are incurred in Option C (EU Centre attached to Europol). A third shortcoming concerns the expected time it takes for the Centre to become fully operational. On several occasions the CSA proposal IA seems to argue that some implementation choices can be fully operational quicker than others, but this is not reflected in the cost or benefit calculations. Finally, taking into account the assumptions made in the CSA proposal IA, it seems that some (small) calculation errors were made concerning the quantitative assessment of benefits.

(3) The researchers attempted to correct these issues. Some cost elements within Option C have been altered slightly by the researchers. Furthermore, the researchers assumed a different implementation time per option, thereby assuming that some options are fully operational earlier than others. Finally, the researchers consider the options to have smaller differences in terms of expected benefits, than presented in the CSA proposal IA.

(4) This study concludes that Option C has the highest net present value and is therefore considered to be the most efficient option and consequently the preferred option. This is different to the conclusion reached in the CSA proposal IA, in which Option B (stand-alone agency) was found to be the preferred option. The main reason for this difference is that the researchers expect Option C to have a quicker implementation time, with the benefits expected to materialise earlier than in other options. In the calculations, the quicker implementation time for Option C outweighs the perceived inefficiency from having the Centre scattered over two entities.

(5) The researchers note that differences in costs and benefits between options are small. Moreover, certain aspects could not be quantified and expressed in monetary terms. Factors associated to independence, institutional culture and the signalling function of the EU Centre (i.e., that the EU takes the matter seriously) can hardly be captured in a cost-benefit analysis. Finally, the study also notes that conducting a cost-benefit analysis of the EU Centre in this study is challenging. The EU Centre would enable the impact of other policy measures within the initiative. As such, the EU Centre's benefits depend on the actions of other stakeholders, such as the ability of service providers to detect CSAM, the prosecution of offenders and the adoption of new policies to combat CSA at the Member State level.

6.1. Introduction

This study critically reviews the cost-benefit analysis in the CSA proposal IA, with a particular focus on Chapter 7, Annex 4 and Annex 10. Annex 4 consists of the analytical methods that were used to assess the impact of measures and options, in terms of costs and benefits. For the assessment of Measure 3 (EU Centre on prevention and assistance to victims and combating CSA online), Annex 4 of the CSA proposal IA refers to Annex 10 of the CSA proposal IA for a detailed analysis.

Before further detailing the findings of the critical review of the cost-benefit analysis, it should be noted that the researchers did not have access to all underlying files and information that were used for the CBA calculations by the European Commission. Therefore, the review of the CBA mainly relies on a review of the (openly) accessible sources in the CSA proposal IA, such as a study conducted by ICF[359], additional desk research[360] and written feedback received from Europol.[361]

The researchers were not able to obtain all the data relevant to validate the cost figures as presented in the CSA proposal IA. Data sources and calculations used for the assessments were not shared and from the CSA proposal IA is not always clear which sources were used for the exact specification of each cost category. As a result, the full operational costs of the Centre could be validated, but its breakdown into the different cost components (in particular when resources are shared by two entities in Option C) could not. Also, the justification for drawn assumptions is sometimes missing, in particular where it concerns the (quantitative) assessment of the benefits. Therefore, the focus of this assessment is the extent to which differences in costs and benefits between options, and their timing, can be explained.

[359] Study on options for the creation of a European Centre to prevent and counter child sexual abuse, including the use of ICT for creation of a database of hashes of child sexual abuse material and connected data protection issues (Final Report V2.0), ICF, 2021.

[360] Carr, J., 'Mechanisms for collective action to prevent and combat online child sexual exploitation and abuse', 2019; Edwards et al. 'Cyber strategies used to combat child sexual abuse material', 2021; Guerra, E., and Westlake, B., 'Detecting child sexual abuse images: Traits of child sexual exploitation hosting and displaying websites', 2021.

[361] The researchers invited Europol and FRA to reflect on some assessments made within the CSA proposal IA. Europol did not consider itself to be in the position to provide their (detailed) views on the assessment of costs and benefits. FRA kindly declined to respond. Thereby, the provided answers did not yield additional evidence or insights.

6.2. Objectives and activities of the EU Centre

The CSA proposal aims to establish an EU Centre to prevent and counter child sexual abuse (the EU Centre). This EU Centre would serve as an essential facilitator for the implementation of the obligations imposed on providers.

The CSA proposal lists the following specific objectives for the EU Centre:

(19) Help ensure that victims are rescued and assisted as soon as possible, and offenders are brought to justice by facilitating detection, reporting and removal of CSA online.

(20) Support Member States in putting in place usable, rigorously evaluated and effective prevention measures to decrease the prevalence of CSA in the EU.

(21) Support Member States to ensure that victims have access to appropriate and holistic support, by facilitating efforts at EU level.

The EU Centre would support providers of information society services by:

(22) Providing them with a database of CSAM indicators to detect (known and new) CSAM and grooming in their services (under the preferred option as laid down in the CSA proposal IA);

(23) Providing them with (free-of-charge) detection tools. The support of the EU Centre would in particular be useful to small and medium enterprises, which would also be subject to requirements concerning the mandatory detection of CSAM and grooming;

(24) Reviewing the reports submitted by providers of information society services to ensure accurate reporting to LEA (identify false positives).

By doing so, the EU Centre would avoid the duplication of efforts on the side of providers of information society services. Also, the establishment of an EU Centre ensures that (only) online (known) CSA verified by courts or independent administration authorities of Member States is detected by providers of information society services. For new CSAM and grooming, it would ensure that a method for the detection of new CSAM and grooming is established, and that this system is based on EU rules. As such, it would prevent over-reporting (false positives) or underreporting by providers of information society services and thereby ensures efficient reporting. Finally, by reviewing the reports submitted by providers of information society services, it would ensure that only actual CSAM is forwarded to LEA at the national level. The added value of the EU Centre in this respect is to ensure that CSAM is adequately detected by providers of information society services and that offenders can be held accountable ("detection, reporting, and removal" - specific objective 1).

The EU Centre would support Member States by:

(25) Helping to implement the relevant provisions via the organisation of expert workshops and;

(26) Acting as a hub of expertise to support the development of evidence-based policy associated with CSA at the national level through helping to develop and disseminate research and expertise and;

(27) Facilitating dialogue among stakeholders.

By doing so, it would avoid duplication of efforts, thereby reducing costs at the Member State level, in particular concerning implementation costs and the costs for knowledge building on the combat against CSAM. The role of the EU Centre in this respect would be to prevent CSA from taking place, through efforts at the Member State level ("prevention"- specific objective 2). The EU Centre would support victims by:

(28) Acting as a hub of expertise to support the development of evidence-based policy associated with the assisting victims, by helping to develop and disseminate research and expertise, and by facilitating dialogue among stakeholders;

(29) Setting up an online platform where victims can find information on support resources that are available to them in their area or online;

(30) Requesting providers of information society services to remove (known) CSAM from their platform and refer to national authorities for actions if CSAM is not removed.

By doing so, the EU Centre would reduce the harm of CSAM to victims, as victims are better assisted and known CSAM would be removed in a more effective manner ("victim assistance" - specific objective 3).

As the Centre's main role in the initiative would be to support other stakeholders affected by it, the EU Centre is considered to be an 'enabler' of the impacts that materialise from other measures (in which, for example, providers of information services are required to look actively for CSAM on their platforms). As such, the cost and in particular the benefits of different implementation choices are deduced from the extent to which different implementation choices for the EU Centre can effectively carry out the activities mentioned above.

6.3. Retained implementation options

In the CSA proposal IA, the European Commission has analysed several possible options for an EU Centre. Eventually, the European Commission assessed four options in more detail, as these were deemed the most feasible ones. However, only the functions within Option B to D would serve the required needs of the preferred policy option within the CSA proposal IA, as the Centre within option A would not have a function in CSAM detection. Thereby, the focus of the researchers is on the following three retained options:

1. An EU Centre as an independent EU body (*decentralised agency*) (Option B);
2. An EU Centre with some functions in Europol and others in an independent organisation under Member State law (*Europol+*) (Option C);
3. An EU Centre within the Fundamental Rights Agency (*FRA integrated*) (Option D).

Table 5 presents a comparison of the three options regarding the function of the EU Centre (that are directly linked to its specific objectives (SO) listed above), the legal status, funding as well as the governance structure. For Option C, a breakdown between the part integrated within Europol and the part organised as a separate entity is made.

Table 5: Comparison of legislative options for the EU Centre

Option	Option B **(preferred in CSA proposal IA)**	Option C		Option D
Set-up	Self-standing, independent EU Body	EU Centre with some functions at Europol	Independent organisation under Member State law	EU Centre set up within the FRA
Functions	Prevention (SO2) and victim assistance (SO3) + Detection, reporting and removal of CSA online (SO1)	Detection, reporting and removal of CSA online (SO1)	Prevention (SO2) and victim assistance (SO3)	Prevention (SO2) and victim assistance (SO3) (currently project basis) + Detection, reporting and removal CSA online[362] (SO1)
Legal status	Own legal personality, decentralised EU agency	Europol Regulation	Own legal personality under a Member State's law	FRA regulation
Funding	DG HOME, additional funding from other sources such as MS, Not-for-Profit donors, and private sector (no Conflicts of Interest)	Europol budget, additional funding from other sources such as MS, Not-for-Profit donors, and private sector (no Conflicts of Interest)	EC, ISF grant, additional funding from other sources such as MS, Not-for-Profit donors, and privacy sector (no Conflicts of Interest)	FRA budget
Governance	EC governance	Current Europol governance	Determined by legal personality under Member State's law, involve EC and relevant stakeholders	Current FRA governance, additional mechanism to involve relevant stakeholders

Source: Ecorys

6.4. Review of costs

6.4.1. Assessment of costs in the CSA proposal IA

The costs for each of the three options can be broken down into two main cost categories: (i) the initial investment costs to set up the EU Centre and (ii) the annual recurring cost.

The *initial investment costs* in turn can be broken down into two cost elements (a) costs related to creating the databases and indicators and (b) housing costs.

(31) The costs for creating the databases and indicators are estimated to be similar for all options and are derived from a study conducted by ICF.[363] The investment costs are estimated at € 1.59 million, with a margin of error of 50 to 100%.[364] As the costs for this factor are estimated at € 3

[362] Note: expanding FRA's legal basis needed.

[363] Study on options for the creation of a European Centre to prevent and counter child sexual abuse, including the use of ICT for creation of a database of hashes of child sexual abuse material and connected data protection issues (Final Report V2.0), ICF, 2021.

[364] Ibid., p. 68.

million, the estimate is deemed conservative by the researchers (not underestimating the costs).

(32) The housing costs differ between the three options. For Option C, a distinction is made between the housing costs for the part that will be integrated within Europol and the part that is established as a separate entity. The estimate for housing costs is based on assumptions.

Table 6 presents the total initial costs per option.

Table 6: Overview of total initial investment costs per option in million Euro (year 1)

	Option B: Decentralised agency	Option C: Europol+	Option D: FRA integrated
Databases + indicators costs	3	3	3
Housing costs	2	1	1
Additional housing costs	-	1	-
Total costs	5	5	4

Source: CSA proposal IA

The *annual costs* can be broken down into three main cost categories (a) staffing expenditure, (b) infrastructure expenditure and (c) operational expenditure. These costs, in particular the total annual costs per year, are based on budgets of similar organisations in the EU and outside of the EU. However, the researchers found no clear justification for the costs associated to particular expenditures (such as operational expenditures).

For all options, the CSA proposal IA assumes it would take two years to set up an EU Centre and up to four years for the EU Centre to reach its full size and capacity. During the start-up phase of the EU Centre, the annual costs increase gradually. From year five onwards the EU Centre is in full operation and annual costs remain the same. However, it appears that, in the calculations, the EU Centre would only be fully operational in year six within Option C. Again, for option C, these cost categories are assessed both for the part integrated within Europol and the separate entity. Table 7 presents annual costs per option assuming the EU Centre is fully operational.

Table 7: Overview of annual cost per option in million Euro (year 6)

	Option B: Decentralised agency	Option C: Europol+	Option D: FRA integrated
Staff expenditure (a)	15.9	14.5	13.9
Infrastructure expenditure (b)	3.2	3.6	3.2
Operational expenditure (c)	6.6	6.0	6.6
Total costs	25.7	24.1	23.7

Source: CSA proposal IA

The differences in staff expenditure (a) result from differences in costs for overhead. Within option B, the overhead costs are largest as all three functions (detection, prevention, and assistance to victims) would require dedicated overheads staff. In Option C, functions associated to prevention and assistance to victims would require dedicated overheads staff, but the overheads staff for 'detection, reporting, and removal' can benefit from the existing management structure in Europol and as such, fewer (new) overheads staff would be required. Within option D, the EU Centre can benefit from the FRA's overheads structure for all the functions, and as such, staff expenditure is lowest in this option.

The differences in infrastructure expenditure (b) result from the allocation of functions to different entities. As Option C consists of two different entities, the costs for auditing, administrative

expenditures, and movable property are incurred twice. As such, the costs of Option C would be higher than those of Option B and Option D.

The differences in operational expenditure (c) result from differences in the costs associated to operational activities (technical meetings with stakeholders) and support to expert networks (coordination activities, meetings). The costs associated with these activities are lowest in Option C, although no explanation is offered on the underlying reason. Possibly, these activities can be more easily embedded in existing activities by Europol: no new structure has to be set up. On the other hand, the costs for translation and interpretation, publishing, and research dissemination and communication (campaigns) are higher in Option C. Again, no explanation is given as to what drives this cost difference. Likely, this difference results from duplication of efforts between Europol and the separate entity.

6.4.2. Review of the cost estimation

Differences in initial costs, staff expenditure and infrastructure and operational expenditure between various options are considered reasonable by the researchers, who confirm initial costs as presented in the CSA proposal IA (presented in Table 6). It is logical that new entities require more overhead than embedding the EU Centre into an existing agency. The same applies to the costs for the building infrastructure and related expenditure. As a result, it seems reasonable that costs of embedding all functions of the EU Centre within an existing agency are lowest.

For the assessment of annual costs, there are doubts as to the accuracy of the operational expenditures (c). There seems to be no clear reason to assume that all activities associated to publishing and research dissemination are fully duplicated between the two EU Centres within Option C. The researchers consider the annual costs of Option C to be € 250,000 lower than as presented in the CSA proposal IA. A detailed explanation is included in Annex V. An overview of annual costs, as assessed by the researchers, is presented in Table 8.

Table 8: Overview of annual cost per option in million Euro (year 6)

	Option B: Decentralised agency	Option C: Europol+	Option D: FRA integrated
Staff expenditure (a)	15.9	14.5	13.9
Infrastructure expenditure (b)	3.2	3.6	3.2
Operational expenditure (c)	6.6	5.8	6.6
Total costs	25.7	23.9	23.7

Source: Ecorys

Furthermore, the researchers consider that the timing in which the EU Centre can be operational would differ between Options B, C, and D. In particular, Europol is already involved in obtaining information on CSAM from the US Department of Homeland Security Investigations, cross-checking these reports and forwarding them to different Member States. As a result, it already has some in-house expertise and might be able to conduct the required activities of the EU Centre quicker by offering better training for new staff. Also, as noted in the CSA proposal IA, cooperation frameworks with LEA already exist at Europol. In Options B and D, these have to be newly established.

Based on the development of staff over the years for existing EU Centres,[365] it was attempted to make an estimate of the time it takes for an agency to become fully operational. It would stand to reason that the staff employed by an agency increases in the first year after being established and at some point, reaches a certain level from which the number of staff remains more or less constant. From this year onwards, the analysis operates under the assumption that the agency has become

[365] FRA, CEPOL, EUROPOL, EMSA and EASA have been considered in this analysis.

fully operational. Details are provided in Annex V (Table 24). The derived implementation time per agency is offered in Table 9.

Table 9: Development of staff of five existing agencies

	Established in	Fully operational in	Staff in year where EU Centre is assessed fully operational
FRA	2007	2012	117
CEPOL	2005	2008	27
EUROPOL	1998	2005	536
EMSA	2002	2008	181
EASA	2002	2008	403

Source: Researchers' assessment based on Annual Reports from the European Court of Auditors (ECA)

From Table 9, it can be understood that the implementation varies per agency and is generally estimated at between 3 and 7 years. Typically, agencies that currently employ more staff take longer to reach a stable staffing level. Based on Table 9, it seems reasonable to assume that a new EU Centre would take five years to become fully operational. All new staff (and overheads) has to be sought, no expertise would be readily available at the EU Centre, all cooperation mechanisms with LEA at the national level have to be setup from scratch and no building structure currently exists. In short, the EU Centre would need to be entire newly established. This analysis further supports the assumed implementation time for Option B in the CSA proposal IA.

Under Option C, the EU Centre embedded in Europol would not be newly established. The implementation time is likely lower. For example, the mandate of EASA was changed in 2008. In the years following, the staff at EASA increased (from 333 in 2007 to 570 in 2010 and 574 in 2011). It took EASA some three years to fully become operational. It is therefore assumed that the functions of the EU Centre under Option C, embedded in Europol, would take three years to become operational.

This gives sufficient time to build the database on CSAM indicators, also providing that Europol already has existing databases with images, videos, and hashes, and also has experiences with hash lists it collects from other organisations. Also, three years would give sufficient time to provide a list of indicators of CSAM to providers of information society services. Functions established within the separate, newly established entity, mainly focusing on victim assistance and prevention, would also take three years to become operational. The staff that needs to be employed is similar to staff employed by CEPOL, which also took three years to become operational (also consider Table 9).

Similar to option C, the researchers assume that the EU Centre under option D, embedded in FRA, would take four years to become operational. This is slightly longer than under Option C. The reason for this is that no cooperation framework with national LEA currently exists and these would all need to be set up from scratch. However, when compared to Option B, and similar to Option C, the FRA already has building infrastructure and overhead staff. Thereby, it would take less time to become fully operational than under Option B.

6.5. Review of benefits

6.5.1. Assessment of benefits in the CSA proposal IA

Qualitative assessment

The CSA proposal IA considers in its qualitative assessment, the social and economic benefits associated to the establishment of the Centre, as well as its contribution to safeguarding fundamental rights.

The social benefits originate through a reduction in CSA(M). Through better policies at the Member State level and improved capacities of relevant public authorities to respond to cases of online CSA,

CSA can be better prevented. Furthermore, the reporting of CSAM by service providers would reduce the amount of online CSAM and helps LEA to ensure that offenders can be held accountable. Finally, the Centre would improve the assistance of victims of CSA and protection of children online by reducing the sense of impunity of offenders.

In terms of social benefits, the CSA proposal IA argues that Option B would have the largest impact, as all functions are embedded into one entity which can dedicate all its resources to combatting CSAM.[366] Also, the establishment of a dedicated agency has a signalling function and enhances visibility of EU efforts, sending a message that the EU is taking the matter seriously. If the Centre is embedded into other agencies (Option B and Option D), there is a risk that tasks associated to combatting CSAM are deprioritised.

