Commission proposal on the temporary derogation from the e-Privacy Directive for the purpose of fighting online child sexual abuse

Mifsud Bonnici, Jeanne; Tudorica, Melania; Modh, Ketan; Abraha, Halefom Hailu

Commission proposal on the temporary derogation from the e-Privacy Directive for the purpose of fighting online child sexual abuse

Targeted substitute impact assessment

STUDY

EPRS | European Parliamentary Research Service

Ex-Ante Impact Assessment Unit
PE 662.598 – February 2021

EN

Commission proposal on the temporary derogation from the e-Privacy Directive for the purpose of fighting online child sexual abuse

Targeted substitute impact assessment

On 10 September 2020, the European Commission presented a proposal (COM(2020) 568 final) on the temporary derogation from Articles 5(1) and 6 of the e-Privacy Directive, which protect the confidentiality of communications and traffic data. This proposal is targeted at ensuring the continuation of voluntary practices conducted by providers of 'number-independent interpersonal communications services' for the detection, reporting and removal of child sexual abuse material online after the European Electronic Communications Code has entered into force at the end of December 2020.

The European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) raised concerns over the proposal's potential impact on the human and fundamental rights of the users of those services, and requested that the European Parliamentary Research Service (EPRS) carry out a targeted impact assessment to this end, in the absence of a European Commission impact assessment accompanying this proposal.

The assessment finds that while the EU has the competence to adopt the proposed regulation per Article 5 of the Treaty on European Union, the impact of such practices on human and fundamental rights has not been adequately addressed. It should provide a clear legal basis for these practices, along with effective remedies for users. Some technologies covered by the proposed regulation have a disproportionate impact, and thus require additional safeguards unavailable in the proposal in its current form.

EPRS | European Parliamentary Research Service

AUTHORS

This study has been written by Professor Jeanne Pia Mifsud Bonnici and Melania Tudorica of the Security, Technology and e-Privacy (STeP) Research Group at the University of Groningen and Ketan Modh and Halefom Hailu Abraha of the Department of Information Policy and Governance at the University of Malta 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, Ex-Ante Impact Assessment Unit

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

LINGUISTIC VERSIONS

Original: EN

Manuscript completed in January 2021.

DISCLAIMER AND COPYRIGHT

PE 662.598
ISBN: 978-92-846-7691-0
DOI: 978-92-846-7691-0
CAT: QA-02-21-024-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 10 September 2020, the European Commission published a **Proposal for a Regulation for a temporary derogation from certain provisions of Directive 2002/58/EC (e-Privacy Directive) for the purpose of fighting online Child Sexual Abuse (CSA) (COM(2020) 568 final)**. This proposed regulation is in line with the European Union's (EU) strategy for a more effective fight against CSA (COM(2020) 607 final) (adopted on 24 July 2020) which aims to provide an effective response, at EU level, to this offence. The proposed regulation is a temporary measure aimed at allowing tech companies to continue to voluntarily track child sexual abuse material online following the deadline for transposition by Member States of the European Electronic Communications Code Directive (Directive 2018/1972), which passed in December 2020.

The European Electronic Communications Code Directive (EECC Directive) extends the definition of electronic communication services under EU law. In particular, the definition of an electronic communications service now includes internet-based services that do not connect with publicly assigned numbering resources (i.e. a number or numbers in national or international numbering plans). These 'number-independent interpersonal communications services' (NI-ICS), as they are called in the EECC Directive, also include services which use numbers as a mere identifier, such as instant messaging. This change in the definition of electronic communications service will be part of the national transpositions of the e-Privacy Directive once Member States transpose the EECC Directive. Those Member States which failed to meet the transposition deadline of 21 December 2020, must interpret their national rules in light of the wording and the purpose[1] of the EECC Directive, in so far as this is possible and does not, for instance, conflict with the explicit wording of their domestic laws.[2]

The proposed regulation seeks to derogate from the following provisions of the e-Privacy Directive: Article 5(1) (Confidentiality of Communications) and Article 6 (Traffic data), wherein NI-ICS would, in particular, be prohibited from listening, tapping, storing or engaging in other kinds of interception or surveillance of communications and the related traffic data, by persons other than the users themselves, and without the consent of the users concerned, except unless legally authorised to do so. The proposed regulation targets not only current voluntary activities to detect and report CSAM but also voluntary efforts to detect solicitation of children for sexual purposes ("grooming"). Both sets of activities (that is, to detect CSAM and to detect grooming), according to the Commission, "must be limited to the use of existing, state-of-the-art technology that corresponds to the safeguards set out"[3] in the proposed regulation.

The proposed regulation is a temporary regulation and would expire on 31 December 2025. Once the long-term legislation containing more elaborate safeguards, as planned by the Commission and stated in recital 16 of the proposed regulation, has been adopted (before 31 December 2025), the temporary regulation would be repealed.

In the absence of a European Commission impact assessment accompanying this proposal, the European Parliamentary Research Service (EPRS) was asked on 28 October 2020 by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) to carry

---

1 As established in Case 14/83 *Von Colson and Kamann* [1984] ECR 1891. Catherine Barnard and Steve Peers (2014) European Union Law. Oxford University Press p153.

2 In Case C212/04 *Adeneler* [2006] ECR 1-6057 has formulate three possible limits to the duty of consistent interpretation: (a) interpretative methoda recognised by national law; (b) general principles; and (c) no interpretation *contra legem*. Catherine Barnard and Steve Peers (2014) European Union Law. Oxford University Press p157.

3 COM(2020) 568 final on page 2.

out a targeted substitute impact assessment, restricting the analysis to **four main research questions:**

1. What are the impacts of the proposed regulation on EU privacy and data protection rights (e-Privacy Directive and GDPR), as well as EU fundamental rights and the ECHR human rights of persons affected?
2. Does the proposed regulation comply with the principle of proportionality and the principle of subsidiarity, which includes an 'EU added value' test?
3. Are the safeguards provided for in the proposed regulation sufficient to ensure compliance with Article 52(1) of the EU Charter of Fundamental Rights (EU Charter), taking account of the current case law of the CJEU and GDPR rules?
4. What is the impact of the proposed regulation on the right to an effective remedy in accordance with Article 47 of the EU Charter of Fundamental Rights, if the users are not aware that the content of their private communications is being scanned and potentially flagged up for human review?

The targeted substitute impact assessment is based on an external study, which was outsourced by the Ex-Ante Impact Assessment Unit of EPRS. The impact assessment is primarily based on desk research, but the input of stakeholders (including from the European Commission, European Data Protection Supervisor, European Union Agency for Fundamental Rights, Europol and Microsoft) has also been taken into account. The study is limited in scope and was conducted within a limited time frame. Any information on Member States' practices is based on publicly available sources.

The findings of this targeted substitute impact assessment are set out below.

A. EU competence to adopt proposed regulation

With regard to the second question on whether the proposed regulation complies with the principle of proportionality and the principle of subsidiarity, the assessment (in section 2) finds that the proposed regulation respects the principle of subsidiarity (Article 5(3) TEU) because an EU-level action ensures that policies regarding the effective detection, reporting and removal of CSAM online by NI-ICS providers are not fragmented. It also allows the EU to set a higher standard for the protection of the rights of both children and service users than those which may be set by individual Member States, thus showing that there is added value in combating CSA online through an EU-level action.

The principle of proportionality (in terms of Article 5(4) TEU) for EU competence is also respected because the proposed regulation is a targeted and temporary measure that will expire either on 31 December 2025 or once long-term legislation for combating CSA online is adopted (if this happens earlier than the set deadline).

B. Impact on human rights

With regard to the first question on the impact of the proposed regulation on EU privacy and data protection rights (e-Privacy Directive and GDPR) as well as EU fundamental rights and ECHR human rights of persons affected, the assessment finds that the measures envisaged by the proposed regulation could have both positive and negative impacts on a number of fundamental rights and freedoms. While the detection, removal, and reporting of CSAM by NI-ICS may have a positive contribution to the protection of the fundamental rights of the child, the same measures may also negatively affect the fundamental rights of others, such as the users' rights to privacy, data protection and the right to freedom of expression and confidentiality of communications. For this reason, the measures envisaged by the proposed regulation constitute an interference with the exercise of the fundamental rights to confidentiality of communications and protection of personal data.

C. Sufficiency of safeguards in the proposed regulation

Article 52(1) of the Charter sets out specific criteria that must be met by any legislation that seeks to limit the exercise of the rights and freedoms provided by the Charter. These criteria are that: 1) the limitation must be provided for by law; 2) it must respect the essence of the rights; 3) it must genuinely meet the objectives of general interest recognised by the Union; and 4) it must be necessary and proportionate. Sections 3 and 4 of this study examine whether the proposed regulation meets these criteria, since it does interfere with the fundamental rights to confidentiality of communications and the protection of personal data.

To examine the first criterion, which requires any rights limitation to be provided for by law, it is necessary to consider the legal basis used, in this case for the voluntary processing of content or traffic data for the purpose of detecting, removing and reporting CSA online. This is because the proposed regulation does not itself explicitly provide one but leaves it to the NI-ICS providers to determine the legal basis of their practices under Article 6(1)(a) through Article 6(1)(f) of the GDPR. The provisions of the GDPR must be interpreted in light of human and fundamental rights. This assessment finds that Articles 6(1)(a), 6(1)(b), 6(1)(c), and 6(1)(e) of the GDPR would not provide adequate protection to users if they are used as the legal basis, thus making the processing of data illegal. Only Articles 6(1)(d) (for vital interests) and 6(1)(f) (for legitimate interests) could serve as legal bases that would provide adequate protections.

Therefore, the proposed regulation must include clear and explicit language that limits the derogation to the e-Privacy Directive to those voluntary practices expressly conducted using Article 6(1)(d) or 6(1)(f) of the GDPR as their legal basis. Any practices carried out by NI-ICS providers to combat CSA online using any other legal basis should not allow them to be able to avoid their duties and responsibilities under Articles 5(1) and 6 of the e-Privacy Directive.

The second criterion, of 'respecting the essence of the rights', tests whether the right is in effect emptied of its basic content, effectively preventing the individual from exercising the right. Due to the specific standards and safeguards set out under Article 3, the proposed regulation respects the essence of the rights.

The proposed regulation also satisfies the third criterion, of genuinely meeting an objective of general interest. In this case, the objective is the effective prevention, detection, and prosecution of child sexual abuse online, and the protection of victims of this offence. It also provides the protection necessary for the well-being of the child.

It should be noted that meeting the second and third criteria does not necessarily mean that the limitations to the exercise of rights and freedoms provided by the proposed regulation are lawful under EU law. These limitations must also meet the criteria of necessity and proportionality.

Determining whether the requirements of necessity and proportionality are met depends on the detailed factual description of the measure proposed, among other things. However, the proposed regulation is not accompanied by such a detailed explanation of the specific measures or the existence of other measures. Without sufficient evidence to demonstrate that the current practices are effective in fighting CSAM, and that there are no other less intrusive but equally effective alternatives, it is difficult to determine whether the measures envisaged by the proposed regulation would meet the 'strictly necessary and proportionate' test.

Since the impact of the proposed regulation on fundamental rights is being investigated, the effect of the proposed regulation on the voluntary practices used to combat child sexual abuse online must be clarified. Thus, it is necessary to investigate the technologies currently used in these practices for their compliance with Article 3 of the proposed regulation (in Section 3 of this study). These include Microsoft's PhotoDNA (used to detect images and videos known to contain CSAM),

Microsoft's Project Artemis (used to detect text-based child grooming), Facebook's algorithms PDQ and TMK+PDQF (used to detect images and videos known to contain CSAM, as well as other similar images and videos not in the database) and Thorn's Safer tool (which is based on the same technology as Facebook's algorithms). Article 3 of the proposed regulation requires processing of data to be conducted by technologies that are: "well-established" and "regularly in use" (Article 3(a)); "sufficiently reliable" and "least privacy intrusive" (Article 3(b)); and limited to the use of "relevant key indicators" (Article 3(c)).

Due to this formulation of Article 3, the study finds that only Microsoft's PhotoDNA meets all of these requirements. The others, namely Microsoft's Project Artemis, Facebook's algorithms (PDQ and TMK+PDQF) and Thorn's Safer do not fully meet some or all of these requirements. Thus, these service providers may have to stop using and further developing these technologies, even though they may become more effective, well established and less-privacy intrusive in the future. The proposed regulation also does not provide any scope to include these technologies before its expiry on 31 December 2025. Therefore, the objective of the Commission to enable the continuation of certain existing activities aimed at combating child sexual abuse online is only partly met.