The economic benefits mainly originate from an improved coordination of efforts. The CSA proposal IA argues that, against a baseline in which no Centre is established, a more efficient and coordinated system of handling the reports would likely lead to a net reduction of costs and necessary resources for each report for both service providers and LEA. This also holds for the database of CSAM indicators. Furthermore, the Centre could prevent duplication of efforts to combat CSA at the Member State level. By contributing to combatting CSAM, the Centre also allows for a reduction of economic costs associated to CSAM in the long run. This, for example, entails more efficient victim support service, better victim compensation programmes, lower unemployment levels among victims.

In terms of economic benefits, Option B and Option D seem to be favoured over Option C in the CSA proposal IA. The main reason for this is that the scattering of functions between different agencies within Option C might result in inefficiencies and the risk of working in silos.

The fundamental right benefits relate to the protection of children that are victim of CSA. Furthermore, it is also foreseen that the EU Centre would provide support in filtering reports in order to alleviate the burden on LEA. Finally, the creation of transparent and accountable process safeguards the protection of fundamental rights of internet users. The independence of the Centre is vital to sufficiently safeguard these rights.

In terms of fundamental rights impact, the CSA proposal IA argues that, overall, none of the options considered for the Centre would have any significant negative impact on any fundamental right. The analysis shows that the Centre's own impact is limited from a fundamental rights perspective, but that it serves as an important safeguard to ensure that the measures strike a fair balance between the different rights at stake.

However, the CSA proposal IA identifies a risk that providers would be reporting innocent persons to LEA directly if the EU Centre is partly established within Europol.[367] For Option D, the CSA proposal IA argues that in particular functions associated to detection, reporting, and removal of CSAM requires a significant change in the setup of FRA, as it would require an 'active' role of FRA. At this point, the main focus of FRA is helping policy makers by collecting and analysing data and providing independent advice. There is a certain risk that FRA would become an active player in the field if the Centre would be embedded in this agency, instead of being an independent observer.
After the description of pros and cons, the CSA proposal IA scores the different options in a qualitative manner for comparison purposes, according to their effectiveness, efficiency (cost-

[366] Impact Assessment Report Accompanying the document Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, European Commission, May 2022, pp. 350-352.

[367] Ibid, Annex 10.

benefit assessment) and coherence. Option B scores highest in terms of effectiveness and benefits, with +++, and Options C and D both have a score of ++.[368]

Quantitative assessment

The quantification of benefits within the CSA proposal IA is conducted based on the estimated reduction of CSAM costs that are attributed to the EU Centre. The estimation was done based on the qualitative scores on effectiveness. The scores on effectiveness are closely linked to the qualitative assessment of the social benefits. The CSA proposal IA, for comparative purposes, assumes that each '+' in the assessment of effectiveness is associated with a reduction of CSAM costs by 3%, thereby suggesting that Option B is expected to reduce CSAM costs by 9% and Options C and D by 6%.

As the costs of CSAM at the EU level are estimated at € 13.8 billion per annum[369], the yearly benefits are estimated at € 1.24 billion in Option B and € 0.83 billion[370] in Options C and D per year. A detailed overview is presented in Table 10.

Table 10: Overview of the benefits per option as estimated in the CSA proposal IA (year 6)

	Option B: Decentralised agency	Option C: Europol+	Option D: FRA integrated
Reduction in CSAM costs	9.0%	6.0%	6.0%
Benefit in millions of €	€ 1,242.0	€ 828.0	€ 828.0

Source: CSA proposal IA (corrections made by researchers)

6.5.2. Review of the benefit estimation

Qualitative assessment

The researchers agree with the three different identified benefits in the CSA proposal IA, which originate from the Centre, being a social, an economic and a fundamental rights benefit. The researchers have has not identified other benefit categories that originate from the creation of a Centre.

The social and economic benefits mainly materialise from the ability of the Centre to combat CSAM. On top, there is an additional economic benefit from the creation of the Centre as it improves coordination and prevents a duplication of efforts. Finally, the CSA proposal IA discusses some issues associated to fundamental rights.

Ability of the Centre to combat CSAM and reduce associated CSAM costs

In terms of its ability to combat CSAM, the researchers consider small differences between the different options. The researchers agree with the CSA proposal IA that Option C is considered less effective as functions are scattered between two entities. When considering the ability of the Centre to fulfil the specific objectives listed for the Centre, all aimed at combatting CSAM, the following small differences between options are observed by the researchers.

In terms of detection, reporting, and removal of CSAM (SO1), the EU Centre in all implementation choices is assigned with the same task. The researchers consider that there is a benefit associated to

[368] Ibid., p. 371.

[369] In Annex 4 of the CSA proposal IA, a cost of € 13.5 billion is also mentioned. This is considered to be a mistake, as in various other parts of the report, the costs are estimated at € 13.8 billion.

[370] According to calculations by the researchers, the cost reduction should equal € 0.83 billion and not € 0.89 billion as presented in the CSA proposal IA for Option C and D and equal € 1.24 billion in option B and not € 1.23 billion as presented in the CSA proposal IA. There seems to be an error in the calculations conducted within the CSA proposal IA.

the in-house expertise with reporting of CSAM that already exists within Europol, which nowadays receives, cross-checks and enrich reports obtained from NCMEC. Thereby, the researchers consider that new staff can be trained by experts that already have expertise in cross-matching and enriching reports. Thereby, the researchers consider that Option C might be able to carry out this function more effectively. On the other hand, the signalling function of embedding the Centre within an existing agency might be somewhat lower, favouring option B. Thereby, the ability to fulfil this specific objective is assessed to be (slightly) bigger in Option B and Option C. However, the expected differences between the different options are likely negligible.

In terms of prevention (SO2), by providing Member States with support to implement evidence-based policy concerning the prevention of CSA, all implementation choices are assigned with the same task. In Options B and C, these tasks are performed by a dedicated entity and in Option D this task is performed by FRA. This might limit the focus of FRA on CSAM-related matters, but at the same time, this activity fits well with their current role of providing input for policy makers. It is expected that these two effects balance out. As such, all Centres are considered to be equally effective in carrying out this function.

In terms of victim assistance (SO3), Option B and Option D are considered equally effective. All functions are embedded within the same organisation. In Option C, CSAM removal is located in both the separate entity as within Europol. The hotline, through which victims can request removal of CSAM, is located in the separate entity. This entity has to forward the request to Europol, which then requests providers of information society services to remove the material from their platform. This might make Option C slightly less able to effectively assist victims. In this assessment, it is expected that Option C is somewhat less able to fulfil its function related to 'victim assistance' than in Options B and D.

Concluding, the researchers see no clear differences in the expected benefits associated to the ability of the Centre to fulfil SO1 and SO2. For SO3, the benefits under Option C are likely lower than under the other options as the function is scatted between two entities. Thereby, this study concludes that the social and economic benefits, indicated by a reduction in CSAM costs, of Option C are lower than the benefits under Option B and D.

Ability of the Centre to enhance coordination and prevent duplication of efforts

The researchers follow the CSA proposal IA and consider that all implementation choices contribute to an improved coordination and prevent the duplication of efforts. However, in order to enhance coordination, knowledge sharing and a fruitful cooperation between the different actors involved in combatting CSAM, activities are required by the Centre (for example in terms of knowledge sharing, coordination meetings, etc.). A closer look at the operational costs associated to the Centre reveals that the expected costs for these activities are lower in Option B than in Option C and Option D. When the Centre (in Option C) needs to invest fewer time in these activities, a lower burden is also placed on other actors affected by the initiative (such as Member States that need to attend the meetings or coordination activities with service providers).

Concluding, there seems no clear difference between options in their ability to enhance coordination and prevent duplication of efforts. Thereby, the economic benefits associated to improved coordination are equal in all options. However, the researchers note that Option C is expected to conduct activities associated to improving coordination most efficiently.

Ability of the Centre to safeguard the protection of fundamental rights

In terms of fundamental right benefits, The CSA proposal IA argues that, overall, none of the options considered for the Centre would have any significant negative impact on any fundamental right. The analysis shows that the Centre's own impact is limited from a fundamental rights perspective.

However, the CSA proposal IA discusses some specific risks that should be taken into consideration in the assessment of the preferred option.

It considers that, when a Centre is established within Europol, providers that detect CSAM directly report to LEA. When the reported case concerns a false positive, providers report innocent people to LEA, which might negatively impact their fundamental rights. This would be an unintended consequence of hosting the Centre (partly) within Europol. [371]

The researchers consider that this unintended consequence will not materialise. Europol officers never arrest citizens or instigate investigations. As such, innocent people are not directly investigated when a false positive case is reported to Europol. Also, the researchers consider that Europol has no incentive to forward false positives to national LEA. Europol already works closely with national LEA and is therefore likely (best) aware of capacity issues at the Member State level. In order to maintain its relations with national LEA as well as possible, Europol would likely be hesitant in providing national LEA with cases that are non-actionable and is thereby likely quite cautious in forwarding non-actionable reports.

A second risk that the CSA proposal IA identifies lies within embedding the agency within FRA. The risk that embedding the function within FRA might result in the agency becoming an active player in the field is reckoned by the researchers. However, the researchers consider that this potential risk is offset by the expertise of FRA in safeguarding the protection of fundamental rights when the Centre would be embedded in FRA. Thereby, the researchers see no clear difference in fundamental right benefits per option.

Considering the fundamental right impact, the researchers are of the opinion that the implementation choices do not significantly differ from another.

Assessment of benefits by the research team

Concluding, the view expressed in this study, based on the explanations offered in the CSA proposal IA, is that there are very small differences in the benefits between the different options. The CSA proposal IA provides no clear indication why one option would have sufficiently more benefits than another option. The researchers do agree that Option C, in which the functions (in particular victim assistance) of the EU Centre are split between two entities, is likely somewhat less able to achieve the social and economic impact, due to a risk of the two entities working in silos.

Quantitative assessment

The quantitative assessment of benefits per option in the CSA proposal IA is offered for comparative purposes. No explanation is offered for the 3% reduction per '+'. It is noted that, in general, it is necessary to be very careful in counting pluses and argue proportionality. The pluses are meant for comparative purposes ("Option B is more effective than Options C and D") and are not meant to say anything about the magnitude. Hence, one cannot conclude that Option B is 50% more effective than Options C and D based on the number of pluses.

As mentioned under the qualitative assessment, the researchers see no clear reason why the benefits per choice would differ much from another. The only significant difference in terms of perceived effectiveness is the ability of Option C to effectively carry out the task under SO3. Activities associated to this objective are scattered between the two entities, which makes option C somewhat less effective when compared to Option B and D.

As no information is available to express the effectiveness in terms of a reduction in CSAM cost, it will be assumed that Options B and D are both able to reduce CSAM costs with 6%. For Option C,

[371] Ibid., 62.

the effectiveness is assessed to be slightly below 6% as this Option is somewhat less effective in victim assistance, since this function of the EU Centre would be scattered between two entities.

In order to derive a quantitative estimate for Option C, it is assumed that each (operational) staff member employed by the EU Centre is equally contributing to reaching the benefit by the Centre. When only considering operational staff, 78% of the Centre's staff would be dedicated to 'detection, reporting and removal'. The other functions (prevention and assistance to victims) both cover 11% of the operational staff needed. These ratios are applied to the total benefit offered by the EU Centre (6% reduction in CSAM costs) to estimate the benefit that results from activities to achieve SO3 within Option B and D. As Option C is assessed to be slightly less effective in reaching SO3, the found impact of Option D and B was multiplied with 0.5 to obtain the impact of activities to reach SO3 for Option C (indicating that Option C is assumed to be 50% less effective in carrying out this function than Option B and D). The effectiveness of Option C is thereby assessed at 5.7%.

As a result, the following effectiveness percentages are obtained once the EU Centre is fully operational (Table 11). It is conservatively assumed that, prior to the EU Centre becoming fully operational, there are no benefits to be derived from the EU Centre.

Table 11: Overview of the benefits per option as estimated by researchers (year 6)

	Option B: Decentralised agency	Option C: Europol+	Option D: FRA integrated
Reduction in CSAM costs	6.0%	5.7%	6.0%
Benefit in millions of €	€ 828.0	€ 782.0	€ 828.0

Source: Calculations by researchers based on the values provided in the CSA proposal IA.

The quantification of benefits only concerns the extent to which the Centre is able to reduce the societal costs associated to CSA. Factors associated to independence, institutional culture and the signalling function of the EU Centre (i.e., that the EU takes the matter seriously) can hardly be captured in a cost-benefit analysis. As a result, these factors should be considered in addition to the assessment of the monetary benefits in Table 11.

6.6. Review of the cost-benefit analysis

6.6.1. Calculation of the present value of costs

The researchers consider that the cost-benefit analysis for the EU Centre, conducted within the CSA proposal IA, does not strictly follow the requirements for a CBA, as laid down in Tool #63 of the Better Regulation Guidelines. The costs and benefits within the CSA proposal IA are not properly expressed over time and are not 'discounted' to one year. As a result, no (accurate) net present value or benefit-to-cost ratio is provided in the CSA proposal IA. Based on the values indicated in the CSA proposal IA, the researchers calculated the present value the costs and benefits over a ten-year period (which is also the time horizon mentioned in Annex 4 of the CSA proposal IA).

For each of the three options, the present value is calculated. It is assumed that all investment costs (associated to the database and housing) are incurred in year one. The results are presented in Table 12. Detailed calculations are offered in Annex V (Table 25 and Table 27).

Table 12: Overview of total costs per option in million Euro based on the estimates in the CSA proposal IA (in present value year 1 – year 10)

	Option B: Decentralised agency	Option C: Europol+	Option D: FRA integrated
Total costs in present value	184.3	174.2	171.9

Source: Calculations by researchers based on the values provided in the CSA proposal IA.

Based on the assessment of the costs, Option D seems to be the most attractive option as the total costs of this option are the lowest. However, it also seems that all options have fairly similar costs. The most expensive option (Option B) is only 7.2% more expensive than the least expensive option (Option D). In the bigger picture of drawn assumptions and uncertainty, the different implementation choices do not significantly differ in terms of costs.

As noted in Section 6.4, the researchers consider a different implementation time per option and have corrected the costs for publishing and research dissemination within Option C. As a result, the cost estimates of the researchers, and its present value, differ from the cost estimates as presented in Table 12. Based on the revised values, the present value is calculated, for each of the three options. The results are presented in Table 13. Detailed calculations are offered in Annex V (Table 25 and Table 27).

Table 13: Overview of total costs per option in million Euro based on estimates from the researchers (in present value year 1 – year 10)

	Option B: Decentralised agency	Option C: Europol+	Option D: FRA integrated
Total costs in present value	184.3	194.3	182.6

Source: Calculations by researchers based on the values provided in the CSA proposal IA.

When comparing the present value in Table 13 with the present value in Table 12, it can be observed that the total costs for Options C and Option D have increased. The main reason is that the EU Centre is operational sooner in Options C and D and as such, full staff expenditures are already incurred earlier in time (and run for more years). In quantitative terms, this means that more costs are incurred in the first years. However, when all hypothetical EU Centres are fully operational, the annual costs under Option B would still be highest. Finally, it could be noted that the total cost for the different implementation choices have further converged, and that the most expensive option (Option C) is 6.4% higher than Option D, which is still the least expensive option.

6.6.2. Calculation of the present value of benefits

Just as for the costs, the CSA proposal IA does not provide the present value of the benefits. Based on the values indicated in the CSA proposal IA, the researchers calculated the present value of the benefits over a ten-year period. It is assumed that the benefits only originate after the EU Centre has become fully operational. Based on the values provided in the CSA proposal IA, the present value of benefits is calculated by the researchers in Table 14. Detailed calculations are offered in Annex V (Table 26 and Table 28).

Table 14: Overview of the benefits per option in million Euro based on the estimates in the CSA proposal IA (present value year 1 – year 10)

	Option B: Decentralised agency	Option C: Europol+	Option D: FRA integrated

Total benefits (in present value)	5,977.9	3,985.3	3,985.3

Source: Calculations by researchers based on the values provided in the CSA proposal IA.

As noted in Section 6.5, the researchers consider a different implementation time per option and proposes a different method to estimate the benefit. As a result, the benefit estimates of the researchers, and its present value, differ from the benefit estimates as presented in Table 14. Based on the revised values, the present value is calculated, for each of the three options. The results are presented in Table 15. Detailed calculations are offered in Annex V (Table 26 and Table 28).

Table 15: Overview of total benefits per option in million Euro based on estimates from the researchers (in present value year 1 – year 10)

	Option B: Decentralised agency	Option C: Europol+	Option D: FRA integrated
Total benefits (in present value)	€ 3,985.3	€ 5,174.3	€ 4,720.9

Source: Calculations by researchers based on the values provided in the CSA proposal IA.

From Table 15, it can be deduced that the highest benefits materialise in Option C. This is because the EU Centre would already be operational in year 3. Closely following is Option D. The EU Centre within FRA would become operational in year 4 and therefore the benefits (in terms of a reduction in CSAM costs) is only experienced one year later. However, the annual benefits are slightly higher in this option, as it is more effective in victim assistance than Option C (also consider the benefits for year 6, as presented in

Table 11). The lowest benefit is experienced within Option B, as it would the longest time for this EU Centre to become fully operational.

6.6.3. Calculation of the net present value

Table 16 provides the costs and benefits (expressed in present value) as well as the Net Present Value[372] for the cost and benefit estimates as presented in the CSA proposal IA. The (net) present value calculations are performed by the researchers.

Table 16: Overview per option in million Euro based on the estimates in the CSA proposal (in present value year 1 – year 10)

	Option B: Decentralised agency	Option C: Europol+	Option D: FRA integrated
Total costs	184.3	174.2	171.9
Total benefits	5,977.9	3,985.3	3,985.3
Net present value (NPV)	5,793.6	3,811.0	3,813.3

Source: Calculations by researchers based on the values provided in the CSA proposal IA.

Based on the value calculated by using the values of the CSA proposal IA, Option B provides the highest net present value.

[372] The net present value is the difference between the benefits and the costs in present values, See Better regulation toolbox, European Commission, tool #64, p. 558.

Table 17 provides the costs and benefits (expressed in present value) as assessed for this study for the various options in the CSA proposal IA.

Table 17: Overview per option in million Euro based on estimates from the researchers (in present value year 1 – year 10)

	Option B: Decentralised agency	Option C: Europol+	Option D: FRA integrated
Total costs	184.3	194.3	182.6
Total benefits	3,985.3	5,174.3	4,720.9
Net present value (NPV)	3,800.9	4,980.0	4,538.3

Source: Calculations by researchers based on the values provided in the CSA proposal IA.

Based on the value calculated by using the values of the CSA proposal IA (Table 13), Option B provides the highest net value.[373] According to the assessment by the researchers (Table 14), Option C provides the highest net value. This is mainly because the researchers expect the EU Centre within Option C to be fully operational quicker.

However, the researchers note that differences in costs and benefits between options are expected to be small. All options are able to carry out the required functions of the Centre, although some options are expected to become fully operational earlier in time and/or benefit from existing (building) infrastructure and overhead. Other considerations, for example concerning the signalling function, the independence of the Centre and the ability to safeguard the protection of fundamental rights are difficult to (quantitatively) reflect in the cost-benefit analysis.

6.6.4. Sensitivity analyses

As the estimates were derived by making assumptions, it is good practice to conduct some sensitivity analyses. Three sensitivity analyses were conducted by the researchers. The first analysis concerns the implementation period. Different implementation periods per option were assumed. In this sensitivity analysis, the implementation time of options follows the assumption in the CSA proposal IA. The sum of costs and benefits than favours Option D, closely followed by Option B (net value of € 3,813.3 million in Option D versus € 3,800.9 million in Option D and € 3,591.2 million in Option C)**.** In this sensitivity analysis, the total benefits of Option B and D are equal, but Option D is somewhat less costly to implement. The total benefits of Option C are smaller than the total benefits of Option B and D, due to its limited effectiveness in terms of victim assistance. Details are provided in Annex V (Table 29, 30, 31, 32 and 33).

The second analysis concerns the added value of each function of the Centre. It was assumed that, based on the number of staff employed by the Centre, the detection, reporting, and removal function of the EU Centre is contributing most to combatting CSA. In this analysis, it will be assumed that each function is equally important. The sum of costs and benefits then favours Option D (net value of € 4,538.3 million in Option D versus € 3,800.9 million in Option B and € 4,371.2 million in Option C). This sensitivity analysis only affects the benefits of Option C, as this sensitivity analysis assumes that all functions of the EU Centre are all equally contributing towards reducing the costs of CSAM. In the main analysis (Table 14), it was assumed that, based on the number of operational staff, the function detection, reporting, and removal was the main driver behind the benefits of the Centre. Details are provided in Annex V (Table 34, 35, 36, 37 and 38).

[373] Impact Assessment Report Accompanying the document Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, European Commission, May 2022.

The third analysis concerns the assessment period of costs and benefits. In the main analysis (Table 14), the costs and benefits are assessed over a period of ten years. However, in many other IAs, costs and benefits are considered over a longer period. In this sensitivity analysis, the costs and benefits of the various options are assessed over a twenty-year period. All costs and benefits are assumed to remain constant in year 11 to year 20, at the level of year 10. The sum of costs and benefits still favours option C (net value of € 9,792.1 million in Option C versus € 8,893.4 million in Option B and € 9,643.4 million in Option D). This sensitivity analysis increases the costs and benefits for all options, as costs and benefits are studied over a longer period. Also, the added value of having the EU Centre operational earlier in time becomes somewhat less important and the slightly lower impact of Option C on CSAM costs become somewhat more important. However, even over a twenty-year assessment period, the analysis still favours Option C, as the EU Centre can be operational quickest. Details are provided in Annex V (Table 39, 40, 41, 42 and 43).

7. Conclusions

This chapter provides overarching conclusions gathering all of the findings given above. Before presenting the key conclusions in more detail, it must be underlined that **the need to protect children against CSA is undisputed, and that this study does not question this principle**. At its core lies the achievement of a balance between protecting children and safeguarding the fundamental rights of users of covered online services under the EU Charter of Fundamental Rights. It is from this perspective that this research was conducted. Furthermore, it is stressed that the study at hand is not a fully-fledged Impact Assessment, but rather focuses on specific elements of the CSA proposal, as requested by the LIBE committee.

Combining the above findings allows us to assess the effectiveness and efficiency of the CSA proposal in addressing the identified problem (i.e., part of research question 1). It can be concluded that the overall effectiveness of the proposed legislation is expected to be limited. This is due to a variety of factors, including:

a) a problem definition that reasons that fragmentation across Member States' legal frameworks results in challenges in cooperation between public authorities and service providers, thereby negatively impacting the internal market, without sufficiently clarifying this causal effect;

b) the fact that the proposal targets known content, new content, and grooming, while the technologies to detect new content and grooming are of low accuracy (compared with the technologies to detect known CSAM). While expert's views on the impact of deploying such technologies differs, a majority of experts consulted predict that this will result in an increase of reported content and a reduction in accuracy, thereby substantially impacting the workload of LEAs. In a further factor;

c) perpetrators that are keen to continue their activities will likely resort to the dark and deep web, where identification is more complicated;

d) besides the fact that the detection of CSAM in E2EE raises fundamental issues with regards to the secure nature of E2EE, it also creates vulnerabilities for users of E2EE communication channels;

e) weighing all the fundamental rights affected, it can be concluded that the CSA proposal would violate the prohibition on general data retention and the prohibition against general monitoring obligations. While the proposal would generally benefit the protection of children (i.e., rapid identification and take-down of material, reduce risks of re-victimisation and better protect against grooming), the proposal would interfere with the fundamental rights of users of these services;

f) the establishment of an EU centre would positively impact the effectiveness of the combat against CSAM.

Given the expected limited effectiveness of the CSA proposal, it is difficult to draw solid conclusions with regards to its efficiency. Moreover, there is little insight on the ultimate results of the proposed legislation. Based on the available material, it can be concluded that the CSA proposal would result in efficiency gains in the fight against CSA. In particular, the decreased reliance on United States databases and services for the detection of CSAM would benefit efficiency. In addition, this study concludes that the establishment of an EU centre as part of Europol (rather than as a decentralised agency as per the preferred option in the CSA proposal IA), would also allow for improved coordination and collaboration. Although such benefits could also be observed for an EU centre in other shapes (i.e. as a self-standing agency or as part of the FRA), this set-up is expected to become operational faster and hence efficiency gains could be observed sooner.

The remainder of this chapter provides more detailed conclusions, supporting the overall conclusions on effectiveness and efficiency.

Problem definition

In regard to the problem definition in the CSA proposal IA, this study identifies several weaknesses. First, in the problem definition, the European Commission argues that fragmented legal frameworks across Member States negatively impact cooperation between public authorities and providers of information society services. However, having national legal frameworks in place might actually improve cooperation between public authorities and providers of information society services on the national level, rather than hamper it. Therefore, the strength of this argument is debatable. In addition, the problem definition argues that the fragmentation of legal frameworks across Member States also negatively impacts the internal market. The evidence to support this claim is found to be rather weak. Moreover, it can be questioned whether the fragmentation of legal frameworks across Member States can be considered as the driver that calls for the introduction of an EU-wide approach, or whether the actual problem driver is CSA.

The study also finds that the completeness of the problem assessment requires further strengthening. While end-to-end encrypted (E2EE) communication substantially impacts the detection of CSAM, the problem definition only addresses this element briefly. It does not mention this challenge in the problem tree and, therefore, no measure is designed to address this challenge directly.

Furthermore, the problem definition is weakened by contextualising quantitative data to a limited extent, by providing insufficient evidence for the persistence of the problem and by presenting stakeholder views to a limited extent.

Impact of the CSA proposal on the internet

The impact of the CSA proposal on the internet can be broken down into three types of impact, namely: (1) the impact on technology, (2) the impact on the quantity and quality of detection, and (3) the impact on the behaviour of providers of information society services, children, and users of online services. As the CSA proposal lays down that providers of information society services should detect known content, new content, and grooming, this distinction will be referred to below, where relevant.

With regards to the impact of the CSA proposal on technology, it can be concluded that only the detection of known CSAM on open communication channels can, at this point in time, be carried out with relatively high accuracy levels. Nevertheless, the risk of images being altered to avoid detection remains.

The accuracy levels of technologies to detect new content is gradually improving, but they remain substantially lower compared with those detecting known content. At this point in time, deploying the currently available technologies to detect new content on a large scale would result in high error rates and a very large number of false positives. As for the detection of grooming, the current accuracy levels of these technologies means that they cannot be deployed on a large scale without causing high error rates. The detection would, moreover, require language, cultural and context sensitive technologies to, for instance, assess messages in languages other than English and across various cultural contexts. These are currently not sufficiently developed. While technologies to detect new content and grooming are developing rapidly, it is unlikely that these technologies will achieve high accuracy rates in the near future.

Detecting CSAM (known CSAM, new CSAM and grooming) in E2EE communications presents substantial challenges. Technologically, detection of content in E2EE communications is possible, however, the currently available solutions to do so are neither sufficiently transparent nor secure. The complexity and lack of transparency of these technologies does not allow for independent evaluation by external experts and, therefore, quality control. Moreover, detection of CSAM on E2EE communications is disputed because it would impact the boundaries between a user's private life and their shared (semi-)public sphere, and would enhance vulnerabilities to attacks and abuse. The concerns with regards to the detection of CSAM in E2EE communications are of a fundamental nature and technologies to detect CSAM on E2EE communication are unlikely to reach high levels of accuracy in the next two to five years, without undermining the secure nature of E2EE communications.

The views on the expected impact of the CSA proposal on the quantity of reported content vary. Some experts expect that the amount of reported content will diminish, as the CSA proposal obliges providers of information society services to detect and report – in the absence of a legal basis for voluntary monitoring. The use of restricted classifiers and the 'disincentivising' effect of the CSA proposal will also have effects. However, the majority of experts consulted expect a steep increase in reported content, as the CSA proposal obliges providers of information society services to detect and report known content, as well as new content and grooming. It is important to note that an increase in the quantity of reported content may not necessarily result in an equivalent increase in investigation and prosecution, and, thus, better protection of children. Furthermore, the role envisaged for an EU centre in filtering the expected vast amount of (false positive) reports before they are shared with LEAs, thereby alleviating the burden on LEAs, is deemed unrealistic, given the huge number of resources this would require.

While experts' views vary, the majority expects the quality of detection to deteriorate due to the compulsory detection of new content and grooming. These types of CSAM require the application of technologies that have low accuracy levels, which would result in higher error rates. As long as the capacity of LEAs remains limited, the increased error rates, in conjunction with the rise in detected content, are expected to negatively impact LEAs' ability to investigate CSAM, because substantial efforts will be required to sift through the data to verify which content is worth investigating. Considerable efforts would be required to sift through the large sets of data to verify which content is worthwhile investigating further. While the proposed EU centre to prevent and combat CSA is envisaged to act as a central hub for hashes (digital fingerprinting) and would help standardise approaches, it is unlikely that an EU centre would substantially improve the quality of detection, considering that decades of research and development have, to date, not resulted in high accuracy levels for detecting new CSAM and grooming.

Finally, behavioural impacts are expected for providers of information society services, and child and adult users of online communication services. It is expected that the CSA proposal impacts the workload of providers of information society services substantially due to the obligations that the CSA proposal introduces for providers of information society services. Furthermore, the impact on the incentive for providers of information society services to innovate is expected to be twofold. On the one hand, the CSA proposal might negatively impact the desire to innovate in E2EE, as the CSA proposal directly interferes with the core principle of E2EE. The experts consulted point out that the CSA proposal requires the deployment of technologies that are inherently in conflict with what E2EE communications stand for, namely private communication. On the other hand, there is a need to develop technologies that can accurately detect new content and grooming, thereby providing innovation opportunities.

The proposal would help online communication services to become more child-friendly, and it would lead to a more rapid identification and take-down of CSAM, a minimised risk of re-victimisation, and better protection against grooming. Simultaneously, the CSA proposal might also

negatively impact the online (sexual) development of teenagers, some consulted experts note, as their consensually shared images could be classified as CSAM.

Adult users of online services without malicious intentions are expected to change behaviour to avoid false accusations of disseminating or consuming CSAM. Some users with malicious intent are expected to resort to the dark web, where detection is highly complex. Others are expected to continue their illegal activities on 'regular' communication channels and a part of this group is expected to be disincentivised to continue or start activities as a result of the CSA proposal.

Impact of the CSA proposal on fundamental rights

The CSA proposal is expected to impact the fundamental rights of the three main stakeholder groups differently. In aiming to prevent children falling victim to CSA, the proposal impacts several fundamental rights positively. It creates positive obligations for public authorities to act in protecting: Articles 3 CFR (the right to integrity of the person) and 4 CFR (prohibition of torture) requiring that children's physical and mental integrity are ensured; Article 7 CFR (right to privacy) mandating that children's private and family lives are protected, and Article 24 CFR, demanding that children are protected from any form of violence. The measures, including detection orders for CSAM, provided in the CSA proposal, can also negatively impact the fundamental rights of children as users of online services. More specifically, Articles 7 CFR (right to privacy), 8 CFR (right to data protection) and 11 CFR (right to freedom of expression and information) are affected. Limiting these rights may impact the personal development of children and their space to develop.

The proposal interferes with several fundamental rights of users of services by allowing for the issuing of detection orders that oblige service providers to screen their services for the dissemination of CSAM, known or new, or grooming. Firstly, the proposal would interfere with the right to private life and communications (Article 7 CFR), as the CJEU already acknowledged in respect of instances where traffic and location data are monitored, and would likely trigger a particularly serious infringement in cases where content of interpersonal communications is concerned. Secondly, it would interfere with the right to protection of personal data (Article 8 CFR), screening by service providers constitutes a form of data processing. Thirdly, it would seriously impact the freedom of expression and information (Article 11 CFR), as screening of users' communications might deter people from openly expressing their views and receiving the views of others.

The proposal is prejudicial to one of the fundamental rights of providers of information society services. Article 16 CFR (freedom to conduct a business) aims at safeguarding the right to each individual in the EU to operate a business without being subject to either discrimination or disproportionate restrictions. Imposing an obligation on service providers to install and maintain a costly computer system to monitor all electronic communications made through its network interferes with this right.

Prohibition of general data retention and general monitoring obligations

As part of the fundamental rights test carried out, the study analysed whether the negative impact on Articles 7 and 8 CFR in particular, is justifiable (following the criteria established in Article 52 CFR and case law of the CJEU. In these considerations, the study looks at the criteria the CJEU have established on the prohibitions of general data retention and general monitoring obligations.

The parameters to detect known material can be set with a high degree of specificity. However, as the CSA proposal does not require a detection order to be targeted at a specific group of users or content, the detection orders would violate the EU prohibition of general data retention and the prohibition of general monitoring obligations. In theory, the CSA proposal could be amended to require detection orders to specify a certain group of users to be targeted, in line with the requirements of the CJEU case law, to prevent detection orders from violating the prohibitions of

general data retention and general monitoring. However, certain classifiers, such as geographic location, age, or gender would not be appropriate features for specifying the groups of users subject to detection orders, because they cast the net too wide.

With respect to new CSAM and grooming, the parameters for detection cannot be set with high specificity, as in contrast with the detection of known CSAM, which exact content a technology ought to identify is not predetermined. With regard to new material, the technologies can only be applied indiscriminately to all users of both hosting services and interpersonal communication services. The proposed rules regarding obligations to detect new CSAM both on hosting providers and (all the more) on interpersonal communications providers affect the right to privacy disproportionately in terms of the group of users affected, which will amount to unlawful generalised monitoring and unlawful generalised surveillance. The requirements to be set to detect grooming would not be sufficiently targeted and thus amount to generalised and indiscriminate automated analysis of all communications transmitted through interpersonal communication services by default.

With regard to obligations on scanning the content of interpersonal communications by interpersonal communications providers, which includes grooming, new CSAM and likely known CSAM, this study concludes that the proposed rules compromise the essence of the fundamental right to privacy in the form of confidentiality of communications. Scanning content on users' personal devices in E2EE communications violates the essence of the right to data protection. In the case of E2EE channels of communications, even if it is not accepted that the essence of the right to data protection is compromised, the device side scanning of interpersonal communications is disproportionate to the aims pursued. It creates vulnerabilities and exposes users to a particularly increased risk of unlawful access by other governments and criminal organisations.

Necessity and proportionality

The study also analysed the necessity and proportionality of the CSA proposal measures. This examination would only apply in the case that, in the case of interpersonal communications, the argument that the CSA proposal measures impact the very essence of the Article 7 and 8 CFR were to be rejected.

The assessment of the necessity of the measures requires an analysis as to whether the measures will be effective in achieving their goal and, if so, whether less intrusive means could reach the same goal. With respect to the proposal's effectiveness, there are two main concerns: (i) the current state of play of the technology to detect new material and grooming is not sufficiently accurate for effective determination of CSAM; (ii) the extent to which LEA officials will be able to assess detected CSAM or grooming sufficiently accurate to be used as evidence in a prosecution of a suspect. The evidence collected in the CSA proposal IA is too limited with respect to both concerns.

Turning to the question of whether less intrusive ways could reach the same goal as the detection order, Article 4 of the CSA proposal presents the possibility of mitigation measures for service providers to reduce the risk of abuse of their service. Should the provider fail to adopt such measures voluntarily, the competent coordinating authority can issue a detection order. However, it does not provide the coordinating authority with a legal basis to take other, less-intrusive measures, and as such, the CSA proposal does not allow the coordinating authority to opt for less-intrusive measures to achieve the same objectives.

In considering proportionality of the measures, the study followed the *La Quadrature du Net* case, where the CJEU has set that for serious crime, as is the case for CSAM, the options for data retention are more restricted and should be more targeted (compared with issues of national security). The proposed rules regarding the issuance of detection orders do not rule out detection orders that would provide a generalised data retention obligation on service providers. Therefore, with regard to the detection of known material, the CSA proposal raises proportionality concerns, because of a

lack of requirements as to how specific the detection order will be carried out with respect to the targeted individuals. It is feasible for detection orders to specify a certain group of users to be targeted in line with the case law of the CJEU. However, with regard to known material, proportionality concerns are raised in relation to the technologies used in detection in E2EE communications, the procedural safeguards regarding the issuance of detection orders and the duration of the detection order.

Furthermore, due to the nature of new CSAM and grooming, detection orders to detect these types of CSAM would require a general data retention duty for service providers. For the detection of new CSAM and grooming in E2EE communications, the same concerns as those raised in relation to the detection of known material arise. Therefore, new binding obligations stemming from detection orders for relevant service providers to detect, report, and remove new material and grooming from their services would likely fail the proportionality test. In addition, in relation to the technology used regarding the detection of CSAM in E2EE communications, the device-side scanning of interpersonal communications is disproportionate to the aims pursued.

The proposed safeguards regarding the technologies used, the procedural aspects, such as the involvement of the proposed EU centre, the conditions of issuance of a detection order and the duration of a detection order cannot compensate for the lack of substantive safeguards in relation to all three types of content.

Proposed EU centre to prevent and counter child sexual abuse

With regards to the establishment of an EU centre to prevent and counter child sexual abuse, the option of establishing an EU centre with some functions hosted by Europol and others in an independent organisation under Member State law is found to be most efficient. Based on calculations conducted in this study, this option has the highest net present value and is thereby considered to be most efficient. This differs from the conclusion reached in the CSA proposal IA, in which the option of a decentralised agency was found to be the preferred option. The main reason for this difference is that this study expects an EU centre with some functions in Europol and others in an independent organisation under Member State to be implemented faster. The benefits, therefore, are expected to materialise earlier than in other options.