Furthermore, the current technologies that would be covered by the proposed regulation are different in terms of accuracy, effectiveness, and level of intrusiveness. Hashing algorithms, which use one-way techniques to transform personally identifiable information into irrevocably randomised identifiers (or cryptographic hashes), are used to convert images and videos into hashes that are stored in a database. Instead of using the original images and videos, comparisons are done against this database. Thus, they are the least-intrusive technologies, meeting the proportionality test. By contrast, other technologies, especially text-based child grooming detection techniques, involve the automated analysis and indiscriminate scanning of the original content of communications and related traffic data. At the same time, they are also prone to errors and vulnerable to abuse. Without clear and precise additional safeguards, these technologies could not meet the necessity and proportionality test under Article 52(1) of the Charter.

The assessment considers additional safeguards (in Section 6 of the study) that can be included in the proposed regulation to meet the requirements of the necessity and proportionality test under Article 52(1) of the Charter. These include: protecting against indiscriminate monitoring; adding nuance by differentiating between safeguards based on the type of technology in use; protecting personal data that are transferred to third countries; receiving prior authorisation from Data Protection Authorities (DPAs); adding a more elaborate internal review mechanism; expanding human oversight before reports are sent to law enforcement; adding safeguards for data retention; clearly carving out end-to-end encryption from the proposed regulation; and improving transparency and accountability.

D. Availability of remedies for impacted persons

With regard to the fourth research question, on the impact of the proposed regulation on the right to an effective remedy in accordance with Article 47 of the Charter, if the users are not aware that the content of their private communications is scanned and potentially flagged up for human review, the assessment (in section 5) finds that the lack of reference to options for effective remedies in the proposed regulation has a significant impact for users.

As the proposed regulation stands, users are dependent on NI-ICS providers voluntarily introducing remedies. Furthermore, following current interpretations of Article 47 of the Charter, the right to an effective remedy cannot be invoked against a private actor (e.g. NI-ICS provider) unless the state shares responsibility in the acts of the private actor. This leaves users who are not aware that the content of their private communications is scanned and potentially flagged up for human review in a position that they cannot avail themselves of their rights as provided for in Article 47 of the Charter.

The assessment also concludes that the remedies provided in the GDPR (Article 77 – to lodge a complaint with a supervisory authority, and Article 79 – right to effective judicial remedy against a controller or a processor) are also not sufficient. The exercise of both these rights is dependent on the user knowing that the decision of the NI-ICS providers to block or suspend access to their account is related or based on the processing of their personal data.

To avoid users being dependent on voluntary remedies introduced by NI-ICS, the proposed regulation should introduce provisions anticipating possible remedies for users that are not restricted to access to court but also include, for instance, a right to inquiry, explanation, reply, correction, apology, reinstatement, reconnection and compensation for actions carried out by a private actor and/or the setting up of a supervisory mechanism for as long as the measures taken by NI-ICS cannot be disclosed (for instance, pending legal investigations or proceedings by competent authorities).

Concluding remarks

In summary, the assessment finds that while the EU has the competence to adopt the proposed regulation per Article 5 TEU, it has significant direct and indirect impacts on human and fundamental rights which have not been addressed. In its current form, there are several problems with the proposed regulation: (a) it explicitly does not provide a legal basis for the voluntary practices used by NI-ICS providers that process communications data to combat child abuse online; (b) it only partially meets the Commission's objective of ensuring the continued use of these technologies; (c) the impact of some of the technologies covered by the proposal are disproportionate in their current form; and (d) there are no effective remedies for users of NI-ICS when they are not aware that they are being monitored.

To alleviate these concerns, the proposed regulation should be amended. This assessment suggests the following major changes: (1) the proposed regulation should include clear and explicit language so that only those practices that use Article 6(1)(d) or Article 6(1)(f) of the GDPR as their legal basis can avail themselves of the derogation from the e-Privacy Directive. Any other legal basis would not provide adequate protections, rendering such data processing illegal; (2) a nuanced approach needs to be taken with regard to the test of proportionality required by Article 52(1) of the Charter. Unlike cryptographic hashes, those technologies that analyse original communications data (such as text messages) are not proportionate and thus require additional safeguards; and (3) introduce several additional safeguards such as protecting personal data that is transferred to third countries; receiving prior authorisation from DPAs; adding a more elaborate internal review mechanism; clearly excluding communications technologies that use end-to-end encryption from the scope of the proposed regulation; and improving transparency and accountability.

Contents

Table of Figures

Abbreviations and acronyms

Charter	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
CSA	Child Sexual Abuse
CSAM	Child Sexual Abuse Material
DPAs	Data Protection Authorities
DPIA	Data Protection Impact Assessment
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EECC	European Electronic Communications Code
EP	European Parliament
EPRS	European Parliamentary Research Service
EU	European Union
FRA	Fundamental Rights Agency of the European Union
GDPR	General Data Protection Regulation
LEAs	Law enforcement authorities
NCMEC	National Center for Missing and Exploited Children
NI-ICS	Number-Independent Interpersonal Communications Service
TFEU	Treaty on the Functioning of the European Union
US	United States of America

1. Background, Objectives, methodology

1.1. Background and Objectives

As reported in Interpol's report on *Threats and Trends Child Sexual Exploitation and Abuse COVID-19 Impact,* "with increased time being spent online by the general population, and often in more private settings than in the work environment, the illegal consumption of child sexual exploitation material has increased."[4] While Europol's *Internet Organised Crimes Threat Assessment* for 2020, reports an increase in the quantity of child sexual abuse material (CSAM) detected online,[5] the resources of law enforcement authorities (LEAs) have been severely impacted by the crisis.[6] The amount of CSAM that has been created or that is in circulation online cannot be quantified in absolute terms[7] because new content is constantly being added and only a proportion of older content has been identified and taken down.[8] There is evidence[9] that illegal consumption of CSAM takes place in different online settings (e.g. peer-to-peer networks, Darknet forums, social media platforms, messaging application/platforms, online gaming etc.).

As reported by the Council of Europe,[10] both in Europe and within other countries around the world, multi-stakeholder cooperation has been identified as the basis for the response against CSAM. Stakeholders include, among others, LEAs, national authorities, safer internet hotlines/reporting mechanisms and service providers/industry. There have been several calls for industry to take down CSAM materials from their services and several have developed dedicated reporting mechanisms to enable materials to be taken down once notified.[11] Over the last decade industry has also adopted more automated systems to detect CSAM, which once reviewed by a human reviewer, enable them to take down the content and take action against the user (e.g., through the termination or interruption of services). Often the basis for these activities are the terms and conditions of the service, wherein it is provided that illegal content (or behaviour) can lead to the termination or

---

4 Interpol (2020), Threats and Trends Child Sexual Exploitation and Abuse COVID-19 Impact, September 2020 https://www.interpol.int/en/content/download/15611/file/COVID19%20-%20Child%20Sexual%20Exploitation%20and%20Abuse%20threats%20and%20trends.pdf.

5 Europol (2020), Internet Organised Crimes Threat Assessment 2020, October 2020 https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf.

6 Interpol (2020), Threats and Trends Child Sexual Exploitation and Abuse COVID-19 Impact, September 2020 https://www.interpol.int/en/content/download/15611/file/COVID19%20-%20Child%20Sexual%20Exploitation%20and%20Abuse%20threats%20and%20trends.pdf .

7 Bursztein, Elie et al in their paper 'Rethinking the Detection of Child Sexual Abuse Imagery on the Internet' report on a first longitudinal measurement study of child sexual abuse imagery distribution online. Their results show that child sexual abuse imagery has grown exponentially-to nearly 1 million detected events per month-exceeding the capabilities of independent clearinghouses and law enforcement to take action.

8 ECPAT International (2018), "Trends in online child sexual abuse material", April 2018, Bangkok: ECPAT International https://www.ecpat.org/wp-content/uploads/2018/07/ECPAT-International-Report-Trends-in-Online-Child-Sexual-Abuse-Material-2018.pdf.

9 Interpol (2020), Threats and Trends Child Sexual Exploitation and Abuse COVID-19 Impact, September 2020.

10 Council of Europe (2019), Member state responses to prevent and combat online child sexual exploitation and abuse. Baseline mapping. Report prepared by Victoria Baines Available at: https://rm.coe.int/191120-baseline-mapping-web-version-3-/168098e109 (Accessed: 15 December 2020).

11 UNICEF and GISMA (2016) Notice and Takedown: Company policies and practices to remove online child sexual abuse material. Available at: https://www.gsma.com/publicpolicy/wp-content/uploads/2016/05/UNICEF_GSMA2016_Guidelines_NoticeAndTakeDown_PoliciesAndPracticesToRemoveOnlineChildSexualAbuseMaterial.pdf (Accessed: 15 December 2020).

interruption of services.[12] Indeed, there is also an increasing societal expectation that online providers take responsibility for illegal (or harmful) content on their platforms.[13]

As the study on *Online Platforms' Moderation of Illegal Content Online: Law, Practices and Options for Reform* requested by the European Parliament Committee on the Internal Market and Consumer Protection (IMCO) notes: "The EU regulatory framework on content moderation is increasingly complex and has been differentiated over the years according to the category of the online platform and the type of content reflecting a risk-based approach".[14]

The e-Commerce Directive of 2000[15] sets the baseline regime applicable to all categories of platforms and all types of content. The e-Commerce Directive provides for an exemption from liability for hosting platforms which remain passive and neutral and which remove the illegal online content as soon as they are made aware of it. Additionally, it provides for a prohibition of general monitoring measures in order to protect fundamental rights. In the revised Audio-Visual Media Services Directive,[16] video-sharing platforms have been given more obligations: they are expected to take appropriate and proportionate measures, preferably through co-regulation, in order to protect the general public from illegal content (terrorist content, CSAM, racism and xenophobia or other hate speech), and to protect minors from harmful content.

So far, other platforms have not been expected to actively protect the public from CSAM. However, several Number-Independent Interpersonal Communications Service (NI-ICS) providers have voluntarily set up specific technologies to detect and remove CSAM online within their services. They then report CSAM material that has come to their attention to the United States (US) National Center for Missing and Exploited Children (NCMEC)[17], who after reviewing the CSAM forwards the reports to LEAs and relevant third-party organisations established within the European Union (EU) and other third countries. There is no equivalent to the NCMEC in the EU. In September 2019, the New York Times noted that in the previous year technology companies reported to NCMEC over 45

---

12 Lee, HE. Ermakova, T., Ververis, V., and Fabian, B. Detecting child sexual abuse material: A comprehensive survey. Forensic Science International: Digital Investigation 34 (2020) https://doi.org/10.1016/j.fsidi.2020.301022.

13 Flash Eurobarometer 469 – Report Illegal content online. Fieldwork June 2018 Publication September 2018 https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/83669; Ofcom, Internet users' experience of harm online: summary of survey research. Conducted by Kantar Media. Fieldwork June-July 2018 www.ofcom.org.uk › Internet-harm-research-2018-report ; Ofcom, Internet users' experience of potential online harms: summary of survey research. Fieldwork: January/February 2020 https://www.ofcom.org.uk/__data/assets/pdf_file/0024/196413/concerns-and-experiences-online-harms-2020-chart-pack.pdf.

14 European Parliament (2020), Online Platforms' Moderation of Illegal Content Online: Law, Practices and Options for Reform study requested by the IMCO committee. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652718/IPOL_STU(2020)652718_EN.pdf.

15 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') OJ L 178, 17.7.2000, p. 1–16 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN.

16 Consolidated text: Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (codified version) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02010L0013-20181218&from=EN.

17 This duty to report is established by US law, in particular 18 U.S. Code § 2258A - Reporting requirements of providers https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section2258A&num=0&edition=prelim.

million photographs and videos of children being sexually abused.[18] This was more than twice the number reported in the previous year.

Within the EU the legal framework regulating NI-ICS is changing. The new European Electronic Communications Code (EECC) Directive[19] regulating electronic communication services and networks enacted in December 2018 has extended the definition of electronic communication services under EU law. In particular, the definition of an electronic communications service now includes internet-based services that do not connect with publicly assigned numbering resources (i.e., number or numbers in national or international numbering plans). The EECC calls these services "number-independent interpersonal communications services"[20]. The definition of NI-ICS also includes services using numbers as a mere identifier, such as instant messaging.[21] This change in definition of an electronic communications service will also be applied in the national transpositions of e-Privacy Directive[22] once the Member States transpose the EECC Directive. Where Member States failed to meet the transposition deadline of 21 December 2020, the national rules must, following the expiration of the deadline, be interpreted in the light of the wording and the purpose[23] of the EECC Directive in so far as this is possible and does not, for instance, conflict with the explicit wording of domestic laws.[24]

Article 5(1) of the e-Privacy Directive provides that electronic communications services have to ensure the confidentiality of communications and the related traffic data and, in particular, that Member States shall prohibit (electronic communications services from) '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)'.[25] Given the change in definition of electronic communications services, from 21 December 2020, NI-ICS will too be subject to this obligation of confidentiality and non-listening, tapping, storage or other kinds of interception or surveillance of communication and the related traffic data. In effect, NI-ICS would be precluded from continuing to voluntarily use specific technologies to detect and remove CSAM (mentioned earlier).

Article 15(1) of the e-Privacy Directive provides that "Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, … of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public

---

18 Keller, M.H., Dance, G.J.X.: The Internet is overrun with images of child sexual abuse. What went wrong? (2019). Available at https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html.

19 Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) OJ L 321, 11 December 2018, p36-214.

20 In article 2(7) of the EECC Directive.

21 See article 2(7) of EECC Directive.

22 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, p. 37–47.

23 As established in Case 14/83 *Von Colson and Kamann* [1984] ECR 1891. Catherine Barnard and Steve Peers (2014) European Union Law. Oxford University Press p153.

24 In Case C212/04 *Adeneler* [2006] ECR 1-6057, the court has formulated three possible limits to the duty of consistent interpretation: (a) interpretative methods recognised by national law; (b) general principles; and (c) no interpretation *contra legem*. Catherine Barnard and Steve Peers (2014) European Union Law. Oxford University Press p157. See also See Legislative Train Schedule: Promoting our European Way of Life. Proposal for a Regulation on a temporary derogation from certain provisions of the e-Privacy Directive for the purpose of combating child sexual abuse online https://www.europarl.europa.eu/legislative-train/theme-promoting-our-european-way-of-life/file-temporary-derogation-from-the-e-privacy-directive-for-ott-services.

25 Article 5(1) e-Privacy Directive.

security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union".

In line with this provision and given that Child Sexual Abuse (CSA) is a serious crime with life-long consequences for victims, on 10 September 2020, the European Commission (the Commission) introduced a proposal for a Regulation on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by NI-ICS for the processing of personal and other data for the purpose of combatting CSA online.[26] This proposed regulation is in line with the EU strategy for a more effective fight against CSA (adopted on 24 July 2020)[27], which aims to provide an effective response, at EU level, to the crime of CSA. This proposed regulation is a temporary measure aimed at enabling NI-ICS to continue the use of voluntary practices after the entry into force of the EECC Directive. In Recital 16 of the proposed regulation, the Commission foreshadows the introduction of a long-term legal framework in the second quarter of 2021 that will replace the temporary derogation.

The Commission considers that this proposed regulation is "a narrow and targeted legislative interim solution with the sole objective of creating a temporary and strictly limited derogation from the applicability of Articles 5(1) and 6 of the e-Privacy Directive, which protect the confidentiality of communications and traffic data".[28] The proposed regulation targets not only current voluntary activities used to detect and report CSAM but also voluntary efforts to detect solicitation of children for sexual purposes ("grooming"). According to the Commission, both sets of activities (that is, to detect CSAM and to detect grooming) "must be limited to the use of existing, state-of-the-art technology that corresponds to the safeguards set out"[29] in the proposed regulation. The temporary Regulation is for a limited period of five years or until long-term legislation is adopted and enters into force.

In the opinion of the Commission, "This proposal respects the fundamental rights, including the rights to privacy and protection of personal data, while enabling providers of number-independent interpersonal communications services to continue using specific technologies and continue their current activities to the extent necessary to detect and report child sexual abuse online and remove child sexual abuse material on their services" and to detect solicitation of children for sexual purposes. The Commission also submits that "In addition, the proposal takes into account Article 24(2) of the Charter [of Fundamental Rights] which provides that, in all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration. Moreover, to the extent that processing of electronic communications by number-independent interpersonal communications services for the sole purpose of detecting and reporting child sexual abuse online and removing child sexual abuse material falls into the scope of

[26] COM(2020) 568 final.

[27] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, EU strategy for a more effective fight against child sexual abuse, 24.7.2020 COM(2020) 607 final.

[28] COM(2020) 568 final on page 2.

[29] COM(2020) 568 final on page 2.

the derogation created by this proposal, the General Data Protection Regulation, which implements in secondary legislation Article 8(1) of the Charter, continues to apply to such processing".[30]

The proposed regulation was not accompanied by a Commission impact assessment. In view of the policy objective and time-sensitive nature of the issue, the Commission considered that there were "no other materially different policy options available" and thus no impact assessment was appropriate.[31] Given the lack of an impact assessment, more detailed considerations on the possible impact of the proposed regulation on fundamental rights has not been undertaken. In the introduction to 'Tool #28. Fundamental Rights and Human Rights' of the European Commission Better Regulation Toolbox', it is noted that "The need to ensure compliance and promotion of fundamental rights is not limited to legislative proposals but should be considered in all Commission acts and initiatives. To help in the implementation of this obligation, the Commission has developed an assessment methodology based on a Fundamental Rights Check-list which should be used by all Commission departments".[32]

The lack of a more systematic analysis of the fundamental rights implications of the proposed regulation was raised as a concern by the Rapporteur (Birgit Sippel, S&D, Germany) of the European Parliament Committee on Civil Liberties, Justice and Home Affairs (the LIBE Committee) along with the broad majority of shadow rapporteurs. The European Parliamentary Research Service (EPRS) was asked on 28 October 2020 to carry out a targeted substitute impact assessment restricting the analysis to four questions:

1. What are the impacts of the proposed regulation on EU privacy and data protection rights (e-Privacy Directive and GDPR) as well as EU fundamental rights and ECHR human rights of persons affected?
2. Does the proposed regulation comply with the principle of proportionality and the principle of subsidiarity, which includes an 'EU added value' test?
3. Are the safeguards provided for in the proposed regulation sufficient to ensure compliance with Article 52(1) of the EU Charter, taking account of current case law of the CJEU and GDPR rules?
4. What is the impact of the proposed regulation on the right to an effective remedy in accordance with Article 47 of the EU Charter of Fundamental Rights, if the users are not aware that the content of their private communications is scanned and potentially flagged up for human review?

This document proceeds to answers these questions in the following manner: Section 2 investigates whether the proposed regulation respects the principles of subsidiarity and proportionality; Section 3 examines whether current technologies meet the requirements set out in the proposed regulation as it currently stands; Section 4 looks at the impact of the proposed regulation on the rights of children and users; Section 5 analyses the possibility of effective remedies available to those users; and finally, Section 6 proposes increased safeguards in line with current EU policies.

[30] COM(2020) 568 final on page 5.

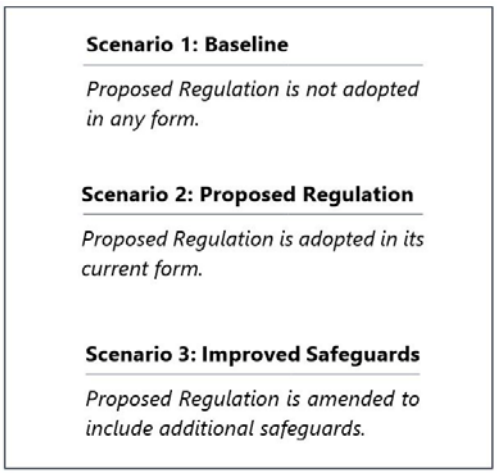
[31] COM(2020) 568 final on page 4.

[32] TOOL #28. Fundamental Rights & Human Rights https://ec.europa.eu/info/sites/info/files/file_import/better-regulation-toolbox-28_en_0.pdf on page 1.

1.2. Possible Scenarios

Since this is a targeted impact assessment, three distinct policy scenarios are available based on the proposed regulation. These are represented in Figure 1 below. All policy scenarios take the EECC's deadline for transposition into account, which has been set at 21 December 2020.

Figure 1. Summary of scenarios in this study



The three scenarios envisaged by this document are as follows:

1. Scenario 1: This scenario looks at a situation where the proposed regulation is not adopted by the EU.
2. Scenario 2: This scenario considers the situation that would exist should the proposed regulation be adopted in its current form.
3. Scenario 3: In this scenario, amendments to the proposed regulation are suggested. These amendments involve the inclusion of additional safeguards for the rights of the users of NI-ICS providers' services.

This targeted impact assessment analyses the four questions set out in Section 1.1 from the perspective of these three scenarios.

The impact assessment considers the following legal context in its analysis:

- The European Convention on Human Rights (ECHR, Article 8);
- The EU Charter of Fundamental Rights (the Charter, Articles 7, 8, 24 and 52);
- The Treaty on the European Union (TEU, Article 3(3), 5);
- The Treaty on the Functioning of the European Union (TFEU, Article 16, 114 and the Protocol on Subsidiarity);
- Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography;
- The e-Privacy Directive;
- The General Data Protection Regulation (GDPR, Articles 4, 6, 94, 95); and
- The European Electronic Communications Code (EECC) Directive;

The corpus of judgements of the Court of Justice of the European Union and the European Court of Human Rights linked to this legal context is also taken as part of the legal analysis baseline.

1.3. Methodology

In order to answer the research questions, the team performed desk research and carried out interviews in order to collect information and test hypotheses. The literature included guidance documents from the Fundamental Rights Agency (FRA), the European Data Protection Supervisor (EDPS) and Article 29 Working Party/European Data Protection Board opinions and guidance. As part of the views and opinions collected during the desk research, views and opinions offered on the proposed actions that were under discussion during the preparation of this research have also been taken into account. This includes[33] the European Parliament (EP) Intergroup expert meeting on EU legislation on the fight against child sexual abuse online held on 15 October 2020;[34] Opinion 7/2020 by the European Data Protection Supervisor published on 10 November 2020;[35] the draft report presented by the Rapporteur and the following debate on 16 November 2020[36] and the draft report (of 11 December 2020) adopted following the debate on 7 December 2020;[37] and the Opinion of the Committee on Women's Rights and Gender Equality (Rapporteur: Christine Anderson, ID Group, Germany) of 2 December 2020[38].

Given the strict and limited time frame within which this study had to be carried out, the team was given access to two Commission documents prepared in response to the Rapporteur's questions of 9 October 2020 and on 6 November 2020. These documents were also referred to during an interview carried out with the Commission services. Another interview with an NI-ICS provider and written responses to the team's requests for information from Europol complemented the desk research. The aim of the interviews/requests for information was to supplement, correct and validate our information baseline obtained through the literature review. Furthermore, the interviews were used to identify the use of specific technologies and to deepen the team's understanding of the voluntary practices in use.

Doctrinal analysis was leveraged in the analysis and to draw conclusions.

---

33 This is not meant to be an exhaustive list. The research team have taken into account all available documents referring to the ongoing legislative process.

34 EP Intergroup expert meeting on EU legislation on the fight against child sexual abuse online, held on 15 October 2020 https://www.youtube.com/watch?feature=youtu.be&v=adY_uWfs90E&app=desktop.

35 European Data Protection Supervisor, Opinion7/2020 on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online, 10 November 2020 https://edps.europa.eu/data-protection/our-work/publications/opinions/opinion-proposal-temporary-derogations-directive_en.

36 Draft Report 13 November 2020 on the proposal for a regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards as the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online (COM(2020)0568 - C9-0288/2020 - 2020/0259(COD)) Committee on Civil Liberties, Justice and Home Affairs Rapporteur: Birgit Sippel https://www.europarl.europa.eu/doceo/document/LIBE-PR-660288_EN.pdf.

37 REPORT AD-0258/2020 on the proposal for a regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards as the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online (COM(2020)0568 – C9-0288/2020 – 2020/0259(COD)) Committee on Civil Liberties, Justice and Home Affairs Rapporteur: Birgit Sippel https://www.europarl.europa.eu/doceo/document/A-9-2020-0258_EN.html.

38 OPINION on the proposal for a regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online 02-12-2020 FEMM_AD(2020)659041 PE659.041v03-00 https://www.europarl.europa.eu/doceo/document/FEMM-AD-659041_EN.pdf.

1.4. Limitations

The major limitation of this targeted impact assessment is the short timeframe within which it was carried out considering the urgency with which the LIBE Committee needed to consider the proposed regulation. In addition, the study was carried out while the European Parliament, the Council, the European Data Protection Supervisor and other committees were also discussing and/or publishing opinions on the proposed regulation. Ideally, an impact assessment is carried out before these processes take place. Instead, the process of carrying out the impact assessment was impacted by the other processes. The restrictive timeframe meant that only limited empirical research could be carried out, e.g., interviews were reduced to solely what was strictly necessary to complement the desk research.

This impact assessment is not a fully-fledged impact assessment of the proposed regulation, but a targeted impact assessment limited to the four questions set by the LIBE Committee in the Terms of Reference. No (alternative) policy options were expected to be examined.

2. Proportionality and Subsidiarity

This section addresses the question "Does the proposed regulation comply with the principle of proportionality and the principle of subsidiarity, which includes an 'EU added value' test?"