However, it should be noted that it is difficult to conduct a cost-benefit analysis of an EU centre in this study, especially because the EU centre would act in close collaboration with many other stakeholders and, therefore, effectiveness of the EU centre substantially depends on the actions of others. Also, the differences in costs and benefits between options are small. Moreover, certain aspects could not be quantified and expressed in monetary terms. It should be noted that factors associated with independence, institutional culture and the signalling function of the proposed EU centre (i.e., that the EU takes the matter seriously) can hardly be captured in a cost-benefit analysis.

References

Academic articles and books

Abelson, H., Anderson, R., Bellovin, S., Benaloh, J., Blaze, M., Callas, J., Diffie, W., Landau, S., Neumann, P., Rivest, R., Schiller, J., Schneier, B., Teague, V. and Troncoso, C. 'Bugs in our Pockets: The Risks of Client-Side Scanning', arXiv, 2021.

Abelson et al. 'Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications', Massachusetts Institute of Technology, 2015.

Anderson, R., 'Chat Control or Child Protection?', arXiv, 2022.

Bartusek, J., Garg, S., Jain, A. and Policharla, G. 'End-to-End Secure Messaging with Traceability Only for Illegal Content', Cryptology ePrint Archive, 2022.

Brkan, M., 'The Concept of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core', *European Constitutional Law Review,* Vol. 14(2), Cambridge University Press, pp.332-368, 2018.

Buiten, M., de Streel, A. and Peitz, M., 'Rethinking Liability for online hosting platforms', *International Journal of Law and Information Technology*, Vol. 28(2), Oxford University Press, 2020, pp.139-166.

Carr, J., 'Mechanisms for collective action to prevent and combat online child sexual exploitation and abuse', 2019.

Edwards et al. 'Cyber strategies used to combat child sexual abuse material', 2021.

Frosio, G,. 'Reforming intermediary liability in the platform economy: A European digital single market strategy', *New York University Law Review Online*, Vol. 112(18), Hein Online, pp. 19-46, 2017.

Gorwa, R., Binns, R. and Katzenbach, C., 'Algorithmic content moderation: Technical and political challenges in the automation of platform governance', *Big Data & Society*, Vol. 7(1), SAGE Journals, pp.1-15, 2020

Guerra, E., and Westlake, B., 'Detecting child sexual abuse images: Traits of child sexual exploitation hosting and displaying websites', *Child Abuse & Neglect* , Vol 122, 2021.

Hao, Q., Luo, L., Jan, S. and Wang, G., 'It's Not What It Looks Like: Manipulating Perceptual Hashing based Applications', The Association for Computing Machinery, 2021.

Hintersdorf, D., Struppek, L., Neider, D. and Kersting K., 'Investigating the Risks of Client-Side Scanning for the Use Case NeuralHash', IEEE Security, 2022.

Jain, S., Creţu, A., and de Montjoye, Y., Adversarial Detection Avoidance Attacks: Evaluating the robustness of perceptual hashing-based client-side scanning, 2022, *31st USENIX Security Symposium (USENIX Security 22).*

Koops, B., 'The concept of function creep', *Law, Innovation and Technology,* Vol 13(1), Routlegde, pp.29-56, 2021.

Lenaerts, K., 'Limits on Limitations: The Essence of Fundamental Rights in the EU', *German Law Journal,* Vol. 20(6), Cambridge University Press, pp.779-793, 2019.

Levy, I. and Robinson, C., 'Thoughts on Child Safety on Commodity Platforms', arXiv, 2022.

Peers, S., Hervey, T., Kenner, J. and Ward, A. 'The EU Charter of Fundamental Rights: A Commentary', 2nd edition, Hart Publishing, 2021.

Peersman, C., Llanos, J., May-Chahal, C., McConville, R., Chowdhury, P., and De Cristofaro, E., REPHRAIN: Towards a Framework for Evaluating CSAM Prevention and Detection Tools in the Context of End-to-end encryption Environments: a Case Study, 2023.

Penney, J., 'Chilling Effects: Online Surveillance and Wikipedia Use', *Berkeley Technology Law Journal,* Vol. 31(1), JSTOR, 2016, pp. 117-182.

Pfefferkorn, R., 'Content-Oblivious Trust and Safety Techniques: Results from a Survey of Online Service Providers', *Journal of Online Trust and Safety,* Vol 1(2), pp.1-38, 2022.

Powell, A., Hills, M. and Nash, V. 'Child Protection and Freedom of Expression Online', *Oxford Internet Institute Forum Discussion Paper,* Vol. 17(1), University of Oxford, 2010, pp. 1-59.

Prokos, J., Jois, T. M., Fendley, N., Schuster, R., Green, M., Tromer, E., & Cao, Y, Squint hard enough: Evaluating perceptual hashing with machine learning. *Cryptology ePrint Archive*, 2021.

Schauer, F., 'Fear, Risk and the First Amendment: Unravelling the "Chilling Effect"', *Boston University Law Review*, Vol 58(685), pp.685-732.

Shumailov, I., Shumailov, Z., Kazhdan, D., Zhao, Y., Papernot, N., Erdogdu, M. and Anderson R., 'Manipulating SGD with Data Ordering Attacks', arXiv, 2021.

Struppek, L., Hintersdorf, D., Neider, D., & Kersting, K., Learning to break deep perceptual hashing: The use case neuralhash, 2022, *2022 ACM Conference on Fairness, Accountability, and Transparency*.

Urban et al., 'Takedown in Two Worlds: an empirical analysis', *Journal of the Copyright Society of the USA*, Vol. 64(483), Hein Online, 2017, pp. 483-520.

Urban et al., 'Notice and Takedown: Online Service Providers and Rightsholders Accounts of Everyday Practice', *Journal of the Copyright Society of the USA*, Vol. 64(371), Hein Online, 2017, pp.371-410.

Van der Hof, S., Georgieva, I, Schermer, B. W. and Koops, Bert-Jaap, *Sweetie 2.0, Using Artificial Intelligence to Fight Webcam Child Sex Tourism*, T.M.C. Asser Press, July 2019.

Vu A., Wilson, L., Chua, Y. Shumailov, I. and Anderson, R., 'ExtremeBB: Enabling Large-Scale Research into Extremism, the Manosphere and Their Correlation by Online Forum Data', arXiv, 2021.

Weng, L. and Preneel, B., 'Attacking some perceptual image hash algorithms', Proc. of IEEE International Conference on Multimedia and Expo 2007, 2007.

Wilman, F.G., 'Two emerging principles of EU internet law: A comparative analysis of the prohibitions of general data retention and general monitoring obligations', *Computer Law & Security Review,* Vol. 46, Elsevier, 2022, pp.1-18.

Witting, S. and Leiser M., 'Outcome Report of expert workshop on EU's proposed regulation on preventing and combatting child sexual abuse', Leiden University and Council of Europe, February 2023.

Other publications

Towards a principled level playing field for an open and secure online environment, Centre for European Policy Studies, October 2022.

Witness Statement in committee meeting on Fostering a Healthier Internet to Protect Consumers, House Committee on Energy and Commerce, 2019.

Study on options for the creation of a European Centre to prevent and counter child sexual abuse, including the use of ICT for creation of a database of hashes of child sexual abuse material and connected data protection issues (Final Report V2.0), ICF, 2021.

Position Paper on the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, Microsoft, September 2022.

Report on Turning The Tide Against Online Child Sexual Abuse, The Police Foundation, July 2022.

Policy Documents

Explanatory Report to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Council of Europe, October 2007.

Opinion on child sexually suggestive or explicit images and/or videos generated, shared and received by children, Lanzarote Committee, Council of Europe, November 2019.

Implementation Report: the Protection of Children Against Sexual Exploitation and Sexual Abuse Facilitated by Information and Communication Technologies (ICTs), Council of Europe, March 2022.

Guide on Article 3 of the European Convention on Human Rights, Council of Europe and European Court of Human Rights, August 2022.

Guide on Article 5 of the European Convention on Human Rights, Council of Europe and European Court of Human Rights, August 2022.

Guide on Article 8 of the European Convention on Human Rights, Council of Europe and European Court of Human Rights, August 2022.

Report assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, European Commission, 2016.

Communication on EU strategy for a more effective fight against child sexual abuse, COM/2020/607 final, European Commission, July 2020.

Proposal for a Regulation on a temporary derogation from certain provisions of Directive 2002/58/EC, COM(2020) 568 final, European Commission, September 2020.

Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act), COM(2020) 825 final, European Commission, December 2020.

Communication on EU strategy on the rights of the child, COM(2021) 142 final, European Commission, March 2021.

Better Regulation Guidelines, European Commission, November 2021.

Better regulation toolbox, European Commission, November 2021.

Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, European Commission, May 2022.

Impact Assessment Report Accompanying the document Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, European Commission, May 2022.

Communication on A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+), COM(2022) 212 final, European Commission, May 2022.

Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, European Data Protection Board and European Data Protection Supervisor, July 2021.

Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, European Data Protection Supervisor, December 2019.

Targeted substitute impact assessment on Commission proposal on the temporary derogation of the e-Privacy Directive for the purpose of fighting online child sexual abuse, targeted substitute impact assessment, European Parliamentary Research Service, February 2021.

Regulatory Scrutiny Board Opinion Regulation on detection, removal and reporting of child sexual abuse online, and establishing the EU centre to prevent and counter child sexual abuse, SEC (2022) 209, European Parliament Regulatory Scrutiny Board, February 2022.

Draft opinion on the proposal for a regulation laying down rules to prevent and combat child sexual abuse, IMCO committee, European Parliament, 8 February 2023.

Explanations relating to the Charter of Fundamental Rights, European Union, December 2007.

Report on Freedom to conduct a business: exploring the dimension of a fundamental right, European Agency for Fundamental Rights, 2015.

Handbook on European Law relating to the rights of the child, European Agency for Fundamental Rights and Council of Europe, 2017.

Handbook on European Data Protection Law, European Union Agency for Fundamental Rights and Council of Europe, April 2018.

The sale and exploitation of children: digital technology, Unicef Office of Research-Innocenti, 2020.

General Comment on The right of the child to freedom from all forms of violence, United Nations Committee on the Rights of the Child, April 2011.

Legislation (treaties, regulations, directives, etc.)

Council of Europe Convention on Cybercrime, November 2001.

Council of Europe Convention on preventing and combating violence against women and domestic violence, May 2011.

Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, July 2014.

Charter of Fundamental Rights of the European Union, December 2017.

Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

Directive 2011/92/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography.

Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code.

Directive (EU) 2019/790 of 17 April 2019 on copyright and related rights in the Digital Single Market.

Regulation (EU) 2015/2120 of 25 November 2015 laying down measures concerning open internet access.

Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

Regulation (EU) 2021/1232 of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC.

Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector.

Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services.

United Nations Convention on the Rights of the Child, November 1989.

Case law

Judgment in Case 6538/74 – *The Sunday Times* v *The United Kingdom*, European Court of Human Rights, April 1979.

Judgment in Case 8978/80 – *X and Y* v *Kingdom of the Netherlands*, European Court of Human Rights, March 1985.

Judgment in Case 13719/88 – *Niemitz* v *Germany*, European Court of Human Rights, December 1992.

Judgment in Case 25803/94 – *Selmouni* v *France (GC)*, European Court of Human Rights, July 1999.

Judgment in Case 48787/99 - *Ilaşcu and Others* v *Moldova and Russia (GC),* European Court of Human Rights, July 2004.

Judgment in Case 21986/93 – *Salman* v *Turkey (GC)*, European Court of Human Rights, June 2000.

Judgment in Case 28761/11 – *Al Nashiri* v *Poland*, European Court of Human Rights, February 2015.

Judgment in Case 5310/71 – *Ireland* v *The United Kingdom*, European Court of Human Rights, September 2018.

Judgment in Case 32427/16 – *Petrosyan* v. *Azerbaijan*, European Court of Human Rights, February 2022.

Judgment in Case 377/98 – *Kingdom of the Netherlands* v *European Parliament and Council of the European Union*, European Court of Justice, October 2001.

Judgment in Case C-36/02 – *Omega Spielhallen- und Automatenaufstellungs-GmbH* v *Oberbürgermeisterin der Bundesstadt Bonn*, European Court of Justice, October 2004.

Judgment in Case C-316/09 – *MSD Sharp & Dohme GmbH* v *Merckle GmbH*, European Court of Justice, May 2011.

Judgment in Case C-324/09 – *L'Oréal* v *eBay International AG and Others*, European Court of Justice, July 2011.

Judgment in Case C-70/10 – *Scarlet Extended SA* v *Société belge des auteurs, compositeurs et éditerus SCRL (SABAM)*, European Court of Justice, November 2011.

Judgment in Case C-360/10 – *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM)* v *Netlog NV*, European Court of Justice, February 2012.

Judgment in Joined Cases C-293/12 and C-594/12 – *Digital Rights Ireland Ltd* v *Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others,* European Court of Justice, April 2014.

Judgment in Case C-362/14 – *Maximillian Schrems* v *Data Protection Commissioner*, European Court of Justice, October 2015.

Judgment in Case C-358/14 – *Republic of Poland* v *European Parliament and Council of the European Union*, European Court of Justice, May 2016.

Judgment in Case C-484/14 – *Tobias Mc Fadden* v *Sony Music Entertainment Germany GmbH*, European Court of Justice, September 2016.

Judgment in Joined Cases C-203/15 and C-698/15 – *Tele2 Sverige AB* v *Post- och telestyrelsen and Secretary of State for the Home Department* v *Tom Watson and Others*, European Court of Justice, December 2016.

Judgment in Case C-18/18 – *Eva Glawischnig-Piesczek* v *Facebook Ireland Limited*, European Court of Justice, October 2019.

Judgment in Case C-78/18 – *European Commission* v *Hungary (Transparency Associations)*, European Court of Justice, June 2020.

Judgment in Case C-393/19 – *OM*, European Court of Justice, June 2020.

Judgment in Joined Cases C-511/18, C-512/18 and C-520/18 – *La Quadrature du Net and Others* v *Premier ministre and Others*, European Court of Justice, October 2020.

Judgment in Joined Cases C-682/18 and C-683/18 – *Frank Peterson* v *Google LLC and Others and Elsevier Inc* v *Cyando AG*, European Court of Justice, June 2021.

Judgment in Case C-140/20 – *G. D.* v *The Commissioner of the Garda Síochána and Others*, European Court of Justice, April 2022.

Websites

The Chilling Effect of Student Monitoring: Disproportionate Impacts and Mental Health Risks, Center for Democracy & Technology, 2022.

Client-Side Scanning And Winnie-The-Pooh Redux (Plus Some Thoughts On Zoom), Center for Internet and Society (at Stanford Law School), accessed 9 March 2023.

Online age verification: balancing privacy and the protection of minors, CNIL, accessed 20 April 2023.

Safety by Design Principles and Background, eSafety Commissioner of the Australian government, accessed 6 February 2022.

The EU Strategy on the Rights of the Child and the European Child Guarantee, European Commission, accessed 6 February 2023.

Combating violence against children and ensuring child protection, European Commission, accessed 6 February 2023.

Private and secure communications attacked by European Commission's latest proposal, European Digital Rights, accessed 3 March 2023.

Member States want internet service providers to do the impossible in the fight against child sexual abuse, European Digital Rights, accessed 9 March 2023.

Does monitoring your phone affect the essence of privacy?, European Law Blog, European Law Blog, accessed 9 March 2023.

EU Charter of Fundamental Rights: Article 1- Human Dignity, European Union Agency for Fundamental Rights, December 2007, accessed on 10 March 2023.

EU Charter of Fundamental Rights: Article 7 – Respect for private and family life, European Union Agency for Fundamental Rights, December 2007, accessed on 10 March 2023.

Internal documents revealed the worst for private communications in the EU; how will the Commissioners respond?, European Digital Rights, accessed 9 March 2023.

The internal market: General principles, European Parliament, accessed 5 March 2023.

Case analysis of Scarlet Extended SA v SABAM, Global Freedom of Expression Columbia University, accessed 9 March 2023.

Fighting child sexual abuse online, Google, accessed 23 December 2022.

What is end-to-end-encryption, IBM, accessed 28 February 2023.

Fact Sheet: Client-Side Scanning, Internet Society, accessed 30 March 2023

New Technology to Fight Child Exploitation, Meta, accessed 23 December 2022.

How PhotoDNA for Video is being used to fight online child exploitation, Microsoft, accessed 23 December 2022.

PhotoDNA, Microsoft, accessed 23 December 2022.

What is Encryption?, Microsoft, accessed 23 December 2022.

Use end-to-end encryption for one-to-one Microsoft Teams calls, Microsoft, accessed 23 December 2022.

A Dad Took Photos of His Naked Toddler for a Doctor. Google Flagged Him as a Criminal, The New York Times, accessed 9 March 2023.

How Safer's detection technology stops the spread of CSAM, Thorn, accessed 23 December 2022.

Why an increase in reports of CSAM is actually a good thing, Thorn, accessed 9 March 2023.

Apple's NeuralHash — How it works and how it might be compromised, Towards Data Science, accessed 9 March 2023.

Europese Verordening ter voorkoming en bestrijding van seksueel kindermisbruik, Tweede Kamer der Staten-Generaal, accessed 9 March 2023.

Global Threat Assessment, WeProtect Global Alliance, 2021.

How WhatsApp Helps Fight Child Exploitation, WhatsApp, accessed 23 December 2022.

HashKeeper, accessed 27 March 2023.

Technologies to stop CSAM: Binary Hashing, NetClean, accessed 27 March 2023.

Reactionary Authoritarianism, Encryption, and You!, Electronic Frontier Foundation, March 2023.

Working together to end online child sexual exploitation and abuse, TechCoalition, accessed 28 March 2023.

Testing End-to-End Encrypted Backups and More on Messenger, Messenger News, accessed 26 March 2023.

Benchmarking, Perception, accessed 27 March 2023.

ANNEX I – Stakeholder consultation

Table 18: Overview of consulted stakeholders

Nr	Organisation	Type of organisation	Type of involvement
1	European Commission	EU government	Interview conducted
2	European Data Protection Board	EU independent body	Interview conducted
3	European Data Protection Supervisor	EU independent body	Invited but kindly declined participation
4	Fundamental Rights Agency	EU independent body	Invited but kindly declined participation
5	ENISA	EU independent body	Interview conducted
6	Europol	LEA	Written input received
7	Law Enforcement Agency	LEA	Interview conducted
8	NCMEC	NGO	Interview conducted
9	European Digital Rights	NGO	Interview conducted
10	IT-POL	NGO	Interview scheduled
11	WeProtect Global Alliance	NGO	Interview conducted
12	Defence for Children – ECPAT Nederland	NGO	Interview conducted
13	Electronic Frontier Foundation	NGO	Interview conducted
14	Leiden University / VU University	Academic	Interview conducted
15	University of Cambridge	Academic	Interview conducted
16	Google	Service provider	Interview conducted
17	Microsoft	Service Provider	Interview conducted
18	Meta	Service provider	Written input received

Source: Ecorys

ANNEX II – Problem definition as in CSA proposal IA

The following table presents the problem definition as included in the CSA proposal IA.