In the Explanatory Memorandum to the proposed regulation, the Commission has explained their position as regards the subsidiarity and proportionality of the interim regulation. Their arguments unfold as follows: (i) this derogation follows the principle of subsidiarity since leaving it to the Member States may result in the fragmentation of standards, disincentivising service providers from continuing their voluntary practices; and (ii) this derogation is proportionate since it only affects Articles 5(1) and 6 of the e-Privacy Directive (with a focus on well-established practices, as strictly necessary) and this derogation is temporary (expires latest on31 December 2025).

Compliance with the principles of subsidiarity and proportionality is only relevant under Scenario 2; the specific measures proposed for Scenario 3 do not have an impact on the EU's competence to adopt the proposed regulation and are instead geared towards clarifying the legal basis and safeguards for the voluntary practices conducted by NI-ICS providers in combating child abuse online.

Each of these steps will be analysed separately in the subsequent sections.

2.1. Legal Basis

The legal basis provided by the Commission for the proposed regulation combines Articles 16 and 114 of the TFEU[39]. Article 16 provides a legal basis for actions related to the protection of individuals with regard to the processing of personal data. Article 16 is the legal basis for the GDPR. Article 114 TFEU is the legal basis for the e-Privacy Directive, which the proposed regulation seeks to derogate from, as well as the EECC.

Article 114 TFEU provides the EU with the competence to harmonise policies across the internal market (with exceptions). The e-Privacy Directive regulates the activities of providers of electronic communications which, as a subset of the internal market, is part of the portfolio of shared competences within the EU (Article 4 TFEU). There are limits placed upon the Union's competence through previous judgments of the CJEU, as Weatherhill[40] discusses: a legislative action can be brought under Article 114 if the "object of a measure must genuinely be to improve the conditions for the establishment and functioning of the internal market" where differences in national legislation have "a direct effect on the functioning of the internal market"[41].

As this study will show, the concern of fragmentation regarding the detection, reporting and removal of CSAM online due to differing standards set by EU Member States is valid. However, there are caveats to this concern, as explored further below. Finally, it has also been argued that children may be better protected at the supra-national level through harmonisation of policies.[42]

---

39 Consolidated version of the Treaty on the Functioning of the European Union *OJ C 326, 26.10.2012, p. 47–390*.

40 Weatherill, S. (2011). The Limits of Legislative Harmonization Ten Years after Tobacco Advertising: How the Court's Case Law has become a "Drafting Guide". German Law Journal, 12(3), 827-864.

41 Ibid. at p. 832.

42 Stalford, H. and Drywood, E. (2009) Coming of Age?: Children's Rights in the European Union, Common Law Market Review, 46, 143-172.

2.2. Definition of subsidiarity

The principle of subsidiarity has been set out under Article 5(3) of the TEU as follows:

"3. Under the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level.

The institutions of the Union shall apply the principle of subsidiarity as laid down in the Protocol on the application of the principles of subsidiarity and proportionality. National Parliaments ensure compliance with the principle of subsidiarity in accordance with the procedure set out in that Protocol."

Additionally, the Protocol on Subsidiarity to the TFEU[43] applies to draft legislative acts. Under the Protocol, the Commission is required to forward its draft legislative acts and its amended drafts to national Parliaments.[44] Such national Parliaments may, within eight weeks from the date of transmission of a draft legislative act, send a reasoned opinion to the Commission stating why it considers that the draft in question does not comply with the principle of subsidiarity.[45] If at least one third of the votes allocated to the national Parliaments state the same, then the Commission is obligated to review the draft and provide reasons for any actions they take due to such a review.[46] It should be noted that the Protocol gives the Commission the option to not conduct such consultations in cases of "exceptional urgency",[47] but the Commission informed the team that they did transmit the draft to national parliaments, and only Portugal chose to respond within the eight week consultation period.

2.3. The subsidiarity of the proposed regulation

The Commission considers the proposed regulation to be a "derogation from certain provisions of Directive 2002/58/EC" (e-Privacy Directive). The Commission has justified the legislation taking the form of a Regulation (instead of a Directive) as an effort to remove the fragmentation of standards and safeguards to be followed by service providers in their effort to combat CSAM across the EU. The e-Privacy Directive, through Article 15(1), gives Member States the ability to adopt legislative measures to restrict the scope of the rights and obligations provided under Articles 5 and 6, but the Commission has noted in its Explanatory Memorandum to the proposed regulation that not all Member States have exercised this competence. In any case, differences in standards set by Member States in exercising this competence can result in fragmentation after the EECC's transposition.

This argument of fragmentation as well as the EU added value test is discussed below.

2.3.1. Fragmentation:

Commission's position: The practices undertaken by NI-ICS to detect, report and remove CSAM are voluntary. Fragmentation of standards could occur if Member States are left to devise their own

[43] Consolidated version of the Treaty on the Functioning of the European Union Protocol (No 2) On the application of the principles of subsidiarity and proportionality *OJ C 202, 7.6.2016, p. 206–209.*

[44] Article 4 of the Protocol.

[45] Article 6 of the Protocol.

[46] Article 7 of the Protocol.

[47] Article 2 of the Protocol.

legislation on this matter, and also, if every Member State has not transposed the EECC by 21 December 2020, assuming that the indirect effect of Directives does not apply. The Commission stated in their interview to the team that in either of these cases, the costs of complying with fragmented standards may be prohibitive enough for NI-ICS to forego undertaking such practices entirely. Given the impact of voluntary practices on reducing the proliferation of CSAM online, this situation should not occur. Therefore, legislation must occur at the EU level.

Analysis: The deadline for the transposition of the EECC into national law by Member States has been set at 21 December 2020. Both the EECC and the e-Privacy Directive, having taken the form of Directives, have only vertical direct effect and not horizontal,[48] meaning that beyond this deadline, NI-ICS providers do not have a legal obligation to comply with them unless they have been transposed by a Member State. However, this situation is complicated by the principle of indirect effect of directives[49], whereby national courts have a duty to interpret existing national legislation in line with EU directives that have not been implemented past their deadline for transposition. In this case, expanding the scope of the e-Privacy Directive (and national legislation transposing that directive) in a given Member State depends on whether national courts and administrations interpret the national telecommunications laws of that Member State as being consistent with the EECC's provisions on the newly added NI-ICS providers. Given this complexity and lack of clarity, it is possible that the deadline may only partially impede the service providers' ability to voluntarily carry out their activities related to CSAM in some Member States, leading to the fragmentation of standards. Further, with most Member States being affected by COVID-19 slowdowns, resulting in delays in the transposition of the EECC, it is even more likely that compliance with the EECC, and thus also the expanded scope of the e-Privacy Directive, will become fragmented after that deadline.

Due to these reasons, fragmentation is likely to occur since all Member States did not transpose the EECC by 21 December 2020. While official figures on this transposition will not be available until the Commission's annual report on its monitoring of the application of EU law, unofficial trackers show that not all Member States are on schedule.[50] The Commission has noted that even if a single Member State transposes the EECC by the deadline, it would expose NI-ICS to fragmented standards, with litigation being possible in that Member State due to infringement of the e-Privacy Directive. To avoid such a scenario, the Commission argues, the proposed regulation is required. Since concerns of added litigation costs for NI-ICS is justified, the Commission considers that the avoidance of this risk may lead to the NI-ICS stopping their voluntary practices across the EU.

However, there are two reasons for this argument being flawed:

(i) The concern of voluntary practices being stopped due to the risk of litigation will not be mitigated by the proposed regulation since the legal basis of the current practices of the NI-ICS for combatting CSAM is not clear, which opens up the NI-ICS to litigation anyway. This lack of clarity will not be resolved simply by harmonising standards. The proposed regulation explicitly does not provide a legal basis through its adoption. Indeed, the Commission has opted to continue with the status quo by not taking a position on the legality of such voluntary practices. This issue is discussed in detail later in Section 4.3.

---

[48] Craig, P. and De Búrca, G., 2015. EU Law. 6th ed. Oxford: Oxford University Press pp. 204-205.

[49] Schütze, R. and Tridimas, T., 2017. Oxford Principles of European Union Law Volume 1: The European Union Legal Order. Oxford: Oxford University Press pp. 290-292.

[50] Bird&Bird, *European Electronic Communications Code* [Online], Bird&Bird. Available at: https://www.twobirds.com/en/in-focus/european-electronic-communications-code/eecc-tracker. (Accessed: 4 December 2020).

(ii) There are other factors that may compel NI-ICS to continue to undertake their voluntary practices regarding CSAM regardless of the proposed regulation, such as maintaining their public reputation as strong opponents of online child abuse being perpetrated through their services. Furthermore, since most NI-ICS are US-based companies (such as Facebook, Twitter and Microsoft), they are obligated under US law to any report CSAM detected on their services to the CyberTipLine hosted by NCMEC.[51] The extent to which it is technically feasible to stop their automated practices specifically in the EU while continuing them in the US is unclear.

Taking these flaws into account, the proposed regulation only partially resolves the risk of fragmentation, and of NI-ICS providers stopping their voluntary practices to combat CSAM, that occurs once the EECC's transposition deadline has passed.

2.3.2. 'EU added value' test

The 'EU added value test' is outlined in Tool #5 of the Commission Better Regulation Toolbox[52]. The Commission has previously used three criteria to judge the added value of the EU budget: effectiveness, efficiency and synergy.[53] Meanings beyond budgetary concerns have been assigned to this test,[54] and are thus relevant here. Efficiency is not a concern here since the proposed regulation does not have any implications for the EU budget, as noted by the Commission in the Explanatory Memorandum. Since the proposed regulation concerns the detection, reporting and removal of CSAM through actions taken voluntarily by NI-ICS providers, the Commission does not envisage any EU-level spending. Regarding effectiveness and synergy, the primary question that must be satisfied is whether the objectives of the proposed regulation could be better achieved at EU level by reason of the scale of effects of that action. Two issues have been addressed by the proposed action being taken at EU level and by taking the form of a Regulation (instead of a Directive): the harmonisation of the standards to be followed by NI-ICS providers across the Member States and reducing fragmentation, as highlighted in the section above. A heterogenous approach with each Member State deciding their own standards may reduce the effectiveness of the voluntary practices. Furthermore, it is important to set safeguards that protect users' fundamental human rights via a Regulation so that Member States do not inadvertently expand the scope of monitoring activities undertaken by NI-ICS providers beyond what is strictly necessary and proportionate.

2.4. Proportionality of EU action

2.4.1. Definition of the principle of proportionality

The principle of proportionality with regards to the competence of the EU to act has been set out under Article 5(4) of the TEU as follows:

"4. Under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties.

---

51 U.S. Code § 2258A. Reporting requirements of providers.

52 Available here: https://ec.europa.eu/info/files/better-regulation-toolbox-5_en. (Accessed: 6 December 2020).

53 European Commission (2011) *The added value of the EU budget,* Brussels: EC.

54 Rubio, E. (2011) *The "added value" in the EU budgetary debates: one concept, four meanings,* Notre Europe, Paris: Institut Jacques Delors.

The institutions of the Union shall apply the principle of proportionality as laid down in the Protocol on the application of the principles of subsidiarity and proportionality."

2.4.2. The proportionality of EU competence

The Commission's argument regarding compliance with the principle of proportionality rests primarily on the "narrow and targeted" scope of the proposed regulation, as well as its temporary nature. The Commission states that this has been achieved by ensuring that the Regulation applies only to "well-established technologies regularly used by providers of number-independent interpersonal communications services for that purpose"[55] – the specific purpose being combatting against CSAM. However, as noted by the LIBE Committee Rapporteur in her questions to the Commission, and as discussed in this study, it is questionable whether the scope of the proposed regulation is narrow and targeted. The second order implications of the proposed regulation could lead to the indiscriminate surveillance of users of NI-ICS' services, allow for users' personal information to be sent to a non-EU location in contravention of the GDPR, and also affect the robustness of end-to-end encryption. Additional safeguards for these implications, not present in the proposed regulation, are discussed later in this document in Section 6. It should be kept in mind that when measures to combat CSAM online are taken by service providers, legislation should ensure that their efficacy is maintained while simultaneously reducing the harm caused to legitimate users of such services to the maximum extent possible. The proposed regulation, even in its current form, does take steps towards this goal, although better safeguards and clearer language can be added.

The temporary nature of the proposed regulation raises two issues. Firstly, as noted by the Rapporteur, the proposed expiration date of 31 December 2025 is arbitrary in nature and may be too long. Secondly, it is possible that the standards set out under the proposed regulation may later be adopted as part of the "long-term" legislation currently being drafted by the Commission. Therefore, it is necessary to analyse the standards set out by the proposed regulation to ensure that, were they to continue indefinitely, they would not disproportionality interfere with fundamental human rights. This is done in the next section of this study. Ultimately, the concern about the arbitrary nature of the expiration date is mitigated by Recital 16 of the proposed regulation, which states: "In case the long-term legislation is adopted and will enter into force before that date, that legislation should repeal this Regulation." Thus, depending on the speed with which the long-term legislation is adopted, the proposed regulation may have a much shorter lifetime.

Conclusion:

The proposed regulation meets the requirements of the principle of subsidiarity and proportionality of EU-level action, as well as adding value by being adopted at the EU level. While there are concerns about the lack of additional safeguards and clarity in the language of the proposed regulation, acting on an EU level through a Regulation ensures that policies regarding the effective detection, reporting and removal of CSAM online by NI-ICS providers are not fragmented. It also allows the EU to set a higher standard for the protection of the rights of both children and service users than those which may be set by individual Member States.

[55] *See* Article 3(a) of the Proposed Regulation.

3. Impact on the Admissibility of Technologies

The objective of the proposed regulation has been set out under Recital (11) of the proposed regulation which states that "the sole objective of this Regulation is to enable the continuation of certain existing activities aimed at combating child sexual abuse online". To this end, the Commission has attempted to create a technology-agnostic provision while hoping to achieve what it believes to be the best compromise between CSAM detection technology and user privacy.

This section analyses the current technologies used by NI-ICS providers to detect, report and remove CSAM online, and examines if they actually meet the Commission's stated objective through the language of the proposed regulation.

Scenario 2 looks at the proposed regulation in its current form, where the analysis of proportionality requires benchmarking the state of the art of technologies used by service providers in combatting CSAM against multiple clauses in Article 3 of the proposed regulation. In particular, Article 3 sets out three criteria of standards and safeguards (under paragraphs (a), (b) and (c)) to be met by NI-ICS providers while deploying technologies to combat CSAM online. These are:

Criterion (a): Article 3(a) requires processing to be limited to "well-established technologies regularly in use" that are "in accordance with the state of the art used in the industry" and are the "least privacy intrusive";

Criterion (b): Article 3(b) requires these technologies to be "sufficiently reliable in that it limits to the maximum extent possible the rate of errors regarding the detection of content" with occasional errors being corrected "without delay"; and

Criterion (c): Article 3(c) requires these technologies to be "limited to the use of relevant key indicators, such as keywords and objectively identified risk factors".

This section will examine current technologies through the lens of these three criteria without regard to the impact of those technologies on user rights, which will be handled in the next section.

3.1. Typology of existing technologies

The proposed regulation is predicated on regulating the voluntary practices of N-ICS providers based on current technologies used by those providers that detect, report and remove different types of CSAM. Three types have been enumerated by the Commission in their response to the Rapporteur's questions: known CSAM; previously unknown CSAM; and grooming/solicitation of children for sexual purposes.[56] However, in practice, the technologies used by service providers can be broadly categorised into two sets:

(i) for detecting images and videos; and

(ii) for detecting text-based child grooming.

This categorisation has been used by the Rapporteur as well. The Commission seems to primarily rely on explanations provided by Microsoft for their CSAM-combating technologies (such as

[56] *See* Explanatory Memorandum to the Proposed Regulation, at p. 1.

PhotoDNA[57] for images and video and Project Artemis[58] for text), as a basis for regulating CSAM-combating technologies in general, since these have been mentioned multiple times in their responses both to the Rapporteur and to the team conducting this targeted impact assessment. These technologies, and others, will be analysed below.

3.2. Current technologies

3.2.1. Microsoft PhotoDNA

PhotoDNA was developed by Microsoft Research and Prof. Hany Farid. Initially geared towards images, it now incorporates detection of video content as well. In brief, it works by creating cryptographic hashes of previously identified CSAM. In other words, images (including key frames of videos) are converted into unique alphanumeric strings (or hashes). These hashes do not include any personal data and cannot be converted back into the original images. The hashes are then stored in a database. All images and videos uploaded to a service provider's server are also hashed and then compared against the database of hashes of known CSAM. Due to the unique nature of these hashes, if there is a match, it is almost a guarantee that the image or video contains CSAM.

Criterion (a): **PhotoDNA meets this requirement**. It is both "well-established" and "regularly in use". Most major service providers are currently using PhotoDNA, as evidenced by the "Project Protect" initiative of Microsoft, Facebook, Google, Apple, etc.[59] Given its widespread use and continuous efforts to keep it up to date, PhotoDNA may also be considered the "state of the art". Further, the technology has been in use for images since 2009[60], and for videos since 2018.[61] The technology also appears to be very privacy friendly, since only cryptographic hashes are stored in the database, and all new images and videos are also hashed before being compared.

Criterion (b): PhotoDNA meets this requirement. PhotoDNA relies on the one-way transformation of images and videos into hashes using mathematical algorithms. Therefore, its reliability depends on the underlying mathematics. The developer of the technology has testified that the expected error rate for hashes created using PhotoDNA is 1 in 50 billion.[62] Therefore, the real risk may therefore be found in the reliability of those responsible for tagging images and videos as containing CSAM and not in the application of PhotoDNA itself.

---

57 Microsoft, *PhotoDNA*. [online] Available at: https://www.microsoft.com/en-us/photodna (Accessed: 4 December 2020).

58 Gregoire, C. (2020), "Microsoft shares new technique to address online grooming of children for sexual purposes", *Microsoft*, 9 January [online]. Available at: https://blogs.microsoft.com/on-the-issues/2020/01/09/artemis-online-grooming-detection/ (Accessed: 4 December 2020).

59 Technology Coalition (2020), *A Plan to Combat Online Child Sexual Abuse*, 10 June [online] Available at: https://www.technologycoalition.org/2020/05/28/a-plan-to-combat-online-child-sexual-abuse/ (Accessed: 4 December 2020).

60 Ith, T. (2015) 'Microsoft's PhotoDNA: Protecting children and businesses in the cloud', *Microsoft*, 15 July [online]. Available at: https://news.microsoft.com/features/microsofts-photodna-protecting-children-and-businesses-in-the-cloud/ (Accessed: 4 December 2020).

61 Langston, J. (2018) 'How PhotoDNA for Video is being used to fight online child exploitation', *Microsoft*, 12 September [online]. Available at: https://news.microsoft.com/on-the-issues/2018/09/12/how-photodna-for-video-is-being-used-to-fight-online-child-exploitation/. (Accessed: 4 December 2020).

62 Farid, H. (2019) 'Fostering a Healthier Internet to Protect Consumers', *House Committee on Energy and Commerce*, 16 October [online]. Available at: https://www.congress.gov/116/meeting/house/110075/witnesses/HHRG-116-IF16-Wstate-FaridH-20191016.pdf (Accessed: 4 December 2020).

Criterion (c): PhotoDNA meets this requirement. Given the nature of this technology, it relies entirely on CSAM being already known. Therefore, it does not require the objective identification of risk factors once the cryptographic hash has been generated.

3.2.2. Microsoft Project Artemis

The technology is based on the analysis of historical chat-based conversations using probability ratings based on objectively identified keywords. When the probability of a conversation containing child grooming meets a specific threshold, it is tagged for human review.

Criterion (a): Project Artemis partially meets this requirement. While the technology is "regularly in use", having been made available to companies, law enforcement and non-government organisations, it is difficult to state that it is "well-established". The technology was unveiled in January 2020[63], and given the general nature of machine learning based technologies has a large scope for future improvement. It is also privacy intrusive to a degree, since conversations tagged by the technology require human review, where they may or may not be found to contain child grooming material.

Criterion (b): Project Artemis may not meet this requirement. Microsoft has reported to the Commission that the accuracy of the technology is 88%. It is unclear if this means that false positives and false negatives combined account for 12% of all conversations flagged by the system. The language of the proposed regulation makes it difficult to interpret if this number makes the technology "sufficiently reliable". Furthermore, given the rapid improvement possible for machine learning initiatives, it is likely that the "maximum extent" to which error rates can be reduced will keep changing over time and cannot be objectively assessed.

Criterion (c): Project Artemis partially meets this requirement. Project Artemis and other text analysis tools depend on the use of keywords, even though such keywords have not been made publicly available. However, the implementation of other "objectively identified risk factors" required by the proposed regulation is unclear, with the onus of determining such factors being left to service providers. A possible consequence of requiring service providers to process indicators such as age difference is that they may need to rely on the automated profiling of all users. This could be disproportionately intrusive on privacy.

3.2.3. Facebook messaging services

Criterion (a): Facebook's technologies partially meet this requirement. It is difficult to analyse the technologies used by Facebook for its various interpersonal communications services such as Messenger, WhatsApp and Instagram (direct messages) given their different characteristics. Facebook currently uses open-sourced perceptual hashing algorithms, or pHash (called "PDQ" for images and "TMK+PDQF" for videos[64]) across its platform to detect images and videos similar to previously identified CSAM.[65] The key difference is that when images or videos are similar to each other, the hashes generated for those images or videos are mathematically close to each other, thus

---

[63] Gregoire, C. (2020), "Microsoft shares new technique to address online grooming of children for sexual purposes", *Microsoft*, 9 January [online]. Available at: https://blogs.microsoft.com/on-the-issues/2020/01/09/artemis-online-grooming-detection/ (Accessed: 4 December 2020).

[64] These are not truly abbreviations, but technical descriptors of the algorithms that do not affect the analysis in this study. "PDQ" means that it is a Perceptual hasher using Discrete cosine transform with a Quality metric output. In "PDQF-TMK", the algorithm has an added Floating point and a Temporal Match Kernel.

[65] Davis, A. and Rosen, G. (2019), "Open-Sourcing Photo- and Video-Matching Technology to Make the Internet Safer", *Facebook*, 1 August [online]. Available at: https://about.fb.com/news/2019/08/open-source-photo-video-matching/ (Accessed: 4 December 2020).

allowing for the detection of not only known CSAM, but also unknown CSAM based on features found in known CSAM; in other words, they check for the similarity of new images and videos to known CSAM This includes Messenger and Instagram's Direct Messages, since they are not end-to-end encrypted. These technologies meet the criteria of being "well-established" and "regularly" in use, while also being the "state of the art" and the "least privacy intrusive", given that they are cryptographic hashing algorithms.

The nature of hashing algorithms (as previously explained for Microsoft PhotoDNA) is such that NI-ICS providers require access to images and videos so that they can be compared against a database of known CSAM. Since Messenger and Instagram are not end-to-end encrypted, Facebook will have access to the content of messages sent using those services. However, WhatsApp is an end-to-end encrypted messaging service, which means that only senders and recipients of messages have access to the unencrypted content of those messages. Since Facebook will not have access, any images or videos sent on WhatsApp cannot be compared against known CSAM and will therefore go undetected. Thus, WhatsApp fails this criterion. Facebook has also committed itself to enabling end-to-end encryption for all messaging services.[66] While this effort may not come to fruition quickly,[67] it is set to hinder the detection of CSAM[68] since Facebook will lose access to all images and videos sent across its messaging services once end-to-end encryption is enabled. In response, Facebook has initiated processes towards building machine learning-based tools for the detection of child abusers while providing safety tips to users.[69] However, given their nascent stage of development, these tools cannot be considered "well-established" even though they may now be "regularly in use". They are the state of the art, but it is also difficult to establish if they are the "least privacy intrusive".

Criterion (b): Facebook's technologies partially meet this requirement. Facebook's algorithms for the detection of images and videos containing CSAM (PDQ and TMK+PDQF) are hashing algorithms and can be analysed in the same way as Microsoft's PhotoDNA which is also a hashing algorithm. While specific procedures for generating hashes are different, the concept of comparing the hashes of all images and videos uploaded to their platform against the hashes of known CSAM remains the same. Their reliability depends on the robustness of the underlying cryptographic hashing mathematics. While third party data on the reliability of Facebook's algorithms in the context of its messaging services could not be found, the open-source nature of these algorithms means that they may improve through crowdsourcing over time. Note that, as before, these algorithms do not work on end-to-end encrypted messages, so they are completely unreliable for detecting CSAM in WhatsApp messages (and in the future, messages in Messenger and Instagram).

Information regarding the reliability of text-based grooming detection algorithms used by Facebook is not available.

---

66 Zuckerberg, M. (2019) *A Privacy-Focused Vision for Social Networking*, 6 March [Facebook]. Available at: https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/ (Accessed: 4 December 2020).

67 Greenberg, A. (2020) 'Facebook Says Encrypting Messenger by Default Will Take Years', *Wired*, 10 January [online]. Available at: https://www.wired.com/story/facebook-messenger-end-to-end-encryption-default/. (Accessed: 4 December 2020).

68 Dodd, V. 'Facebook's encryption plans could help child abusers escape justice, NCA warns, *The Guardian*, 23 November [online]. Available at: https://www.theguardian.com/uk-news/2020/nov/23/facebooks-encryption-plans-could-help-child-abusers-escape-justice-nca-warns. (Accessed: 4 December 2020).

69 Sullivan, J. (2020) *'Preventing Unwanted Contacts and Scams in Messenger'*, *Messenger*, 21 May [online]. Available at: https://messengernews.fb.com/2020/05/21/preventing-unwanted-contacts-and-scams-in-messenger/ (Accessed: 4 December, 2020).