Table 19: Problem definition as presented in CSA proposal IA

Problem	Problem driver	Underlying driver	Specific measure included in CSA proposal
Some child sexual abuse crimes are not adequately addressed in the EU due to challenges in their detection, reporting, and action by relevant service providers, as well as insufficient prevention and assistance to victims. Diverging national responses negatively affect the Internal Market.	1. Voluntary action by service providers to detect online child sexual abuse has proven insufficient.	1.1. Voluntary action varies significantly among companies. 1.2. Voluntary action is susceptible to changes in companies' policies. 1.3. Voluntary action leaves decisions affecting fundamental rights to service providers and lacks harmonised safeguards. 1.4. Voluntary action has failed to remove victims' images effectively.	1. Practical measures to enhance voluntary efforts 3. EU Centre on prevention and assistance to victims and combatting CSA online. 4. Legislation specifying the conditions for voluntary detection. 5. Obligation to report and remove CSA online 6. Obligation to detect known CSAM. 7. Obligation to detect new CSAM. 8. Obligation to detect grooming.
	2. Inefficiencies in public-private cooperation between service providers, civil society organisations and public authorities hamper an effective fight against CSA.	2.1 Inefficient cooperation between public authorities and service providers. 2.2 Inefficient cooperation between civil society organisations and service providers. 2.3 Inefficient cooperation between public authorities and civil society organisations. 2.4 Inefficient cooperation between public authorities, service providers and civil society organisations.	9. EU Centre on prevention and assistance to victims.
	3. Member States' efforts to prevent child sexual abuse and to assist victims are limited, divergent and lack coordination and are of unclear effectiveness.	3.1 Limited, divergent, and uncoordinated prevention efforts. 3.2 Limited, divergent, and uncoordinated assistance to victims' efforts.	10. EU Centre on prevention and assistance to victims.

Source: Ecorys

ANNEX III – Elaboration on technical solutions reflected upon in CSA proposal IA

As part of the CSA proposal IA, the European Commission invited technical experts to reflect on nine technological solutions that could potentially be applied to detect known and new material in E2EE communications.[374] The European Commission acknowledges that technologies to detect grooming are different from those used to detect photos and videos. As such, they note that it is not easy to bundle the assessment of possible technological solutions for photos, videos and text-based threats together. Hence, the European Commission has restricted itself to the assessment of possible solutions for the detection of known and new material.[375] They distinguish device related[376], server related[377] and encryption related solutions.[378] The experts assessed solutions based on five indicators:[379]

(33) *Effectiveness*: how well does the solution detect and report known and new CSAM? [380]

(34) *Feasibility*: how ready is the solution and how easily can it be implemented, in terms of costs, times and scalability?

(35) *Privacy*: how well does the solution ensure the privacy of communications?

(36) *Security*: how vulnerable is the solution to misuse for other purposes than the fight against CSA, including by companies, governments. or individuals?

(37) *Transparency*: to what extent can the use of the solution be documented and publicly reported to facilitate accountability through ongoing evaluation and oversight by policymakers and the public?

The following table provides an overview of how the experts assessed the above indicators for each of the technological solutions. Where relevant or necessary, clarifications by the researchers have been added. These additions are marked in the text. Noteworthy is that experts consulted as part of this study point out that the indicator 'privacy' is interpreted too narrowly as it mainly focuses on the risk of abuse by the service provider. These experts note that 'privacy' could also encompass the exposure risk of sensitive user data as a consequence of system compromise ("hacking" of user device and/or server). Based on the assessment, three solutions stood out in terms of their score on the indicators. These solutions can be perceived to be the most viable solutions, according to the experts consulted by the European Commission, to be applied in the combat against CSAM. These

---

374 Impact Assessment Report Accompanying the document Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, European Commission, May 2022, pp. 284 – 314.

375 Ibid., pp. 284 – 314.

376 This type of solutions consists in moving to the device some or all of the operations done at the Electronic Service Provider (ESP) in communications that are not end-to-end-encrypted.

377 This type of solutions consists in moving to the secure enclaves in the ESP server or third-party servers some or all of the operations done at the ESP server in communications that are not end-to-end-encrypted.

378 This type of solutions consists in using encryption protocols that allow the detection of CSAM in encrypted electronic communication; The nine considered potential solutions are 'all detection done on-device', 'on-device full hashing with matching at server', 'on-device partial hashing with matching at server', 'on-device use of classifiers', 'secure enclaves in the ESP server', 'single third party matching', 'multiple third parties matching', 'on-device homomorphic encryption with server-side hashing and matching'.

379 Impact Assessment Report Accompanying the document Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, European Commission, May 2022, p. 289.

380 I.e., images, videos, and text-based threats.

three most viable solutions are presented in the table in blue and are reflected upon in more detail in the body of the study.

Table 20: Identified solutions for detecting CSAM in E2EE

	Type of content	Effectiveness	Feasibility	Privacy	Security	Transparency
Device related solutions						
All detection done on-device	Known	***	**	***	*	**
On-device full hashing	Known	****	*****	**	**	***
On-device partial hashing	Known	****	***	**	***	**
On-device use of classifiers	Known New	**	**	**	**	***
Server related solutions						
Secure enclave in ESP server	Known New	****	**	**	**	**
Single third-party matching	Known	****	*	**	**	**
Multiple third-parties matching	Known	****	*	***	***	***
Encryption related						
On-device homomorphic encryption	Known	***	*	**	***	***

Ranking runs from * to *****, whereby * represents a low score and ***** a high score.
Solutions marked in blue are those that are deemed most viable.
Source : CSA proposal IA, p. 290

As can be understood from the table, the experts consulted by the European Commission considered the following three technologies as most promising to be developed further:

(38) On-device full hashing (with matching at server);

(39) On-device partial hashing (with matching at server;

(40) Secure enclaves in Electronic Service Provider (ESP) server.

Experts consulted as part of this study noted that the assessment of effectiveness by the European Commission is too positive (i.e., ***, in the table above) in the case of on-device full hashing and on-device partial hashing. In both instances, they note that a more accurate assessment of the effectiveness would have been **. Nevertheless, in the body of the report, the three most viable solutions identified by the European Commission are further explored.

ANNEX IV – Elaborated analysis of impact of the CSA proposal on fundamental rights

Chapter 4 discussed the impact of the CSA proposal on fundamental rights. As discussed in the description of the fundamental right checklist, this formed the basis of the necessity and proportionality test that has been carried in Chapter 5.

Overview of evaluated fundamental rights

The analysis concerns an evaluation of how the CSA proposal impacts different fundamental rights and, in the case of negative interference with some fundamental rights, whether these interferences can nevertheless be compatible with the Charter. Similar as in the CSA proposal IA this analysis is structured along the main groups whose fundamental rights are being impacted by the Proposal (see the table below for an overview of the impacted fundamental rights by the relevant group).

Table 21: Evaluated fundamental rights

Rights of children	Rights of internet users	Rights of providers of information society services
• Article 3 – Right to integrity of the person • Article 4 – Prohibition of torture and inhumane or degrading treatment • Article 6 – Right to liberty and security • Article 7 – Right of private and family life, home and communications • Article 24 – Rights of the Child	• Article 7 – Right of private and family life, home and communications • Article 8 – Protection of personal data • Article 11 – Freedom of expression and information	• Article 16 – Freedom to Conduct a business

Source: Ecorys

There is one fundamental right for which an exception has been made and cannot be put under one of these three groups. It concerns the Right of human dignity as described in Article 1 of the Charter. As will be discussed, this right can be seen as a key principle that is relevant for the interpretation of all other fundamental rights laid down in the Charter. Furthermore, it is important to notice that Article 7 is mentioned twice. The reason is that the Proposal impacts the right of private life of both children and internet users.

The right to human dignity: a special case

The right of human dignity mainly underlines the central role of the individual in the EU legal framework and provides an important principle on how the other fundamental rights should be interpreted. This makes it difficult to assess whether a measure violates Article 1 of the Charter or not.

Article 1: Right of human dignity

Article 1 of the Charter prescribes that 'human dignity is inviolable. It must be respected and protected.' It is an extremely far-reaching right as it protects the central position of the individual in

all activities of the EU.[381] Importantly, it cannot just be considered as a fundamental right in itself, but constitutes the real basis of all other fundamental rights.[382] References to 'dignity' usually refer to offer protection to vulnerable people, such as minors and asylum seekers, by guaranteeing that their 'special needs' are being met.[383]

The scope of article 1 of the Charter on the right of human dignity can be considered as unusually wide due to the nature of this right under the EU Charter as 'a real basis for other fundamental rights.[384] The Charter does not define 'human dignity'. Likely the closest synonym to the concept can be found in the Charter's preamble 'placing the individual at the heart of [EU] activities.[385] It only concerns the protection of humans and involves all the rights guaranteed under Title I of the Charter.[386]

It can therefore be derived that article I of the Charter provides guidance on how the other fundamental rights should be interpreted. It mainly underlines the central role of the individual in the EU legal framework. This also explains why the CJEU is hesitant in addressing human dignity claims directly. Instead, it prefers to resolve cases by focussing on specific dignity rights under title I of the Charter.[387] Furthermore, the CJEU found in the Omega Case that the fundamental freedoms, prescribed under title II of the Charter, have to be interpreted in compliance with the principle of human dignity.[388]

Impact of CSA proposal on fundamental rights of children

Article 3: Right to integrity of the person

Article 3-point 1[389] of the Charter states that 'everyone has the right to respect for his or her physical and mental integrity.' As the CJEU specified in the case Netherlands v European Parliament and Council,[390] the right to integrity (as well as dignity) is applicable across all EU policy areas.[391] This right is conceptually related to the right to integrity deducted by the European Court of Human Rights (ECtHR) from Article 8(1) of the European Convention of Human Rights (ECHR) – The right to

---

381 Charter of Fundamental Rights of the European Union, December 2017.

382 EU Charter of Fundamental Rights, European Union Agency for Fundamental Rights, December 2007, Article 1.

383 Peers et al. 'The EU Charter of Fundamental Rights: A Commentary', 2021, p. 5.

384 Ibid., pp. 15-16.

385 Charter of Fundamental Rights of the European Union, December 2017, p. 3.

386 Peers et al. 'The EU Charter of Fundamental Rights: A Commentary', 2021, p. 16-17. The rights under title I are the right to life (Article 2), the right to the integrity of the person (Article 3), Prohibition of torture and inhuman or degrading treatment of punishment (Article 4) and Prohibition of slavery and forced labour (Article 5).

387 Ibid., p. 20.

388 Judgment in Case C-36/02 – *Omega Spielhallen- und Automatenaufstellungs-GmbH* v *Oberbürgermeisterin der Bundesstadt Bonn*. The rights under title II are the Right to liberty and security (Article 6), Respect for private and family life (Article 7), Protection of personal data (Article 8), Right to marry and right to found a family (Article 9), Freedom of thought, conscience and religion (Article 10), Article 11 (Freedom of expression and information), Freedom of assembly and of association (Article 12), Freedom of the arts and sciences (Article 13), Right to education (article 14), Freedom to choose an occupation and right to engage in work (Article 15), Freedom to conduct a business (article 16), Right to property (article 17), Right to asylum (Article 18), and Protection in the event of removal, expulsion or extradition (Article 19).

389 Article 3 point 2 concerns specific rights in medicine and biology area, and as such is outside of scope of the present analysis. The explanation to the Charter in regards to Article 3 is focused primarily on the medical and biological aspects of the right to integrity, and references the Convention on Human Rights and Biomedicine.

390 Judgment in Case C-377/98 – *Kingdom of the Netherlands* v *European Parliament and Council of the European Union*, European Court of Justice, October 2001, paragraph 70.

391 Peers et al. 'The EU Charter of Fundamental Rights: A Commentary', 2021, p. 41.

private life.[392] In its scope, the right to integrity entails inviolability of a person's body and mental state and health.[393] It is closely related with the right to dignity, right to life, and prohibition of torture and degrading or inhumane treatment (Articles 1, 2 and 4 of the Charter, respectively). From this right it stems, that every person should be protected from physical and psychological harm, and the state has a positive obligation to guarantee such protection.

In the context of the analysed CSA proposal, the key question concerns the level to which the state is obliged to protect the physical and mental (psychological) integrity of citizens. In that regard, the CJEU has established that the required type of protection depends on the seriousness of the crime at stake. While it is not yet clear from CJEU case law as to which offences constitute a serious crime in that sense, there is no doubt that CSA falls under this category. In the case of the *La Quadrature du Net*, the CJEU pointed out that "as regards, in particular, effective action to combat criminal offences committed against, inter alia, minors and other vulnerable persons […] positive obligations of the public authorities […] may also arise from […] Articles 3 and 4, as regards the protection of an individual's physical and mental integrity and the prohibition of torture and inhuman and degrading treatment".[394] In the aforementioned case, the CJEU has also referred to ECtHR jurisprudence regarding Articles 3 and 8 of ECHR, which provide further insight. These are discussed in more detail in the following subsection concerning Article 4 of the Charter.

Impact of CSA proposal on Article 3

Overall, the CSA proposal can be expected to have positive impact on Article 3 of the Charter. The scale of this positive impact will depend on the effectiveness of implementation of the measures provided, as well as subsequent criminal proceedings.

The wide scope of the proposed Regulation, including detection and removal of known and new CSAM, as well as detection of grooming, will likely positively impact the protection of children's physical and mental integrity. There are several channels of this positive impact. It has to be noted that the present assessment is carried out based on the assumption that the Proposal will lead to increased detection and prevention, as provided by the CSA proposal IA. However, it needs to be underlined that this assumption itself has been questioned by the experts (see Chapter 3).

First, the mandatory risk assessment and risk mitigation requirements for the hosting or interpersonal communications providers, and the requirement to report those to competent authorities[395] might increase detection of the CSAM-related crimes on internet platforms (see Chapter 3).

Second, paired with effective removal or blocking of content, this could further prevent the distribution and spreading of CSAM online, preventing further / secondary psychological harm (see also discussion of Article 24 of the Charter below). A court order mandating removal can be requested by national authorities (and challenged by the platforms, which safeguards their owners' rights, see the Analysis of Article 16 of the Charter below).[396] The court-ordered removal is established as a dominant remedy, while blocking of content instead of removal can also be ordered in case the content "cannot be reasonably removed at source".[397] This solution is aimed to balance

---

392 Judgment in Case 8978/80 – *X and Y* v *Kingdom of the Netherlands*, European Court of Human Rights, March 1985.

393 Guide on Article 8 of the European Convention on Human Rights, Council of Europe and European Court of Human Rights, August 2022.

394 Judgment in Joined Cases C-511/18, C-512/18 and C-520/18 – *La Quadrature du Net,* paragraph 126.

395 Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, European Commission, May 2022, Articles 3 to 6.

396 Ibid., Article 15.

397 Ibid., Articles 16 and 17.

the discussed rights with the rights of platform owners and internet users.[398] The meaning of "reasonable removal" is not specified. This poses a risk of blocking instead of removal of CSAM content – a less effective method of preventing content access, which may significantly compromise the positive impact of these provisions on Article 3 of the Charter.

Third, the detection of grooming along with the CSAM content – if effective – is likely to improve prevention of CSA, in line with Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (the Lanzarote Convention),[399] requirements to increase such prevention.

Article 4: Prohibition of torture and inhumane or degrading treatment

Article 4 of the Charter establishes that 'no one shall be subjected to torture or to inhuman or degrading treatment or punishment.' This right sets out an indispensable condition for protection of the right to human dignity (Article 1) and should be interpreted in its light. The prohibition of torture is a peremptory norm of international law and an absolute right, which cannot be limited or overridden.

Starting with the scope, the right stipulated by Article 4 of the Charter prohibits the gravest forms of ill-treatment. It has the same meaning and scope that the right defined by Article 3 ECHR. Torture is a particular category of ill-treatment, a deliberate inhuman treatment causing very serious and cruel suffering; inflicted purposefully, with an aim of, i.a., obtaining information or a confession, inflicting punishment or intimidation.[400] As specified by the ECtHR, the difference between torture and inhumane or degrading treatment depends primarily on the level of suffering caused.[401] Degrading treatment humiliates or debases an individual, showing a lack of respect for, or diminishing, his or her human dignity, or arouses feelings of fear, anguish or inferiority capable of breaking an individual's moral and physical resistance.[402] Moreover, the treatment does not have to necessarily be carried out with these intentions to violate Article 3 ECHR (Article 4 of the Charter).[403]

While the Charter as well as the ECHR define the prohibition of torture and inhumane and degrading treatment only in negative terms, the jurisprudence derives also clear positive obligations for the State to prevent such ill-treatment.[404] The ECtHR specified in 'X and Others v. Bulgaria' that there are three types of such obligations.[405] The primary substantive obligation of the state includes providing legislative and regulatory framework to guarantee protection from torture and inhumane or

---

398 Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.; Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, European Commission, May 2022, p. 17.

399 Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, July 2014.

400 Guide on Article 3 of the European Convention on Human Rights, Council of Europe and European Court of Human Rights, August 2022, pp. 7-8. The main relevant European Court of Human Rights cases include: Case 5310/71 – *Ireland* v *The United Kingdom*, paragraph 167; Case 25803/94 – *Selmouni* v *France*, paragraphs 96-97; Case 48787/99 - *Ilaşcu and Others* v *Moldova and Russia*, paragraph 426; Case 21986/93 – *Salman* v *Turkey*, paragraph 114; Case 28761/11 – *Al Nashiri* v *Poland*, paragraph 508; *Petrosyan* v. *Azerbaijan*, paragraph 68.

401 Judgment in Case 5310/71 – *Ireland* v *The United Kingdom*, paragraph 167.

402 Guide on Article 3 of the European Convention on Human Rights, Council of Europe and European Court of Human Rights, August 2022, p. 9.

403 Guide on Article 3 of the European Convention on Human Rights, Council of Europe and European Court of Human Rights, August 2022. The main relevant European Court of Human Rights cases include: Case 22978/05 – *Gäfgen* v *Germany*, paragraph 89; Case 48787/99 - *Ilaşcu and Others* v *Moldova and Russia*, paragraph 425; Case 30696/09 – *M.S.S.* v *Belgium and Greece*, paragraph 220.