Criterion (c): Facebook's technologies partially meet this requirement. Facebook's image and video based detection algorithms depend on a database of previously identified CSAM. Therefore, the use of such algorithms removes the need to adhere to key indicators and objectively identified risk factors other than matching cryptographic hashes. To this extent, these algorithms meet the proposed regulation's criteria.

However, as before, data regarding objectively identified risk factors for text-based grooming detection are largely unavailable; a previous study requested by the EP on the moderation of illegal content online focused only on ensuring human oversight and a 'good samaritan clause' for when mistakes in detection are made.[70] It is possible that Facebook, in the same vein as other service providers, has an internally developed database of such risk factors that is too sensitive to share in public.

3.2.4. Thorn's Safer

Thorn, a US-based international non-profit organisation, has recently developed a tool named "Safer" that uses perceptual hashing algorithms to identify previously unknown CSAM. As of August 2020, it is being circulated for use. Instead of using cryptographic hashing algorithms (as used in Microsoft's PhotoDNA), this tool relies on perceptual hashing algorithms similar to Facebook's algorithms, thus allowing for unknown CSAM to be detected based on features found in known CSAM.[71]

Criterion (a): Thorn's Safer does not currently meet this requirement. It should be stated at the outset that the tool does not meet this criterion primarily due to its novelty. While perceptual hashing algorithms are relatively well-established, the specific implementation by Safer cannot be considered to be "well-established" and "regularly in use" due to its recent release; however, it is likely that it will attain that status in the future. It may be adopted by NI-ICS in the future given its effectiveness.[72] Its privacy intrusiveness is very low, since it uses hashing algorithms that do not require the sharing of complete images and videos. This reveals a limitation in the language used in the proposed regulation, since it does not currently provide any means to include technologies that may become well-established before the proposed regulation expires.

Criterion (b): Thorn's Safer may meet this requirement. The accuracy of the tool has been identified as being 99%.[73] Other sources state that its expected false positive rate may be as low as one in one thousand.[74] Since Thorn has provided benchmarking tools for its technology,[75] it is

---

70 European Parliament (2020), *Online Platforms' Moderation of Illegal Content Online*. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652718/IPOL_STU(2020)652718_EN.pdf. At p. 80 (Accessed: 4 December 2020).

71 Thorn, *How Safer's detection technology stops the spread of CSAM*. [online] Available at: https://www.thorn.org/blog/how-safers-detection-technology-stops-the-spread-of-csam/ (Accessed: 4 December 2020).

72 Macaulay, T. (2020) 'New AI tool detects child sexual abuse material with '99% precision', *TheNextWeb*, 31 July [online] Available at: https://thenextweb.com/neural/2020/07/31/new-ai-tool-detects-child-sexual-abuse-material-with-99-accuracy/ (Accessed: 4 December 2020).

73 Ibid.

74 Faustomorales (2019), 'Show HN: Perceptual hashing tools for detecting child sexual abuse material', *YCombinator News*, 4 November [online blog] Available at: https://news.ycombinator.com/item?id=21445448. (Accessed: 4 December 2020).

75 Thorn, *Perception Benchmarking*. [online] Available at: https://perception.thorn.engineering/en/latest/examples/benchmarking.html (Accessed: 4 December 2020).

possible that the effectiveness of the tool will increase over time as service providers get accustomed to it.

Criterion (c): Thorn's Safer meets this requirement. Since the tool relies on hashing technology as well as using previously known CSAM in order to detect unknown CSAM, it meets this criterion. It does not require arbitrary risk factors to be effective.

Conclusion:

The technologies currently in use focus on detecting, reporting and removing CSAM online, whether it is known or unknown. **Of the investigated technologies, those that combat known CSAM in the form of images and video are likely to meet the criteria set out by the proposed regulation. However, those technologies that combat unknown CSAM in the form of images and video, and detect text-based grooming, may not meet such criteria.** For example, Microsoft's Project Artemis and Facebook's anti-grooming initiatives may fall outside the scope of the proposed regulation since they are not well-established at the time of the adoption of the regulation. Thus, these service providers may have to stop using and further developing these technologies, even though they may become more effective and less-privacy intrusive in the future. Thorn's Safer may be reliable, but it could be judged to be too new to meet the criteria of being well-established and regularly in use. The proposed regulation also does not provide any scope to include these technologies before its expiry on 31 December 2025. Therefore, **the objective of the Commission to enable the continuation of certain existing activities aimed at combating child sexual abuse online is only partly met**.

4. Impact on Fundamental Rights

Against this background of the technologies currently being used (discussed in Section 3), this section addresses the question 'What are the impacts of the proposed regulation on EU privacy and data protection rights (e-Privacy Directive and GDPR) as well as EU fundamental rights and ECHR human rights of persons affected?'. This section focuses on the text of the proposed regulation. The analysis follows the steps suggested in "Tool #28. Fundamental Rights and Human Rights" of the Better Regulation Toolbox.[76]

The proposed regulation could affect a number of fundamental rights, including the following:

1. Children's rights – in particular Article 24(1) and (2) of the Charter as regards the privacy and data protection rights of children (e.g., photos being reviewed by human moderators, shared with concerned third parties) and Article 3(1) of the Charter when read as safeguarding children's rights to respect for their physical and mental integrity;
2. Privacy and data protection rights of the user whose communications are monitored for CSAM – in particular Articles 7 and 8 of the Charter and Article 8 of the ECHR;
3. Freedom of expression – in particular Article 11 of the Charter and Article 10 of the ECHR.

None of these rights is absolute in nature, meaning that they might be subject to limitations. As a result, Article 52 of the Charter will need to be considered. According to Article 52, limitations on the exercise of rights and freedoms needs to be provided for by law and needs to respect the essence of such rights and freedoms. Furthermore, such limitations need to be proportionate, necessary and need to genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.

There is no easy co-existence between these rights and reducing or increasing the attention paid to the set of rights enjoyed by one group may have an irreversible effect on the enjoyment of the set of rights enjoyed by others. In other words, where more than one fundamental right could be affected, these fundamental rights often need to be balanced against one another, leading to limitations which benefit one group, but which may have an irreversible effect on another group.

In particular, the rights contained within Article 24 of the Charter require that the child's best interests must be a primary consideration in any action relating to children. The well-being and best interests of children are fundamental values shared by all Member States. According to a UNICEF study,[77] one in three global internet users is a child. However, children may not have the appropriate knowledge or understanding to recognise the implications of their online activities.

To ensure the protection of children's rights in the digital world, the United Nations (UN) Convention on the Rights of the Child includes a number of rights, including the right to privacy, data protection and freedom of expression.[78] The EU is guided by the principles set out in this Convention, which

[76] EU Better regulation: guidelines and toolbox. In particular Better regulation guidelines – Impact Assessment found at https://ec.europa.eu/info/sites/info/files/better-regulation-guidelines-impact-assessment.pdf and Better Regulation Toolbox 28 found at https://ec.europa.eu/info/sites/info/files/file_import/better-regulation-toolbox-28_en_0.pdf A reference is made in particular to the steps identified in Box 2 – Fundamental Rights Check List.

[77] Berman G. and K. Albrights, Children and the data cycle: rights and ethics in a big data world, Office of Research – Innocenti Working Paper WP-2017-05, June 2017.

[78] See also UNICEF's Industry Toolkit on Children's online Privacy and Freedom of Expression.

has been ratified by all of the Member States of the EU.[79] In this digital world, children also need to be protected against CSA.

According to the European Court of Human Rights (ECtHR), in the case of *K.U. v. Finland,*[80] sexual abuse is unquestionably a detestable type of wrongdoing with devastating effects on the victims for which children are entitled to State protection considering the threat to their physical and mental welfare and the vulnerability arising from their young age. The Court concluded in this case that "although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others". In this case, the child's safety interests outweighed the privacy interests of the perpetrator. There is however, no other caselaw establishing criteria that can be followed in assessing the value tensions and difficult balancing of rights that may be needed in the case of this proposed regulation.

The EU protects children in this regard by way of Directive 2011/92/EU on combating the sexual abuse and the sexual exploitation of children and child pornography.[81] The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse reiterates that all forms of sexual abuse of children are destructive to children's health and development. Online child sexual abuse is unquestionably a detestable type of wrongdoing with devastating effects on the victims for which children are entitled to State protection considering the threat to their physical and mental welfare and the vulnerability arising from their young age.

The proposed regulation will also have an impact on other rights and freedoms, especially the right to freedom of expression and confidentiality of communications guaranteed under EU law. These rights and freedoms could be affected by the proposed measures regardless of whether that measure involves the processing of personal data.

In fact, the e-Privacy Directive protects not only the right to privacy and the personal data protection of natural persons but also the legitimate interests of legal persons (see Recitals 12 and 26). Article 1(2) states that the provisions of the e-Privacy Directive "provide for the protection of the legitimate interests of subscribers who are legal persons." The expression "the processing of (…) other data" in Article 1 of the proposed regulation suggests that the derogations are not limited to the rights to privacy and data protection. In this regard, the proposed regulation would allow NI-ICS providers to scan the communications content and related traffic data of legal persons "to the extent necessary to detect and report child sexual abuse online and remove child sexual abuse material on their services" (Article 1). The right to communications confidentiality is also at the core of the e-Privacy Directive (Article 5), which should apply for legal persons as well.

Positive impacts

The primarily positive impact of this proposed regulation will be on the rights of the child. In creating a way to allow for NI-ICS to continue to identify and take down CSAM, it contributes to the protection of fundamental rights of the child including the right to respect for physical and mental integrity, the right to liberty and security, respect for private and family life, and the protection of dignity

[79] See https://ec.europa.eu/info/policies/justice-and-fundamental-rights/rights-child/eu-action-rights-child_en.

[80] ECtHR Case of *K.U. v. Finland*, application no. 2872/02.

[81] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA [2011] OJ L 335/1. See also the EU strategy for a more effective fight against child sexual abuse, 24.7.2020 COM(2020) 607 final.

and well-being.[82] Furthermore, the taking down of CSAM containing (sensitive) personal data of children allows children not to be confronted with CSAM involving them in the future. Another possible positive impact is on LEAs, in that, as end recipients of reports of CSAM found via these voluntary actions by the service providers, they will be in a better position to carry out their obligation of prevention, detection and prosecution of crimes, including CSA.

Negative impacts

There is a potential that these measures will have an impact on all users of NI-ICS, in that their communications will be monitored for CSAM. The 'monitoring' of communications may have a negative impact on the enjoyment of the right to communication (Article 7) and the right to data protection (Article 8) enshrined in the Charter and potentially a chilling effect on the freedom of expression.

In the proposed regulation the Commission states that non-adoption of the proposed regulation would have a negative impact on NI-ICS providers and their responsibility to the customers to keep their services free from CSAM.

4.1. EU Human and Fundamental Rights requirements

This section highlights the relevant EU legal framework on the right to respect for private life and the right to personal data protection as enshrined in the EU primary and secondary law and as interpreted in the caselaw of the CJEU and the ECtHR.

Article 8 of the ECHR protects the right to respect for private and family life, home and correspondence, commonly referred to as "the right to privacy". The scope of this provision is also broadly interpreted to incorporate the right to protection of personal data.[83] According to the case-law of the ECtHR, for instance, "the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention".[84]

Contrary to the ECHR system, the Charter recognises the right to protection of personal data as a distinct fundamental right. Reaffirming Article 16 of the TFEU, the Charter provides that "everyone has the right to the protection of personal data concerning him or her" (Article 8(1)). This provision also lays down the core values and principles of data protection (Article 8(2)).[85] Article 7 of the Charter establishes the right to privacy. Even though the Charter treats the fundamental rights of privacy and data protection separately, both rights are closely related and strive to protect similar values.[86]

The GDPR and e-Privacy Directive are the EU secondary laws relevant to this study. Before evaluating the proposed regulation, it is important to understand the interplay between the e-Privacy Directive

---

[82] European Commission, 'Inception Impact Assessment' (Ref. Ares(2020)7284226 - 02/12/2020). Available at <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726-Child-sexual-abuse-online-detection-removal-and-reporting-?utm_source=POLITICO.EU&utm_campaign=e38501e716-EMAIL_CAMPAIGN_2020_12_03_11_18&utm_medium=email&utm_term=0_10959edeb5-e38501e716-190646140>.

[83] Note that the debate about the difference and interplay between the right to privacy and data protection is beyond the purview of this study.

[84] See *ECtHR, Satakunnan Markkinapörssi Oy and Satamedia Oy V Finland, no 931/13 (2017)* Para.137.

[85] For detail analysis on this, see European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (Publications Office of the European Union 2018).