404 Peers et al. 'The EU Charter of Fundamental Rights: A Commentary', 2021, p. 64.

405 Judgment in Case 22457/16 – *X and Others* v *Bulgaria*, paragraph 178.

degrading treatment.[406] Secondly, in certain circumstances, the State is also obliged to apply operational measures preventively – "to protect specific individuals against a risk of treatment contrary to that provision".[407] Finally, there is also a procedural obligation to carry out an effective investigation into claims of violation of that right.

In the context of the analysed proposal, all three positive obligations of the state to prevent torture and inhumane or degrading treatment are relevant. Firstly, the ECtHR established that for children and other vulnerable persons, effective protection from the state is particularly important.[408] Secondly, sexual abuse of children constitutes a serious act that requires not only effective criminal law provisions,[409] but may also require the State to 'include reasonable steps to prevent ill-treatment of which the authorities had or ought to have had knowledge'.[410] However, the Court qualified this obligation, indicating that it should not impose an impossible or disproportionate burden on the State. At the same time in the context of CSA in the relation of authority, the Court indicated the crucial role of detection and reporting mechanisms.[411] The latter may also indicate a potential direction of interpretation in certain qualified cases of online CSAM. Thirdly, in cases concerning CSA, the authorities ought to primarily consider children's best interests, and take their particular vulnerability into account within the proceedings, in line with the Lanzarote Convention.[412]

Impact of CSA proposal on Article 4

The Proposal is expected to impact Article 4 of the Charter positively, and the considerations provided in the analysis of impact on Article 3 of the Charter above apply here. The measures provided by the proposed Regulation would facilitate attainment and compliance with positive obligations in all three aspects analysed above.

Moreover, by introducing the court detection order requests[413] and mandatory reporting obligations for providers that have become aware of the presence of the CSAM on their platforms,[414] the Regulation equips public authorities with relevant tools to gather evidence to persecute these crimes, which is in line with the procedural positive obligation of the state discussed above.

---

406 Guide on Article 3 of the European Convention on Human Rights, Council of Europe and European Court of Human Rights, August 2022, p. 24.

407 Judgment in Case 22457/16 – *X and Others* v *Bulgaria*, paragraph 178.

408 Judgment in Case 22457/16 – *X and Others* v *Bulgaria*, paragraph 177; Judgment in Case 22597/16 – *R.B.* v *Estonia*, paragraph 78. See also: Guide on Article 3 of the European Convention on Human Rights, Council of Europe and European Court of Human Rights, August 2022, p. 24.

409 Judgment in Case 29272/98 – *M.C.* v *Bulgaria*, paragraph 150; Judgment in Case 5786/08 – *Söderman* v *Sweden,* paragraph 82.

410 Judgment in Case 22457/16 – *X and Others* v *Bulgaria*, paragraph 182.

411 Judgment in Case 35810/09 – *O'Keeffe* v *Ireland,* paragraph 148.

412 Judgment in Case 22457/16 – *X and Others* v *Bulgaria*, paragraph 192.

413 Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, European Commission, May 2022, Articles 7 to 10.

414 Ibid., Articles 12 and 13.

Article 6: Right to liberty and security

Article 6 is the first right enlisted under the "Freedoms" chapter of the Charter. It establishes that 'everyone has the right to liberty and security of the person.' It corresponds to the right established by Article 5 ECHR, which is primarily focused on the physical liberty and prohibition of unlawful detention.[415] The jurisprudence of both Courts focuses predominantly on those aspects. [416] The remaining question is whether the right to security, stipulated in Article 6 of the Charter, raises any positive obligations of the State to guarantee security of persons by, i.a., introducing specific legislative or regulatory measures.

In this context, the CJEU in *La Quadrature du Net* indicated clearly that "since that provision applies to deprivations of liberty by a public authority, Article 6 of the Charter cannot be interpreted as imposing an obligation on public authorities to take specific measures to prevent and punish certain criminal offences".[417] At the same time, the CJEU indicated that such obligations, regarding "in particular, effective action to combat criminal offences committed against, inter alia, minors and other vulnerable persons", may result from Articles 3, 4 and 7 of the Charter (the right to integrity, prohibition of torture and inhumane or degrading treatment, and the right to private life).[418] These articles are discussed in the relevant sections of this annex.

Impact of CSA proposal on Article 6

The analysed proposed Regulation introduces certain provisions regarding the cross-border cooperation among national coordinating authorities and the possibility of them undertaking joint investigations. At the same time, the CSA proposal might lead to increased detection of online CSA (see Chapter 3). In that context, it may be highlighted that the considerations right to liberty and security (Article 6) of the alleged perpetrators would be relevant in the future. However, as none of the proposed measures introduce changes in that regard, it is noted that the CSA proposal does not pertain directly to Article 6 of the Charter. In the light of the abovementioned case law, it is concluded that the CSA proposal does not directly impact the right to liberty and security.

Article 7: Right of private and family life, home and communications

Following Article 7 of the Charter 'everyone has the right to respect for his or her private and family life, home and communications'. The scope of this Article is broad and consists of four components: the protection of private life, family life, home and communications.

The rights guaranteed under Article 7 of the Charter involve that in principle there shall be no interference by a public authority with the exercise of this right.[419] In other words, public authorities should respect people's private and family life, and more specifically their home and communications. Importantly, as emphasised in the case *La Quadrature du Net*, from Article 7 does not only follow a prohibition for public authorities to interfere with people's private and family lives but it also creates an active obligation for the public authorities to adopt legal measures that effectively protect private and family life.[420] The failure by public authorities to adopt effective

---

415 Peers et al. 'The EU Charter of Fundamental Rights: A Commentary', 2021, p. 115.

416 Guide on Article 5 of the European Convention on Human Rights, Council of Europe and European Court of Human Rights, August 2022.

417 Judgment in Joined Cases C-511/18, C-512/18 and C-520/18 – *La Quadrature du Net,* paragraph 125.

418 Ibid.

419 EU Charter of Fundamental Rights: Article 7 – Respect for private and family life, European Union Agency for Fundamental Rights, December 2007.

420 Judgment in Joined Cases C-511/18, C-512/18 and C-520/18 – *La Quadrature du Net*, paragraph 126. See also: Judgment in Case C-78/18 – *European Commission* v *Hungary,* paragraph 123.

legislation that protects private and family life can thus also be qualified as interference with Article 7.

The CJEU did not yet provide a clear definition of 'private life'. However, this does in practice not matter much as the applicability of Article 7 will be beyond doubt in most cases.[421] This aligns with the view held by the European Court of Human Rights as expressed in the case *Niemitz vs. Germany* that it is not possible or necessary to provide an 'exhaustive definition of the notion of "private life"'.[422] In the same case, the European Court of Human Rights stated that also private and business activities fall in the scope of 'private life'.

Impact of CSA proposal on Article 7

Following the case law of the CJEU, public authorities have a positive duty to prevent people from infringing on each other's private lives.[423] Following this line of thought by the CJEU involves that public authorities ought to actively protect children's private lives. However, it needs to be noted that the CSA proposal potentially affects the children's privacy rights in two opposite directions. First, providing a regulatory framework for improved detection and removal of the CSAM material may have a positive impact on safeguarding children's private lives as protected by Article 7, especially if this provides for quicker removal of the CSAM, preventing its dissemination online. It needs to be noted, however, that such a positive impact is conditional on whether the detection would increase, or the deterrent effect of the proposed Regulation would lead to a decrease in generation and/or dissemination of CSAM online. This is an assumption made in the CSA proposal IA, which however have not been supported by sufficient evidence (see Chapter 3).

On the other hand, the proposed Regulation does not provide any indication regarding the subsequent procedure regarding investigation and persecution of the detected CSAM, notably, as regards the principles that should guide the investigations including children victims or other children who may have encountered CSAM online. Potentially, this can be a serious gap in the proposal, as the stage of investigation and persecution poses particular risks to children's privacy especially where the child's social and sexual life, sexual orientation, and similarly sensitive information are referred to by LEA in the investigation.[424] This gap is however rather limited due to the fact that the Law Enforcement Directive can supplement the CSA proposal by offering an appropriate legal framework that limits this negative impact on the private life of victims.

Article 24: Rights of the Child

Article 24 establishes that 'Children shall have the right to such protection and care as is necessary for their well-being. They may express their views freely. Such views shall be taken into consideration on matters which concern them in accordance with their age and maturity. In all action relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration.'

As indicated in the Explanatory note to the Charter, this Article has been based on the UN Convention on the Rights of the Child (CRC)[425] [426] Two key elements of the rights of the Child are particularly relevant for the present analysis: the right to protection and care to guarantee children's well-being, and the primacy of a child's best interest consideration in all action relating to children.

---

421 Peers et al. 'The EU Charter of Fundamental Rights: A Commentary', 2021, p. 154.

422 Judgment in Case 13719/88 – *Niemitz* v *Germany*, paragraph 29.

423 Judgment in Joined Cases C-511/18, C-512/18 and C-520/18 – *La Quadrature du Net,* paragraph 125.

424 Expert input by service provider and NGO.

425 United Nations Convention on the Rights of the Child, November 1989.

426 Explanations relating to the Charter of Fundamental Rights, European Union, December 2007, Article 24.

Regarding protection, Article 34 the CRC requires States Parties to protect children against 'all forms of sexual exploitation and sexual abuse', which encompasses coercion or inducement of a child into any unlawful sexual activity, the exploitation of children in unlawful sexual practices or prostitution, as well as exploitation of children in pornography.[427] In pursuing that goal, the EU introduced its Directive on combating the sexual abuse and sexual exploitation of children and child pornography in 2011.[428] The Directive defines the scope of CSA and introduces minimum rules regarding criminal qualifications of different sexual abuse acts. The CSA proposal explicitly refers to the definitions therein. The intention to strengthen the protection of the rights of the child was further underlined in The EU Strategy on the Rights of the Child and the European Child Guarantee.[429] Its thematic area 3 focuses specifically on Combating violence against children and ensuring child protection.[430] In the regional international context, the rules for protection of children from sexual abuse has been further stipulated in the Lanzarote Convention which has been ratified by all EU Member states.[431] The Lanzarote Convention introduces mandatory criminalisation of all acts of CSA and highlights the need for prevention and education in that regard.[432] The Council of Europe Convention on preventing and combating violence against women and domestic violence (the Istanbul Convention)[433] as well as the Convention on Cybercrime are also of relevance.[434]

In terms of the scope, the right to protection and care, stipulated by Article 24 entails, importantly, preventing children from any forms of violence. As specified by the United Nations Committee on the Rights of the Child, in the context of the rights of the child the violence refers not only to physical and / or intentional harm, but also non-physical and / or non-intentional forms of harm (for example, neglect and psychological maltreatment).[435] Moreover, the Committee underlined that, as regards sexual abuse, "Many children experience sexual victimisation which is not accompanied by physical force or restraint but which is nonetheless psychologically intrusive, exploitive and traumatic".[436] Online sexual child abuse is particularly damaging, as it inflicts harm not only at the moment when the picture or recording (or, mutatis mutandis, the streaming) is taken, but also "every time the images and videos are posted, circulated and viewed". [437] The awareness of the material being

[427] Convention of the Rights of the Child, United Nations, November 1989, Article 34.

[428] Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography.

[429] The EU Strategy on the Rights of the Child and the European Child Guarantee, European Commission website, accessed 6 February 2023.

[430] Combating violence against children and ensuring child protection, European Commission website, accessed 6 February 2023.

[431] Implementation Report: the Protection of Children Against Sexual Exploitation and Sexual Abuse Facilitated by Information and Communication Technologies (ICTs), Council of Europe, March 2022. p. 8.

[432] Explanatory Report to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, October 2007.

[433] Council of Europe Convention on preventing and combating violence against women and domestic violence, May 2011.

[434] Convention on Cybercrime, Council of Europe, November 2001.

[435] Convention on the Rights of the Child, The right of the child to freedom from all forms of violence, United Nations Committee on the Rights of the Child, April 2011, p. 4.

[436] Ibid., p.10.

[437] Report assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, European Commission, 2016, p. 3,

publicly available, and the mere potentiality of encounter for its viewers in real life, is traumatising and inflicting additional suffering on the child victims.[438]

Both the CJEU as well as the ECtHR interpreted violence against children as an indication that CSA constitutes serious crime, which inflicts a positive obligation on the state stemming from Articles 3, 4 and 7 of the Charter (see discussion on those provisions above).[439] It has been underlined by the CJEU in the context of possible limitations to the right of privacy in La Quadrature du Net.[440] Moreover, the ECtHR referred to the understanding of the best interests of children as provided by the UN Committee on the Rights of the Child, i.e., that the interpretation of a child's best interests must be consistent with the whole Convention [on the Rights of the Child], including the obligation to protect children from all forms of violence.[441] This indicates that children's best interests, especially when children's physical and mental integrity and dignity are at stake, have a powerful weight, also when other potentially conflicting rights are under consideration.

Impact of CSA proposal on Article 24

Overall, in the light of the analysis above and conditional on the effectiveness of detection and subsequent LEA, the expected impact of the proposed Regulation on the rights of the children should be assessed as positive. The expected positive impact is closely related with the expected positive impact on Articles 1, 3, 4, and 7. However, it needs to be highlighted that the impact of the Proposal on Article 24 should also be considered in light of risks to infringements of children's right to private life from Article 7 (recall that the CSA proposal presents both a potential positive and a potential negative development for children's right to privacy, see the analysis on Article 7 above).

An important caveat, in the context of the CSA proposal, which focuses on the issue of online CSA, concerns potential risks to fundamental rights of children regarding self-generated sexually explicit content. As the Council of Europe Lanzarote Committee indicates, adolescents may also explore and express their sexuality by generating and sharing sexually suggestive or implicit material, without the aim of distributing sexually abusive material.[442] While awareness of consequences of such behaviour depends on the child's age and maturity, publication of such material may render those children vulnerable to sexual perpetrators online.[443] The Committee therefore suggests to, by default, treat the children represented in online sexual material online, even if it is self-generated, as victims, and even for child perpetrators of online CSAM to refer to criminal proceedings only as the last resort.[444]

Moreover, it is proposed that the sexually explicit material generated solely for private use, shared on a voluntary and consensual basis, or received by children unknowingly, are not considered as production, distribution or knowingly obtaining access to child pornography.[445] Neither the

---

438 Ibid.

439 Handbook on European Law relating to the rights of the child, European Agency for Fundamental Rights and Council of Europe, June 2015, pp. 120-121.

440 Judgment in Joined Cases C-511/18, C-512/18 and C-520/18 – *La Quadrature du Net*.

441 Convention on the Rights of the Child, The right of the child to freedom from all forms of violence, United Nations Committee on the Rights of the Child, April 2011, p. 23. This has been emphasised in: Judgment in Case 30808/11 – *A, B and C* v *Latvia,* paragraph 11.

442 Opinion on child sexually suggestive or explicit images and/or videos generated, shared and received by children, Lanzarote Committee, Council of Europe, November 2019, p. 5.

443 Ibid.

444 Ibid., pp. 6-7.

445 Ibid.

Directive on combating the sexual abuse and sexual exploitation of children[446] nor the CSA proposal specify details of the criminal proceedings regarding investigation and persecution of crimes. The question as to whether it can reasonably be expected that the implementation of the proposed Regulation would lead to increased detection of online CSAM is of central importance here (see Chapter 3), including the child self-generated sexually explicit content. Both factual detection rates and the proceedings following detection of the material, including investigation, are important determinants of the impact of the CSA proposal on children's rights. If the assumption that the Proposal will lead to increased detection is true, then so are the chances of its positive impact on children's rights by increased protection. This assumption, however, is contested by the experts, questioning the detection possibilities of technologies available, as well as the capacity of law enforcement authorities to process the predicted amount of cases (including false positives) that such imprecise detection mechanisms could generate.[447] Moreover, the Proposal does not entail any safeguards of children's rights in subsequent proceedings, which raises serious concerns about whether children's right to privacy will be adequately safeguarded (see analysis of Article 7 of the Charter above). In this context, it is worth underlining that the Article 24 (rights of the child) obligation to put children's best interest as the primary consideration should be safeguarded in investigation and criminal proceedings at all times. Moreover, the children's right to integrity in criminal proceedings (Article 3, see earlier discussion), as well as presumption of innocence (Article 48), are potentially of great importance in such cases.

Impact of CSA proposal on fundamental rights of internet users

With respect to internet users, the CSA proposal IA identified that the CSA proposal potentially impacts the fundamental rights laid down in Articles 7, 8, and 11. This also aligns with the case law of the CJEU in which the Court discussed whether legal obligations on providers of information society services to retain and analyse people's private communication data and, in some cases, making this data available to public authorities, can be legitimised under the Charter. These cases have in common that they assess the impact of such a legal obligation as compatible with the fundamental rights of internet users, and more specifically the ones laid down in articles 7, 8 and 11 of the Charter.[448]

Article 7: right of private and family life, home and communications

Article 7 of the Charter notes that 'Everyone has the right to respect for his or her private and family life, home and communications'. The scope of this Article is broad and consists of four components: the protection of private life, family life, home and communications.

The rights guaranteed under Article 7 involve that, in principle, 'there shall be no interference by a public authority with the exercise of this right'.[449] In other words, public authorities should respect people's private and family life, and more specifically, their home and communications. The proposal being studied in this report potentially presents interference with internet users' right to have private communications.

---

446 Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography.

447 Expert input by academics.

448 Judgment in Joined Cases C-293/12 and C-594/12 – *Digital Rights Ireland,* paragraphs 25 and 70; Judgment in Joined Cases C-203/15 and C-698/15 – *Tele2 Sverige*, paragraphs 76 and 91-92; Judgment in Joined Cases C-511/18, C-512/18 and C-520/18 – *La Quadrature du Net*, paragraph 113.

449 EU Charter of Fundamental Rights, European Union Agency for Fundamental Rights, December 2007, Article 7.

People's right to have private communications involves a general prohibition for state authorities on interference with one's personal communications.[450] It includes all sorts of communications, including telephone calls, email, and other forms of internet-based communication. Furthermore, the right encompasses the protection of communications for both private, professional and commercial purposes.[451]

In the context of the Proposal, the CJEU has in different cases considered that retainment and analysis of both meta (in the cases Digital Rights Ireland[452] and Tele2[453]) and content data (in the case *Schrems*)[454] by state authorities fall within the scope of Article 7 of the Charter.[455] The rationale is that, as established in Digital Rights Ireland, the retainment of this data provides very precise conclusions on the private lives of the individuals whose data has been retained.[456]

Impact of CSA proposal on Article 7

The fact that communication data, following a detection order, is being retained, analysed, and, in the case of a positive hit, subsequently shared with the public authorities constitutes interference with Article 7. As established in the case Digital Rights Ireland, it is irrelevant whether this retainment and / or analysis causes actual harm.[457] Finally, in the case of Tele2, the Court established that the retainment of communication data by private providers of information society services who subsequently provide access to this data to state authorities also falls within the scope of Article 7.[458]

Article 8: Protection of Personal Data

According to Article 8 'everyone has the right to the protection of personal data concerning him or her.' Article 8 is closely linked to Article 7 as the origins of the right to data protection lie in the right to privacy.[459] The Charter is unique in recognising data protection as a right separate from the right to privacy.[460]

Following the added explanation in the Charter, the purpose of protection of personal data is to offer protection to individuals with respect to the processing of their personal data. Two important definitions are 'personal data' and 'processing'. According to the GDPR Regulation[461] personal data refers to any information related to an identified or identifiable person. Processing involves any operation performed on this personal data. Any operation is being defined broadly and comprises among others the collection, storage, alteration and dissemination of personal data.[462]

---

450 Handbook on European Data Protection Law, European Union Agency for Fundamental Rights and Council of Europe, April 2018.