[86] ibid 19.

and the GDPR. The e-Privacy Directive, which focuses on the confidentiality and security of electronic communications, was designed to give effect to Article 7 of the Charter in the electronic communications sector. On the other hand, the GDPR concerns a separate right, i.e., the right to protection of personal data as guaranteed under Article 8 of the Charter.[87]

Unlike the GDPR, the material scope of the e-Privacy Directive is not limited to the processing of personal data, but broadly covers security and confidentiality of electronic communications (content and traffic data), which may also contain non-personal data and data related to legal entities. As explicitly provided under Article 1(2) and Recital 7, the e-Privacy Directive protects the confidentiality of communications and the legitimate interests of legal persons. The CJEU also held that "legal persons can claim the protection of Articles 7 and 8 of the Charter in relation to such identification only in so far as the official title of the legal person identifies one or more natural persons".[88] For instance, confidential business information, that does not necessary also contain personal data, is protected under the e-Privacy Directive.[89]

The GDPR applies only to the processing of personal data, regardless of the technology used. This means that the material scope of the GDPR and the e-Privacy Directive could overlap with respect to the processing of personal data in the electronic communications sector. In its 2019 Opinion, the European Data Protection Board (EDPB) has identified matters that may fall within the material scope of both the e-Privacy Directive and the GDPR at the same time, in so far as the processing relates to a natural person.[90] Some of the issues that may trigger the material scope of both the GDPR and the e-Privacy Directive include the use of cookies and the processing of traffic and location data.

This raises the question: which legislation applies when an issue falls within the material scope of both the GDPR and the e-Privacy Directive? The combined reading of Article 95 and Recital 173 of the GDPR, and Article 1(2) of the e-Privacy Directive provides the answer to this question. Article 1(2) of the e-Privacy Directive states that "the provisions of this Directive particularise and complement" the GDPR with respect to the processing of personal data in the electronic communications sector. Similarly, Article 95 (and Recital 173) of the GDPR provides that the Regulation does not apply to matters that are "subject to specific obligations with the same objective" set out in the e-Privacy Directive. These provisions reflect the principle of *lex specialis* ('special provisions prevail over general rules in situations which they specifically seek to regulate').[91]

This means that the GDPR applies to the extent that there are no specific provisions in the e-Privacy Directive. For instance, the e-Privacy Directive particularises the protection of confidentiality and protections with respect to the processing of communications content and traffic data relating to subscribers and users of electronic communications service. While traffic data falls within the material scope of both the GDPR and the e-Privacy Directive, the latter particularises the provisions of the GDPR by explicitly limiting the conditions in which traffic data can be processed.[92]

Another noteworthy relation between the GDPR and the e-Privacy Directive is that the two instruments complement one another. In this regard, the EDPS stated that "by requiring consent (as

---

87 Opinion 5/2016 Preliminary EDPS Opinion on the review of the e-Privacy Directive (2002/58/EC) 8.

88 *CJEU, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen [GC], Joined cases C-92/09 and C-93/09, 9 November 2010* Para.53.

89 Opinion 5/2016 Preliminary EDPS Opinion on the review of the e-Privacy Directive (2002/58/EC) 7.

90 EDPB Opinion 5/2019 on the interplay between the e-Privacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities (12 March 2019) 11.

91 EDPB Opinion 5/2019 13.

92 ibid p.13.

a legal basis) for the processing of traffic and location data, the e-Privacy Directive (Article 5 and 6) offers a higher level of protection than the GDPR". The GDPR, at least potentially, allows other legal grounds, such as legitimate interests or performance of a contract. A controller might try to argue, for example, that tracking users on the internet, and building detailed profiles on them would be part of their legitimate interest to market their services and products.[93]

4.2. Conditions for lawful interference with the right to privacy and data protection

None of the human and fundamental rights discussed above are absolute in nature, meaning that they are subject to lawful limitations. In other words, the exercise of the right to privacy and personal data protection must be balanced against other legitimate interests and rights. The cumulative conditions under which limitations can be imposed on the exercise of the right to privacy and personal data protection are set out under Article 8 (2) of the ECHR and Article 52(1) of the Charter. These conditions and their scope of application are also further developed by the caselaw of ECtHR and the CJEU.
According to Article 52(1), limitations on the exercise of the right to privacy and data protection can be lawful only if these limitations are:[94]

- provided for by law;
- respect the essence of the rights;
- genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others;
- necessary; and
- proportional.

Similarly, Article 8(2) of the ECHR provides that an interference with the right to respect for private and family life could be justified only if that interference is (i) in accordance with the law, (ii) pursuing a legitimate aim, and (iii) necessary in a democratic society.

In the area of privacy and data protection, Article 52(1) of the Charter is further specified by Article 15(1) of the e-Privacy Directive (applicable only to Member States) and Article 23(1) of the GDPR. These provisions set out a list of legitimate interests which could justify limitations on the exercise of the right to privacy and protection of personal data. These legitimate interests include, but are not limited to, national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences. To pursue these legitimate aims and subject to the requirements provided under Article 52(1) of the Charter, Member States are free to restrict through national legislation the scope of the rights and obligations in specific articles of the e-Privacy Directive and the GDPR.[95]

The e-Privacy Directive requires Member States to ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available

[93] Opinion 5/2016 Preliminary EDPS Opinion on the review of the e-Privacy Directive (2002/58/EC) p.17.

[94] For detailed analysis on each requirement, see EDPS, 'Guidelines on Assessing the Proportionality of Measures That Limit the Fundamental Rights to Privacy and to the Protection of Personal Data' (19 December 2019); EDPS, 'Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit' (11 April 2017); European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law (Publications Office of the European Union 2018) 35–50.

[95] See Article 15(1), e-Privacy Directive; Article 23(1), GDPR.

electronic communications services, through national legislation.[96] In particular, the Directive requires Member States to prohibit the "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)".[97]

The e-Privacy Directive also imposes negative obligations by requiring electronic communications service providers to erase or make anonymous, traffic data relating to subscribers and users processed and stored by these providers when it is no longer needed for the purpose of the transmission of a communication.[98]

4.3. Testing the proposed regulation

This section examines the proposed regulation against the requirements of Article 52(1) of the Charter. The proposed regulation aims to provide for the temporary derogation from specific obligations set out in Article 5(1) and Article 6 of e-Privacy Directive and thereby allow NI-ICS providers to continue the use of technologies for the processing of personal and other data to the extent necessary to detect and report CSA online and remove CSAM from their services.[99] In other words, the proposed regulation would impose certain limitations on the exercise of rights and freedoms guaranteed under EU law, specifically the right to privacy and confidentiality of electronic communications. One of the criteria under Article 52(1) of the Charter is that the legislation must respect the essence of the rights by ensuring that the right is not in effect emptied of its basic content, which would disallow the individual from exercising the right.[100] The threshold for emptying a right of its basic content is quite high; for example, in the case of *Digital Rights Ireland*, the CJEU found that the essence of the fundamental right to privacy and the protection of personal data was not adversely affected despite Directive 2006/24 (the Data Retention Directive)[101] constituting "a particularly serious interference with those rights".[102] The proposed regulation does not do so due to the specific standards and safeguards set out under Article 3. While the safeguards are not adequate, they do respect the essence of these rights and freedoms. The sub-sections below evaluate the proposed regulation against the remaining requirements of Article 52(1) of the Charter.

A. Interference with the right to privacy and data protection

Before triggering Article 52(1) of the Charter, it is necessary to first determine whether the measures envisaged by the proposed regulation constitute an interference with the right to privacy and protection of personal data. If the legislative measure would not interfere with or restrict the enjoyment of fundamental rights, there is no need to test the measure against the requirements of

96 See Article 5(1), e-Privacy Directive.

97 Ibid.

98 See Article 6(1), e-Privacy Directive. These obligations are without prejudice the requirements set out under Article 6 paragraphs 2, 3 and 5 and Article 15(1).

99 See Article 1, Proposed Regulation.

100 For detail on how the essence of fundamental rights and freedoms can be impaired, see Brkan, M. 'The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning' (2019) 20German Law Journal pp. 864–883.

101 Directive 2006/24/EC of the European Parliament and of the Council 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 and amending Directive 2002/58/EC OJ L 105, 13.4.2006, p. 54–63.

102 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* ECLI:EU:C:2014:238, paragraphs 39-40.

Article 52(1) of the Charter. In other words, the conditions stipulated under Article 52(1) of the Charter can be triggered only if there is an interference regardless of the legitimate aim pursued.

According to the settled caselaw of the CJEU and ECtHR, a measure that provides for processing of personal data in itself constitutes an interference with the right to privacy and the right to the protection of personal data guaranteed by Article 7 and Article 8 of the Charter.

In *Digital Rights Ireland and others*, for instance, the CJEU held that the retention of data relating to a person's private life and to his communications by providers of publicly available electronic communications services or of public communications networks constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter.[103] It constitutes an interference "because it provides for the processing of personal data".[104] Similarly, the ECtHR found that "the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8".[105] Therefore, any processing of personal data by itself constitutes an interference with the right to privacy and data protection regardless of whether or not that interference pursues a legitimate aim. As the EDPS has noted, "any data processing operation (such as collection, storage, use, disclosure of data) laid down by legislation is a limitation on the right to the protection of personal data, regardless of whether that limitation may be justified".[106]

The proposed regulation would provide for the voluntary processing of personal data (communications content and related traffic data) by NI-ICS providers for the purpose of detecting, removing and reporting CSAM online. As such, the proposed regulation constitutes an interference with the exercise of fundamental rights to confidentiality of communications and protection of personal data. Such interference exists regardless of whether the processing is carried out by public authorities or private entities, whether it is carried out on a voluntary basis or is required by law.

In this regard, the EDPS has noted that "even voluntary measures by private companies constitute an interference with these rights when the measures involve the monitoring and analysis of the content of communications and processing of personal data".[107]

As discussed above, any interferences with or derogations from the right to privacy and the protection of personal data can only be justified if they meet the requirements set out under Article 52(1) of the Charter. What follows is an evaluation of the proposed regulation against the requirements. In doing so, we consider the three scenarios identified.

B. Legal basis for interference

In the absence of EU legislative action (Scenario 1), the coming into effect of the EECC would preclude NI-ICS providers from continuing to use current technologies to detect, remove, and report CSAM online within their services. Once NI-ICS providers fall within the purview of the e-Privacy Directive, they will not have a clear legal basis at the EU level to process personal data for the purpose of detecting, removing, and reporting CSAM. Even though Article 15 of the e-Privacy Directive permits individual Member States to adopt national legislation that could require or allow

---

103 *CJEU, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [GC], Joined cases C-293/12 and C-594/12, 8 April 2014* paras. 34 – 36.

104 Ibid, para.36.

105 *ECtHR, S and Marper v the United Kingdom [GC], Nos 30562/04 and 30566/04, 8 December 2008* [67].

106 EDPS, 'Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit' (11 April 2017) 7.

107 EDPS, 'Opinion 7/2020 on the Proposal for Temporary Derogations from Directive 2002/58/EC for the Purpose of Combatting Child Sexual Abuse Online' (10 November 2020) 7.

NI-ICS providers to detect, remove, and report CSAM on their services, most Member States have failed to adopt such legislation.[108]

Therefore, in the absence of legislative measures adopted in accordance with Article 15(1) of the e-Privacy Directive at national level, and in the absence of EU legislative action, the continuation of the current practice by NI-ICS providers post EECC transposition would conflict with the e-Privacy Directive. There is additional legal uncertainty in this scenario. Even in the absence of EU legislative action, US-based NI-ICS providers that offer their services in the EU (and are hence subject to EU law) will continue the practice as they are required under US federal law to report CSAM once obtaining an actual knowledge of it.[109] In such a scenario, NI-ICS providers could be caught in the middle, with US law requiring them to detect, remove, and report CSAM and EU law precluding them from continuing their current voluntary practice.

Scenario 2 considers the situation where the proposed regulation is adopted in its current format. The primary objective of the proposed regulation is to preserve the *status quo,* that is, to allow providers of NI-ICS to continue to voluntarily detect, remove, and report CSAM. This begs the question of whether or not the current voluntary practices themselves comply with EU law.

The proposed regulation does not provide a clear answer to this question. Even though Recital 10 of the proposed regulation states that the GDPR will continue to apply to the voluntary practices, it does not provide specific legal grounds within the meaning of the GDPR. As the EDPS has noted, the proposed regulation 'does not clearly indicate whether or not it seeks to provide a legal basis within the meaning of Article 6 GDPR'.[110] The Commission's assessment of this issue is also vague and at times contradicting. The Commission does not wish to take a stance on whether or not current voluntary practices to detect and report CSAM are in fact legal under EU law. When asked by the LIBE Committee Rapporteur whether the current voluntary practices of detecting, removing and reporting CSAM comply with EU law, the Commission responded that it "does not take a position on the legality of these voluntary practices by operators" arguing that such responsibility "falls into the competence of the national DPAs".[111] The Commission argued that the objective of the proposed derogation is to ensure that the current activities remain allowed "to the extent that they currently comply with Union law"[112], suggesting that the current practice is in compliance with EU law. It is not clear how the Commission seeks to achieve this objective without ensuring that the current activities are in fact in compliance with EU law.