451 Peers et al. 'The EU Charter of Fundamental Rights: A Commentary', 2021, p. 161.

452 Judgment in Joined Cases C-293/12 and C-594/12 – *Digital Rights Ireland.*

453 Judgment in Joined Cases C-203/15 and C-698/15 – *Tele2 Sverige.*

454 Judgment in Case C-362/14 – *Maximillian Schrems.*

455 Meta data concerns information about the communication that does not involve the content of the communication. Examples include the identity of the sender, identity of the receiver, duration of the communication etc. Content data involves the content of the communication.

456 Judgment in Joined Cases C-293/12 and C-594/12 – *Digital Rights Ireland*, paragraph 27.

457 Ibid., 33.

458 Judgment in Joined Cases C-203/15 and C-698/15 – *Tele2 Sverige,* paragraph 76.

459 Peers et al. 'The EU Charter of Fundamental Rights: A Commentary', 2021, p. 238.

460 Ibid.

461 Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

462 Ibid., Article 4.

Impact of CSA proposal on Article 8

Under Article 8 any processing of personal data should be subject to appropriate protection under article 8.[463] The CSA proposal requests that providers of information society services after having received a detection order retain and analyse communication data, and, if CSAM is being detected, forward it to a public authority. All these activities can be qualified as data processing activities and fall thus within the scope of Article 8.

Article 11: Freedom of expression and information

Article 11 prescribes that 'everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontier'. Although the Charter does not define 'expression'[464], the right consists of, among others, the following elements:[465]

(41) The right to hold opinions

(42) The right to impart information and ideas

(43) The right to receive information and ideas

Importantly, the right provides thus a prohibition for public authorities to restrict people's ability to both send and receive information and ideas.[466] Article 11 applies independently of whether the information is being transmitted orally, written, printed or in electronic form[467] and also includes the right to access dissemination networks.[468]

Impact of CSA proposal on Article 11

The CSA proposal involves that providers of information society services, after having received a detection order, retain and analyse communication data and, if there is a positive hit that potentially CSAM is being exchanged, report this to the public authorities. As expressed in *La Quadrature du Net*, the fact that providers of information society services retain communication data for policing purposes already infringes with Article 11 as it may potentially deter people from openly expressing their views.[469]

Impact of the CSA proposal on fundamental rights of information society service providers

Concerning internet users, the CSA proposal IA identified that the Proposal potentially impacts the fundamental right lied down in Article 16.

---

463 Handbook on European Data Protection Law, European Union Agency for Fundamental Rights and Council of Europe, April 2018, p. 20.

464 Peers et al. 'The EU Charter of Fundamental Rights: A Commentary', 2021, p. 346.

465 Ibid., p. 334.

466 Ibid., p. 348.

467 Ibid., p. 346.; Judgment in Case C-316/09 – *MSD Sharp & Dohme GmbH* v *Merckle GmbH*, paragraph 29.

468 Ibid., p. 349.

469 Judgment in Joined Cases C-511/18, C-512/18 and C-520/18 – *La Quadrature du Net*, paragraph 118. See also: Judgment in Joined Cases C-293/12 and C-594/12 – *Digital Rights Ireland*, paragraph 28.

Article 16: freedom to conduct a business

Article 16 prescribes: 'the freedom to conduct a business in accordance with Community law and national laws and practices is recognised'. Article 16 is unique in the sense that no similar provisions exist in other international human rights treaties.[470] The right to conduct a business involves any legitimate form of profit-making activity conducted by one or more individuals. The rights encompass the full life cycle of such activities from setting-up, operating to closing (i.e., liquidating) a business.[471]

The main aim of acknowledging the right to conduct a business is to safeguard the right to each individual in the EU to operate a business without being subject to either discrimination or disproportionate restrictions. In this context, three recognised pillars by the CJEU pillars are: the freedom to exercise an economic or commercial activity, the freedom of contract and the freedom of competition.[472] The right does not necessarily require a trans-border element.[473]

As such, it can be deduced that the scope of Article 16 can be considered as broad. In the context of this Proposal, it is useful to focus on a specific line of case law that weighs the balancing of the right to conduct a business with the right to intellectual property. In the cases *Scarlet Extended*[474] and *Netlog*[475] the Court needed to assess whether Article 16 precludes EU legislation imposing an obligation on providers of information society services to implement technology that screens communications of its users on intellectual property rights infringements. In these cases, the Court held that imposing a general obligation on providers of information society services to install and maintain a costly computer system to monitor all electronic communications made through its network limits the freedom to conduct a business for providers of information society services. At the same time, some differences between the analysed cases are important for the analysis and CSA proposal IA. Firstly, the CSA proposal introduces targeted obligation to detect and remove or block content based on court order, which should specify the details and timespan of these obligations.[476] It also provides for redress measures for the platforms.[477] Secondly, the services providers obliged to detect CSAM are entitled to access the necessary technology free of charge.[478] Thirdly, the intellectual property rights infringement and CSA are different in kind, the latter being considered by CJEU as a serious crime that warrants positive obligation of the State to prevent it (see analysis of Articles 3, 4 and 24 of the Charter above).

Impact of CSA proposal on Article 16

As mentioned, the CJEU decided in the cases *Scarlet Extended* and *Netlog* that imposing a general obligation on providers of information society services to install and maintain a costly computer system to monitor all electronic communications made through its network infringes with the freedom to conduct a business of providers of information society services. The CSA proposal that is being studied in this report provides providers of information society services, after they have

---

470 Freedom to conduct a business: exploring the dimension of a fundamental right, European Agency for Fundamental Rights, 2015, p.10.

471 Ibidl, p. 11.

472 Ibid., p. 21.

473 Ibid.

474 Judgment in Case C-70/10 – *Scarlet Extended*.

475 Judgment in Case C-360/10 – *(SABAM)* v *Netlog*.

476 Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, European Commission, May 2022, Articles 7-11 and 14-18.

477 Ibid.

478 Ibid., Article 10.

received a detection order, with an obligation to screen the content, including the exchanged communications on its network in order to detect CSAM. Based on the text of Proposal and CSA proposal IA, the precise impact on the right to conduct a business cannot be assessed. While negative impact can be expected, it is worth underlining that the Proposal provides for a procedural safeguard and allows the platforms to challenge the detection orders, to limit the infringement of the rights of business owners.[479]

[479] Ibid., Article 15.

ANNEX V - CBA calculations and reflections

Annex to section 6.4

Correction of costs for Option C

The annual costs for Option C have been slightly corrected by the researchers.

In the CSA proposal IA, it is noted that there were several costs differences between costs in Option C and costs in Option B. The differences per cost component, as provided in the CSA proposal IA, expressed in percentages, are presented in Table 21 and Table 22. When the percentage is larger than 100%, Option C is more expensive than Option B. When the percentage is lower than 100%, Option C is less expensive than Option B.

For (total) staff expenditure, Option C is 9% less expensive from year 6 onwards (when the Centre is deemed fully operational within the Impact Assessment) than Option B and 4% more expensive than Option D. For salaries and allowances, the CSA proposal IA finds Option C to be 12% less expensive from year 6 onwards (when the EU Centre is deemed fully operational within the IA) than Option B and 2% more expensive than Option D. The main reason for this is that salaries and allowances are lower in Option C as compared to Option B, as overhead can be shared with the existing Europol overhead, but that new overhead has to be established for the separate entity. The costs for staff recruitment are found to be twice as large, as both entities have to invest in recruitment (whereas these costs in Option B and D only occur once). Mission expenses are 33% higher, indicating that missions are both conducted by Europol and the separate entity, and as such, are less efficient, but these expenses do not double as compared to Option B or Option D. The costs for socio- and medical infrastructure and training are higher in Option C is well, which is again because the costs are incurred by both entities. However, the costs are not doubled.

For infrastructure and operating expenditure, the CSA proposal IA finds Option C to be 13% more expensive than Option B and D from year 6 onwards (when the EU Centre is deemed fully operational within the CSA proposal IA). The costs associated with the rental of buildings and ICT are equal in all options. The same applies to the operating costs of the database of indicators. The differences in cost between Option C and Option B and D are mainly associated with movable property and associated costs and current administrative expenditure. These costs are twice as high in Option C, as these costs occur twice. This seems reasonable, given that there are two buildings and (essentially) two entities setup in Option C. The auditing costs are higher as well. The costs for the audit at the separate entity is equal to the auditing costs of Option B and D. The additional cost for the audit of Europol is the main driver of the difference in costs. However, the costs are not doubled.

It is interesting to note the observed cost differences within the operational expenditures. The costs for operational activities and support to expert networks are significantly lower in Option C when compared with Option B and D. No explanation is offered for this, but the researchers consider that these are lower as Europol already has an established network and, as such, requires fewer additional resources to host technical meetings with stakeholders or support expert networks. Thereby, it seems reasonable that also the burden for the network partners (notably law enforcement authorities) is lower. Costs associated to communications are 20% higher and costs associated with translation and interpretation are 80% higher. This seems logical, considering inefficiencies as two entities are established. However, they also do not double, which is logical given that the different entities are provided with specific and different functions (and as such do not do 'everything' twice).

For publishing and research dissemination, the costs in Option C are twice as high. According to the researchers, this is not logical. Just as for communication, translation and interpretation, socio/medical infrastructure and training, and mission expenses, not all activities are incurred twice. For example, the researchers see no reason why, under Option C, twice as many publications would be expected. Although some overlap in research dissemination might exist, it is not expected that these costs are fully incurred twice. Thereby, the researchers choose to correct this estimate. The researchers thereby take the average of cost components that are incurred by both entities, but for which it is expected that costs are not fully incurred twice (the above-mentioned components).

As a result, the researchers expect the costs associated to publishing and research dissemination under Option C to be 50% higher than in Option B and D, instead of 100%. This percentage is the average of 1.33 (mission expenses), 1.6 (socio/medical infrastructure and training), 1.8 (translation and interpretation) and 1.2 (communication). As a result, the costs for publishing and research dissemination in Option C decrease from € 1,000,000 to € 750,000 once the EU Centre is fully operational.

Table 22: Relative difference in costs between Option C and Option B

Differences between costs in option C versus costs in option B										
Differences option C (Europol and seperate entity) verus Option B	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10
Staff expenditure of the Centre										
Salaries & allowance	133%	140%	90%	81%	77%	88%	88%	88%	88%	88%
Expenditure relating to Staff recruitment	100%	100%	92%	150%	200%	200%	200%	200%	200%	200%
Mission expenses	117%	117%	133%	130%	133%	133%	133%	133%	133%	133%
Socio/medical infrastructure & training	133%	150%	150%	150%	160%	160%	160%	160%	160%	160%
Total staff costs	**127%**	**135%**	**92%**	**85%**	**81%**	**91%**	**91%**	**91%**	**91%**	**91%**
Infrastructure and operating expenditure of the Centre										
Rental of buildings and associated costs	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
ICT (not related to database)	81%	93%	93%	100%	100%	100%	100%	100%	100%	100%
Databases of indicators										
• Technical maintenance		100%	100%	100%	100%	100%	100%	100%	100%	100%
• Allowance for annual hardware licensing	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
• Annual hosting for databases	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
Movable property and associated costs	200%	200%	200%	200%	200%	200%	200%	200%	200%	200%
Current administrative expenditure	200%	200%	200%	200%	200%	200%	200%	200%	200%	200%
Audits	140%	140%	140%	140%	140%	140%	140%	140%	140%	140%
Total infrastructure costs	**105%**	**110%**	**110%**	**112%**	**113%**	**113%**	**113%**	**113%**	**113%**	**113%**
Operational expenditure										
Operational activities (e.g. technical meetings with stakeholders)	40%	25%	20%	20%	25%	40%	40%	40%	40%	40%
Support to expert networks (coordination activities, meetings)	110%	105%	103%	104%	80%	81%	81%	81%	81%	81%
Translation and interpretation	117%	127%	125%	150%	160%	180%	180%	180%	180%	180%
Publishing and research dissemination	200%	200%	200%	200%	200%	200%	200%	200%	200%	200%
Communication (incl. campaigns)	110%	117%	114%	115%	120%	120%	120%	120%	120%	120%
Total operational expenditure	**95%**	**88%**	**83%**	**85%**	**84%**	**91%**	**91%**	**91%**	**91%**	**91%**
TOTAL EXPENDITURE	**114%**	**117%**	**93%**	**88%**	**85%**	**94%**	**94%**	**94%**	**94%**	**94%**

Source: Calculations by researchers based on the values provided in the CSA proposal IA.

Table 23: Relative difference in costs between Option C and Option D

Differences between costs in option C versus costs in option D										
Differences option C (Europol and seperate entity) verus Option D	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10
Staff expenditure of the Centre										
Salaries & allowance	133%	140%	90%	95%	88%	102%	102%	102%	102%	102%
Expenditure relating to Staff recruitment	100%	100%	92%	150%	200%	200%	200%	200%	200%	200%
Mission expenses	117%	117%	133%	130%	133%	133%	133%	133%	133%	133%
Socio/medical infrastructure & training	133%	150%	150%	150%	160%	160%	160%	160%	160%	160%
Total staff costs	**127%**	**135%**	**92%**	**99%**	**92%**	**104%**	**104%**	**104%**	**104%**	**104%**
Infrastructure and operating expenditure of the Centre										
Rental of buildings and associated costs	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
ICT (not related to database)	81%	93%	93%	100%	100%	100%	100%	100%	100%	100%
Databases of indicators										
• Technical maintenance		100%	100%	100%	100%	100%	100%	100%	100%	100%
• Allowance for annual hardware licensing	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
• Annual hosting for databases	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
Movable property and associated costs	200%	200%	200%	200%	200%	200%	200%	200%	200%	200%
Current administrative expenditure	200%	200%	200%	200%	200%	200%	200%	200%	200%	200%
Audits	140%	140%	140%	140%	140%	140%	140%	140%	140%	140%
Total infrastructure costs	**105%**	**110%**	**110%**	**112%**	**113%**	**113%**	**113%**	**113%**	**113%**	**113%**
Operational expenditure										
Operational activities (e.g. technical meetings with stakeholders)	40%	25%	20%	20%	25%	40%	40%	40%	40%	40%
Support to expert networks (coordination activities, meetings)	110%	105%	103%	104%	80%	81%	81%	81%	81%	81%
Translation and interpretation	117%	127%	125%	150%	160%	180%	180%	180%	180%	180%
Publishing and research dissemination	200%	200%	200%	200%	200%	200%	200%	200%	200%	200%
Communication (incl. campaigns)	110%	117%	114%	115%	120%	120%	120%	120%	120%	120%
Total operational expenditure	**95%**	**88%**	**83%**	**85%**	**84%**	**91%**	**91%**	**91%**	**91%**	**91%**
TOTAL EXPENDITURE	**114%**	**117%**	**93%**	**97%**	**93%**	**102%**	**102%**	**102%**	**102%**	**102%**

Source: Calculations by researchers based on the values provided in the CSA proposal IA.

Differences in implementation time

The following table offers an overview of existing agencies and their ramp-up in staffing.

Table 24: Overview of existing agencies and their ramp-up in staffing

FRA		
Established	**2007**	
Staffing		
2007	45	https://fra.europa.eu/sites/default/files/fra-external_evaluation-final-report.pdf
2008	56	https://fra.europa.eu/sites/default/files/fra-external_evaluation-final-report.pdf
2009	81	https://fra.europa.eu/sites/default/files/fra-external_evaluation-final-report.pdf
2010	94	https://fra.europa.eu/sites/default/files/fra-external_evaluation-final-report.pdf
2011	109	https://fra.europa.eu/sites/default/files/fra-external_evaluation-final-report.pdf
2012	117	https://fra.europa.eu/sites/default/files/fra-external_evaluation-final-report.pdf
2013	116	https://www.eca.europa.eu/Lists/ECADocuments/FRA_2013/FRA_2013_EN.pdf
2014	110	https://www.eca.europa.eu/Lists/ECADocuments/FRA_2015/FRA_2015_EN.pdf
2015	107	https://www.eca.europa.eu/Lists/ECADocuments/FRA_2015/FRA_2015_EN.pdf
CEPOL		
Established	2005	
Staffing		
2005	?	https://www.cepol.europa.eu/api/assets/CEPOL_5_Year_Evaluation.pdf
2006	15	https://www.cepol.europa.eu/api/assets/CEPOL_5_Year_Evaluation.pdf
2007	21	https://www.cepol.europa.eu/api/assets/CEPOL_5_Year_Evaluation.pdf
2008	27	https://www.cepol.europa.eu/api/assets/CEPOL_5_Year_Evaluation.pdf
2009	28	https://www.cepol.europa.eu/api/assets/CEPOL_5_Year_Evaluation.pdf
2010	31	https://www.eca.europa.eu/Lists/ECADocuments/CEPOL_2010/CEPOL_2010_EN.PDF
EUROPOL		
Established	1998	
Staffing		
1999	53	https://www.europol.europa.eu/sites/default/files/documents/annualreport2008.pdf
2000	144	https://www.europol.europa.eu/sites/default/files/documents/annualreport2008.pdf
2001	323	https://www.europol.europa.eu/sites/default/files/documents/annualreport2008.pdf
2002	386	https://www.europol.europa.eu/sites/default/files/documents/annualreport2008.pdf
2003	426	https://www.europol.europa.eu/sites/default/files/documents/annualreport2008.pdf
2004	493	https://www.europol.europa.eu/sites/default/files/documents/annualreport2008.pdf
2005	536	https://www.europol.europa.eu/sites/default/files/documents/annualreport2008.pdf
2006	566	https://www.europol.europa.eu/sites/default/files/documents/annualreport2008.pdf
2007	592	https://www.europol.europa.eu/sites/default/files/documents/annualreport2008.pdf
2008	622	https://www.europol.europa.eu/sites/default/files/documents/annualreport2008.pdf
EMSA		
Established	2002	
Staffing		
2002		
2003	40	https://www.eca.europa.eu/Lists/ECADocuments/EMSA_2004/EMSA_2004_EN.PDF
2004	55	https://www.eca.europa.eu/Lists/ECADocuments/EMSA_2004/EMSA_2004_EN.PDF
2005	95	https://www.eca.europa.eu/Lists/ECADocuments/EMSA_2005/EMSA_2005_EN.PDF
2006	132	https://www.eca.europa.eu/lists/ecadocuments/aesm_2006/aesm_2006_en.pdf
2007	153	https://www.eca.europa.eu/Lists/ECADocuments/EMSA_2008/EMSA_2008_EN.PDF
2008	181	https://www.eca.europa.eu/Lists/ECADocuments/EMSA_2008/EMSA_2008_EN.PDF
2009	192	https://www.eca.europa.eu/Lists/ECADocuments/EMSA_2010/EMSA_2010_EN.PDF
2010	200	https://www.eca.europa.eu/Lists/ECADocuments/EMSA_2011/EMSA_2011_EN.PDF
2011	208	https://www.eca.europa.eu/Lists/ECADocuments/EMSA_2011/EMSA_2011_EN.PDF
EASA		
Established	2002	
2002		
2003	17	https://www.eca.europa.eu/Lists/ECADocuments/EASA_2004/EASA_2004_EN.PDF
2004	102	https://www.eca.europa.eu/Lists/ECADocuments/EASA_2004/EASA_2004_EN.PDF
2005	153	https://www.eca.europa.eu/Lists/ECADocuments/EASA_2005/EASA_2005_EN.PDF
2006	276	https://www.eca.europa.eu/Lists/ECADocuments/AESA_2006/AESA_2006_EN.PDF
2007	333	https://www.eca.europa.eu/Lists/ECADocuments/EASA_2008/EASA_2008_EN.PDF
2008	403	https://www.eca.europa.eu/Lists/ECADocuments/EASA_2008/EASA_2008_EN.PDF
2009	506	https://www.eca.europa.eu/Lists/ECADocuments/EASA_2010/EASA_2010_EN.PDF
2010	570	https://www.eca.europa.eu/Lists/ECADocuments/EASA_2010/EASA_2010_EN.PDF
2011	574	https://www.eca.europa.eu/Lists/ECADocuments/EASA_2011/EASA_2011_EN.PDF
2012	647	https://www.eca.europa.eu/Lists/ECADocuments/EASA_2013/EASA_2013_EN.pdf
2013	692	https://www.eca.europa.eu/Lists/ECADocuments/EASA_2013/EASA_2013_EN.pdf
2014	740	https://www.eca.europa.eu/Lists/ECADocuments/SUMMARY_AGENCIES_2015/RAS-Summary_report_2015-EN.pdf
2015	779	https://www.eca.europa.eu/Lists/ECADocuments/EASA_2016/EASA_2016_EN.pdf
2016	774	https://www.eca.europa.eu/Lists/ECADocuments/EASA_2016/EASA_2016_EN.pdf
2017	771	https://www.eca.europa.eu/Lists/ECADocuments/AGENCIES_2017/AGENCIES_2017_EN.pdf
2018	767	https://www.eca.europa.eu/Lists/ECADocuments/EASA_2019/EASA_2019_EN.pdf
2019	762	https://www.eca.europa.eu/Lists/ECADocuments/EASA_2019/EASA_2019_EN.pdf

Source: Ecorys

As the researchers consider that some options can be implemented quicker than others, a second correction in costs is derived. The difference per option is presented below. The correction in costs for Option C are taken into account in 'new' but not in 'original'. The costs in Year 1 include the initial investment costs (such as database costs and housing costs).

Table 25: Overview of EU Centre costs per option and year, including corrections in million Euro

Option	1	2	3	4	5	6	7	8	9	10
B: original	13.3	11.7	18.2	22.6	**25.7**	25.7	25.7	25.7	25.7	25.7
B: new	13.3	11.7	18.2	22.6	**25.7**	25.7	25.7	25.7	25.7	25.7
C: original	14.4	13.7	16.9	19.9	22.0	**24.1**	24.1	24.1	24.1	24.1
C: new	18.5	19.7	**23.9**	23.9	23.9	23.9	23.9	23.9	23.9	23.9
D: original	12.3	11.7	18.2	20.6	**23.7**	23.7	23.7	23.7	23.7	23.7
D: new	15.0	16.4	19.0	**23.7**	23.7	23.7	23.7	23.7	23.7	23.7

Source: Calculations by researchers based on the values provided in the CSA proposal IA. Numbers are rounded to one decimal.

Annex to Section 6.5

Estimated benefit of the Centre

The benefits of the EU Centre are assumed to equal a 6% reduction in CSAM-costs, once the EU Centre is fully operational within Option B and D.

For Option C, the effectiveness is perceived to be slightly lower, due to a somewhat limited effectiveness in victim assistance (as the function is scattered between two agencies). The perceived benefit of the function 'victim assistance', within the three functions that the EU Centre should have, is estimated by the number of staff employed dedicated to this function. The number of staff employed for victim assistance (excl. overhead) is 10, which represents 11% of the total number of staff (90) employed by the EU Centre (excl. overhead). Thereby, the benefit of the function 'victim assistance' is estimated at 0.67% in Option B and D. In Option C, it is assumed that the EU Centre is 50% less effective. As a result, it is only able to offer 0.33% of the benefit.

The total benefit of Option C is thereby calculated at 5.67%.

Benefit calculations per year

Adopting an annual cost of CSAM of 13.8 billion Euro (similar to the value in the CSA proposal) and the estimated benefit, the benefits are calculated per year.

Table 26: Overview of EU Centre benefits per option and year, in million Euro

Option	1	2	3	4	5	6	7	8	9	10
B: orig.	0	0	0	0	1,242.0	1,242.0	1,242.0	1,242.0	1,242.0	1,242.0
B: new	0	0	0	0	828.0	828.0	828.0	828.0	828.0	828.0
C: orig.	0	0	0	0	828.0	828.0	828.0	828.0	828.0	828.0
C: new	0	0	782.0	782.0	782.0	782.0	782.0	782.0	782.0	782.0
D: orig.	0	0	0	0	828.0	828.0	828.0	828.0	828.0	828.0
D: new	0	0	0	828.0	828.0	828.0	828.0	828.0	828.0	828.0

Source: Calculations by researchers based on the values provided in the CSA proposal IA. Numbers are rounded to one decimal.

Annex to Section 6.6

Present value calculations

The costs are discounted adopting a 3% discount rate, which is the social discount factor recommended for EU policy analysis in Tool #64 of the Better Regulation Guidelines. The costs are calculated to year 0 (today). The cost estimate in year n is weighted for 1/(1+0,03)^n. For example, the cost estimate in year 1 is thereby only weighted for 97.1% (1/(1+0,03)^1). In the table 'orig.' indicates the discounted costs for the options as presented in the IA. In the table, 'new' indicates the discounted costs for the options adopting corrections by the researchers.

Table 27: Discounted costs per option and year, including corrections in million Euro

Option	PV	1	2	3	4	5	6	7	8	9	10
B: orig.	**184.3**	12.9	11.0	16.6	20.0	22.2	21.5	20.9	20.3	19.7	19.1
B: new	**184.3**	12.9	11.0	16.6	20.0	22.2	21.5	20.9	20.3	19.7	19.1
C: orig.	**174.2**	14.0	12.9	15.4	17.7	19.0	20.2	19.6	19.0	18.5	17.9
C: new	**194.3**	17.9	18.6	21.8	21.2	20.6	20.0	19.4	18.8	18.3	17.7
D: orig.	**171.9**	11.9	11.0	16.6	18.3	20.4	19.8	19.3	18.7	18.2	17.6
D: new	**182.6**	14.6	15.5	17.4	21.1	20.4	19.8	19.3	18.7	18.2	17.6

Source: Calculations by researchers based on the values provided in the CSA proposal IA . Numbers are rounded to one decimal.

The benefits are discounted adopting a 3% discount rate, as suggested in Tool #64 of the Better Regulation Guidelines. The costs are calculated to year 0 (today). The benefit estimate in year n is weighted for 1/ (1+0,03)^n. The estimated benefit in year 1 is thereby only weighted for 97.1% (1/(1+0,03)^1). In the table 'orig.' indicates the discounted benefits for the options as presented in the IA. In the table, 'new' indicates the discounted benefits for the options adopting corrections by the researchers.

Table 28: Discounted benefits per option and year, in million Euro

Option	PV	1	2	3	4	5	6	7	8	9	10
B:orig.	**5,977.9**	0	0	0	0	1,071.4	1,040.2	1,009.9	980.4	951.9	924.2
B:new	**3,985.3**	0	0	0	0	714.2	693.4	673.2	653.6	634.6	616.1
C:orig.	**3,985.3**	0	0	0	0	714.2	693.4	673.2	653.6	634.6	616.1
C:new	**5,174.3**	0	0	715.6	694.8	674.6	654.9	635.8	617.3	599.3	581.9
D:orig.	**3,985.3**	0	0	0	0	714.2	693.4	673.2	653.6	634.6	616.1
D:new	**4,720.9**	0	0	0	735.7	714.2	693.4	673.2	653.6	634.6	616.1

Source: Calculations by researchers based on the values provided in the CSA proposal IA. Numbers are rounded to one decimal.

Sensitivity analysis 1: all options fully operational in year 5

Table 29: Overview of EU Centre costs per option and year, in million Euro, SA1

Option	1	2	3	4	5	6	7	8	9	10
B: new	13.3	11.7	18.2	22.6	25.7	25.7	25.7	25.7	25.7	25.7
C: new	14.4	13.7	16.8	19.7	21.7	23.9	23.9	23.9	23.9	23.9
D: new	12.3	11.7	18.2	20.6	23.7	23.7	23.7	23.7	23.7	23.7

Source: Calculations by researchers based on the values provided in the CSA proposal IA

Table 30: Discounted costs per option and year, in million Euro, SA1

Option	PV	1	2	3	4	5	6	7	8	9	10
B: new	**184.3**	12.9	11.0	16.6	20.0	22.2	21.5	20.9	20.3	19.7	19.1
C: new	**172.7**	14.0	12.9	15.4	17.5	18.7	20.0	19.4	18.8	18.3	17.7
D: new	**171.9**	11.9	11.0	16.6	18.3	20.4	19.8	19.3	18.7	18.2	17.6

Source: Calculations by researchers based on the values provided in the CSA proposal IA

Table 31: Overview of EU Centre benefits per option and year, in million Euro, SA1

Option	1	2	3	4	5	6	7	8	9	10
B: new	0.0	0.0	0.0	0.0	828.0	828.0	828.0	828.0	828.0	828.0
C: new	0.0	0.0	0.0	0.0	782.0	782.0	782.0	782.0	782.0	782.0
D: new	0.0	0.0	0.0	0.0	828.0	828.0	828.0	828.0	828.0	828.0

Source: Calculations by researchers based on the values provided in the CSA proposal IA

Table 32: Discounted benefits per option and year, in million Euro, SA1

Option	PV	1	2	3	4	5	6	7	8	9	10
B: new	**3,985.3**	0	0	0	0	714.2	693.4	673.2	653.6	634.6	616.1
C: new	**3,763.8**	0	0	0	0	674.6	654.9	635.8	617.3	599.3	581.9
D: new	**3,985.3**	0	0	0	0	714.2	693.4	673.2	653.6	634.6	616.1

Source: Calculations by researchers based on the values provided in the CSA proposal IA

Table 33: Overview per option in million Euro (in present value year 1 – year 10), SA1

	Option B: Decentralised agency	Option C: Europol+	Option D: FRA integrated
Total costs	184.3	172.7	171.9
Total benefits	3,985.3	3,763.8	3,985.3
Net value	3,800.9	3,591.2	3,813.3

Source: Calculations by researchers based on the values provided in the CSA proposal IA

Sensitivity analysis 2: all functions have equal benefits

Table 34: Overview of EU Centre costs per option and year, in million Euro, SA2

Option	1	2	3	4	5	6	7	8	9	10
B: new	13.3	11.7	18.2	22.6	25.7	25.7	25.7	25.7	25.7	25.7
C: new	18.5	19.7	23.9	23.9	23.9	23.9	23.9	23.9	23.9	23.9
D: new	15.0	16.4	19.0	23.7	23.7	23.7	23.7	23.7	23.7	23.7

Source: Calculations by researchers based on the values provided in the CSA proposal IA

Table 35: Discounted costs per option and year, in million Euro, SA2

Option	PV	1	2	3	4	5	6	7	8	9	10
B: new	**184.3**	12.9	11.0	16.6	20.0	22.2	21.5	20.9	20.3	19.7	19.1
C: new	**194.3**	17.9	18.6	21.8	21.2	20.6	20.0	19.4	18.8	18.3	17.7
D: new	**182.6**	14.6	15.5	17.4	21.1	20.4	19.8	19.3	18.7	18.2	17.6

Source: Calculations by researchers based on the values provided in the CSA proposal IA

Table 36: Overview of EU Centre benefits per option and year, in million Euro, SA2

Option	1	2	3	4	5	6	7	8	9	10
B: new	0.0	0.0	0.0	0.0	828.0	828.0	828.0	828.0	828.0	828.0
C: new	0.0	0.0	690.0	690.0	690.0	690.0	690.0	690.0	690.0	690.0
D: new	0.0	0.0	0.0	828.0	828.0	828.0	828.0	828.0	828.0	828.0

Source: Calculations by researchers based on the values provided in the CSA proposal IA

Table 37: Discounted benefits per option and year, in million Euro, SA2

Option	PV	1	2	3	4	5	6	7	8	9	10
B: new	**3,985.3**	0	0	0	0	714.2	693.4	673.2	653.6	634.6	616.1
C: new	**4,565.5**	0	0	631.4	613.1	595.2	577.9	561.0	544.7	528.8	513.4
D: new	**4,720.9**	0	0	0	735.7	714.2	693.4	673.2	653.6	634.6	616.1

Source: Calculations by researchers based on the values provided in the CSA proposal IA

Table 38: Overview per option in million Euro (in present value year 1 – year 10), SA2

	Option B: Decentralised agency	Option C: Europol+	Option D: FRA integrated
Total costs	184.3	194.3	182.6
Total benefits	3,985.3	4,565.5	4,720.9
Net value	3,800.9	4,371.2	4,538.3

Source: Calculations by researchers based on the values provided in the CSA proposal IA

Sensitivity analysis 3: longer assessment period

Table 39: Overview of EU Centre costs per option and year, in million Euro, SA3

Option	1	2	3	4	5	6	7	8	9	10
B: new	13.3	11.7	18.2	22.6	25.7	25.7	25.7	25.7	25.7	25.7
C: new	18.5	19.7	23.9	23.9	23.9	23.9	23.9	23.9	23.9	23.9
D: new	15.0	16.4	19.0	23.7	23.7	23.7	23.7	23.7	23.7	23.7
Option	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
B: new	25.7	25.7	25.7	25.7	25.7	25.7	25.7	25.7	25.7	25.7
C: new	23.9	23.9	23.9	23.9	23.9	23.9	23.9	23.9	23.9	23.9
D: new	23.7	23.7	23.7	23.7	23.7	23.7	23.7	23.7	23.7	23.7

Source: Calculations by researchers based on the values provided in the CSA proposal IA

Table 40: Discounted costs per option and year, in million Euro, SA3

Option	PV	1	2	3	4	5	6	7	8	9	10
B: new	**347.4**	12.9	11.0	16.6	20.0	22.2	21.5	20.9	20.3	19.7	19.1
C: new	**345.7**	17.9	18.6	21.8	21.2	20.6	20.0	19.4	18.8	18.3	17.7
D: new	**333.0**	14.6	15.5	17.4	21.1	20.4	19.8	19.3	18.7	18.2	17.6
Option	**PV**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
B: new	**347.4**	18.6	18.0	17.5	17.0	16.5	16.0	15.5	15.1	14.7	14.2
C: new	**345.7**	17.2	16.7	16.2	15.8	15.3	14.9	14.4	14.0	13.6	13.2
D: new	**333.0**	17.1	16.6	16.1	15.7	15.2	14.8	14.3	13.9	13.5	13.1

Source: Calculations by researchers based on the values provided in the CSA proposal IA

Table 41: Overview of EU Centre benefits per option and year, in million Euro, SA3

Option	1	2	3	4	5	6	7	8	9	10
B: new	0.0	0.0	0.0	0.0	828.0	828.0	828.0	828.0	828.0	828.0
C: new	0.0	0.0	782.0	782.0	782.0	782.0	782.0	782.0	782.0	782.0
D: new	0.0	0.0	0.0	828.0	828.0	828.0	828.0	828.0	828.0	828.0
Option	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
B: new	828.0	828.0	828.0	828.0	828.0	828.0	828.0	828.0	828.0	828.0
C: new	782.0	782.0	782.0	782.0	782.0	782.0	782.0	782.0	782.0	782.0
D: new	828.0	828.0	828.0	828.0	828.0	828.0	828.0	828.0	828.0	828.0

Source: Calculations by researchers based on the values provided in the CSA proposal IA

Table 42: Discounted benefits per option and year, in million Euro, SA3

Option	PV	1	2	3	4	5	6	7	8	9	10
B:new	**9,240.8**	0	0	0	0	714.2	693.4	673.2	653.6	634.6	616.1
C:new	**10,137.9**	0	0	631.4	613.1	595.2	577.9	561.0	544.7	528.8	513.4
D:new	**9,976.5**	0	0	0	735.7	714.2	693.4	673.2	653.6	634.6	616.1
Option	**PV**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
B:new	**9,240.8**	598.2	580.7	563.8	547.4	531.5	516.0	501.0	486.4	472.2	458.4
C:new	**10,137.9**	564.9	548.5	532.5	517.0	501.9	487.3	473.1	459.3	446.0	433.0
D:new	**9,976.5**	598.2	580.7	563.8	547.4	531.5	516.0	501.0	486.4	472.2	458.4

Source: Calculations by researchers based on the values provided in the CSA proposal IA

Table 43: Overview per option in million Euro (in present value year 1 – year 20), SA3

	Option B: Decentralised agency	Option C: Europol+	Option D: FRA integrated
Total costs	347.4	345.7	333.0
Total benefits	9,240.8	10,137.9	9,976.5
Net value	8,893.4	9,792.1	9,643.4

Source: Calculations by researchers based on the values provided in the CSA proposal IA

QA-07-23-178-EN-N

On 11 May 2022, the European Commission presented a proposal for a regulation laying down rules to prevent and combat child sexual abuse. The European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) has requested this complementary impact assessment of the proposal.

Without disputing the need to protect children against child sexual abuse, this study focuses on specific aspects of the proposal, namely the problem definition, the impact of the proposal on the internet and fundamental rights, as well as the necessity and proportionality of the proposed measures.

This is a publication of the Ex-ante Impact Assessment Unit
EPRS | European Parliamentary Research Service

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

PDF ISBN 978-92-848-0446-7 | doi:10.2861/016876 | QA-07-23-178-EN-N