Not only is the current practice taking place on a shaky legal ground, the Commission also does not provide a legal basis for the processing of personal data under the proposed regulation. Recital 7 of the proposed regulation states that "there would be no legal basis for providers of NI-ICS to continue to detect and report child sexual abuse online and remove child sexual abuse material in their services beyond 21 December 2020". And yet, the proposed regulation does not clearly indicate

---

[108] European Parliament, Draft report on the proposal for a regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards as the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online, PE661.791v01-00, 26 November 2020.

[109] 18 U.S. Code § 2258A. Reporting requirements of providers.

[110] EDPS, 'Opinion 7/2020 on the Proposal for Temporary Derogations from Directive 2002/58/EC for the Purpose of Combatting Child Sexual Abuse Online' (10 November 2020) para.17.

[111] Questions for written answer to the Commission by the EP rapporteur Birgit Sippel, S&D, and her shadows (28 September 2020) p.5. *See also* Missing Children Europe, *Intergroup Expert Meeting on EU Legislation on the Fight against Child Sex Abuse Online* (2020). <https://www.youtube.com/watch?feature=youtu.be&v=adY_uWfs90E&app=desktop> accessed 13 December 2020

[112] See Explanatory Memorandum of the Proposed Regulation, p.6.

which legal basis would apply for voluntary processing of content or traffic data for the purpose of detecting CSA online.[113]

Two issues are clear from an analysis of the proposed regulation. First, the e-Privacy Directive does not contain an explicit legal basis for voluntary processing of content or traffic data for the purpose of detecting, removing and reporting CSA online.[114] Second, the proposed regulation itself does not provide a legal basis for the voluntary processing of content or traffic data for the purpose of detecting, removing and reporting CSA online. The proposal would only eliminate potential obstacles and allow NI-ICS providers to continue the current voluntary activities.

As discussed above, the first requirement to justify an interference with or limitation of the right to privacy and data protection under Article 52(1) of the Charter is that the interference must be provided for by law. This requirement implies that limitations must be based on a legal basis that is adequately accessible and foreseeable and formulated with sufficient precision.[115] The proposed regulation is not formulated with sufficient precision. Therefore, if the text of the proposed regulation is adopted in its current format, NI-ICS providers may not have a clear legal basis to process personal data for the purpose of detecting, removing, and reporting CSAM. In such legal uncertainty, NI-ICS providers in the EU may stop their voluntary practice and this in turn, would expose vulnerable children to additional risks.

Scenario 3, which recommends that the proposed regulation include a clear and explicit legal basis for processing, would help mitigate this legal uncertainty. As discussed above, the GDPR will continue to apply to the processing of personal data by NI-ICS providers which would fall within the purview of the proposed regulation.[116] This means, among other things, that the voluntary processing of content or traffic data for the purpose of detecting CSA online by NI-ICS providers must be lawful only on the basis of the specified grounds set out under Article 6(1)(a) to 6(1)(f) of the GDPR. This takes us to the next question: which legal basis within the meaning of Article 6 GDPR could be applicable for the proposed regulation?

Article 6(1) of the GDPR sets out six specific grounds under which personal data can be processed lawfully namely consent, contract, legal obligation, vital interests, public task, or legitimate interest. Of these six grounds, Article 6 (1)(a) which requires the consent of the data subject may not be appropriate within this context. First, data subjects can withdraw their consent at any time and without giving a reason for withdrawal per Article 7(3) of the GDPR. This would make it practically difficult for NI-ICS providers to rely on the consent of the data subject to detect, remove, and report SCAM. Consent for indiscriminate scanning and analysis of private messages, especially in the context of detecting text based CSAM, could also compromise the essence of the right to privacy. Furthermore, consent obtained through the blanket acceptance of terms and conditions may not constitute a freely given, informed, specific and an unambiguous consent within the meaning of the GDPR.[117] It is particularly important to note that silence, pre-ticked boxes or inactivity of the data subject do not constitute valid consent within the meaning of the GDPR and as interpreted in the

[113] EDPS, 'Opinion 7/2020 on the Proposal for Temporary Derogations from Directive 2002/58/EC for the Purpose of Combatting Child Sexual Abuse Online' (10 November 2020).

[114] See Explanatory Memorandum of the Proposed Regulation, p 2.

[115] European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law (Publications Office of the European Union 2018) P.43.

[116] Explanatory Memorandum of the Proposed Regulation, p.4.

[117] Recital 32, GDPR.

caselaw of the CJEU.[118] Relying on consent as a legal basis could be particularly problematic when minors are involved in sharing CSAM.

Under **Article 6(1)(b)** of the GDPR, processing of personal data is lawful if it "is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract". According to the Guidelines of EDPB, this provision can be used as a legal basis in either of the following two situations:

- the processing in question must be objectively necessary for the performance of a contract with a data subject, or
- the processing must be objectively necessary in order to take pre-contractual steps at the request of a data subject.[119]

Considering this purpose limitation, an NI-ICS provider may not validly justify the scanning of communications as being objectively necessary for the performance of a contract, or justify taking pre-contractual steps at the request of a data subject within in the meaning of Article 6(1)(b) of the GDPR. This is especially true when children are communicating. Therefore, Article 6(1)(b) is irrelevant within the context of the proposed regulation.

Processing of personal data "necessary for compliance with a legal obligation to which the controller is subject" (Article 6(1)(c)) is also not applicable in this particular case due to the voluntary nature of the activity. Even though the Commission is preparing mandatory legislation that would require NI-ICS providers to detect, remove and report known child abuse content, the proposed derogation is a voluntary one.

The remaining grounds stipulated under Article 6(1), which are 'vital interest' (d), 'public task' (e), and 'legitimate interest' (f) deserve a detailed analysis.

Article 6(1)(d) GDPR (vital interest): under this provision, the processing of personal data is regarded to be lawful where it is "necessary in order to protect the vital interests of the data subject or of another natural person". Applying this provision as a legal basis for processing requires two questions to be answered: (i) whose vital interests are relevant, and (ii) what constitutes a vital interest.[120] The vital interest referred to in this provision concerns either that of the data subject or any other living individual. This means NI-ICS providers can apply the legal basis of vital interest under the GDPR to the processing of a child's personal data to protect his/her vital interest as a victim of online sexual abuse. Article 6(1)(d) also envisages the processing of personal data in order to protect the vital interests of a person other than the data subject. This would justify the processing of the personal data of a user (data subject) where it is strictly necessary to detect, remove, and report CSAM (that is, to protect the vital interests of a child).

The second element of Article 6(1)(d) concerns the type of interest worthy of protection. Recital 46 indicates that the situation in which the legal basis of 'vital interest' can apply is where the interest is "*essential for the life of the data subject or that of another natural person*" According to a Guidance issued by the Irish DPA, this provision covers mainly "life-threatening situations, but potentially situations which very seriously threaten the health or fundamental rights of an individual".[121] As shall

---

[118] Recital 32, GDPR; Orange România SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) EU:C:2020:901.

[119] EDPB, 'Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects' (9 April 2019) Para 22.

[120] See Data Protection Commission, 'Guidance on Legal Bases for Processing Personal Data' (December 2019).

[121] ibid p.17. see also Article 29 Data Protection Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (WP 217, 9 April 2014) p.20.

be discussed below, online child sexual abuse is a particularly serious crime that threatens the life, morals and health of children. For instance, among the reports of child sexual abuse that NCMEC receives every year include "situations that pose an imminent danger to children (e.g., details of arrangements to meet to physically abuse the child or suicide threats by the child following blackmail by the offender)"[122]. Therefore, the voluntary practice of detecting, removing, and reporting CSAM is necessary in order to protect the vital interest of the child and NI-ICS providers could legitimately rely on Article 6(1)(d) GDPR as their legal basis for the processing of personal data for that specific purpose.[123]

Article 6(1)(e) GDPR (public task): processing of personal data under this provision is lawful when it is "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller." It is unlikely that this provision constitutes a valid legal basis on which processing could rely under the proposed regulation. Article 6(1)(e) could not be validly used as a legal basis for the measures envisaged by the proposed regulation for two reasons. First, the categories of controllers that might rely on this legal basis are mostly public authorities.[124] Even though other categories of controllers (natural or legal persons) "performing a task carried out in the public interest" may also rely on this legal basis[125], it cannot validly extend to the kind of voluntary activities envisaged by the proposed regulation. Second, the processing of personal data under Article 6(1)(e) should be determined in Union or Member State law, as required under Article 6(3)). However, the proposed regulation does not introduce such a legal basis.

Article 6(1)(f) GDPR (legitimate interest): The processing of personal data is lawful under this provision if it "is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child". Three cumulative requirements can be identified from Article 6(1)(f). The first element is that there must be a legitimate interest pursued by the controller or a third party. The kinds of legitimate interests that could be covered under Article 6(1)(f) of the GDPR include commercial interests, individual interests, or broader societal benefits.[126] One of the situations in which these legitimate interests could exist is "where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller".[127] Recital 47 of the GDPR provides two concrete examples of what would constitute legitimate interest of the data controller under Article 6(1)(f). One specific example is the processing of personal data for the purpose of preventing fraud. The processing of personal data for the purpose of direct marketing could also constitute legitimate interests of the data

---

122 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, EU strategy for a more effective fight against child sexual abuse, 24.7.2020 COM(2020) 607 final, p.14.

123 The Guidance issued by the Irish DPA states that 'Controllers are most likely to rely on this legal basis where the processing of personal data is needed in order to protect someone's life, or mitigate against a serious threat to a person, for example a child or a missing person.' See Data Protection Commission, 'Guidance on Legal Bases for Processing Personal Data' (December 2019) p.16.

124 *Judgement of 27.03.2019 - BVerwG 6 C 2.18. Para. 45-46. Available at <https://www.bverwg.de/270319U6C2.18.0>;* Data Protection Commission, 'Guidance on Legal Bases for Processing Personal Data' (December 2019) p.18; Article 29 Data Protection Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (3 October 2017) p.21.

125 Data Protection Commission, 'Guidance on Legal Bases for Processing Personal Data' (December 2019) p.19.

126 Data Protection Commission, 'Guidance on Legal Bases for Processing Personal Data' (December 2019) p.22. See also EDBP, 'Guidelines 3/2019 on processing of personal data through video devices Version 2.0' (29 January 2020) para 18.

127 Recital 47, GDPR.

controller within the meaning of Article 6(1)(f). According to the 2014 Opinion of the Article 29 Working Party, the requirement of legitimate interests under Article 7(f) of Directive 95/46/EC (which was replaced by Article 6(1)(f) of the GDPR) could be extended to include "general public interest" such as combating illegal activities.[128] The Working Party elaborated on this argument by saying that "the legitimate interest of third parties may also be relevant (…) where a controller - sometimes encouraged by public authorities - is pursuing an interest that corresponds with a general public interest or a third party's interest".[129]

The second requirement is that the processing of personal data must be necessary to achieve the identified legitimate interest. The third requirement is that the legitimate interest must be balanced against the data subject's interests, rights, and freedoms. In other words, Article 6(1) (f) does not automatically apply just because a legitimate interest is pursued, and personal data processing is necessary to achieve that legitimate interest. Once the legitimate interests are identified, a balancing exercise must be conducted between those interests and the interests or fundamental rights and freedoms of the data subject.[130] In such a case-by-case balancing exercise, the controller must ensure that the legitimate interests pursued are not overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. The balancing exercise should also take into consideration the reasonable expectations of data subjects based on their relationship with the controller.[131]

From this analysis, one can conclude that Article 6(1)(f) of the GDPR could also serve as a valid legal basis for processing under the proposed regulation, provided that the cumulative conditions identified above are fully respected. Even though the EDPS has recently cast some doubts on the applicability of Article 6(1)(f) to the proposed regulation,[132] the Opinion of the Article 29 Working Party suggests otherwise. In this regard, the Article 29 Working Party stated that the legitimate interests of third parties under Article 6(1)(f) "include situations where a controller goes beyond its specific legal obligations set in laws and regulations to assist law enforcement or private stakeholders in their efforts to combat illegal activities, such as (…) child grooming".[133] Therefore, following the Article 29 Working Party's Opinion, NI-ICS providers could justify their voluntary activities as legitimate in order to pursue a general public interest or a third party's interest (in this case, the child).

C. Objectives of general interest

As described above, Article 52(1) of the Charter requires that any limitation on the exercise of the right to privacy and protection of personal data must genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of other persons. According to the caselaw of the CJEU, public authorities have positive obligations to adopt substantive and procedural provisions as well as practical measures enabling effective action to combat

[128] Article 29 Data Protection Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (WP 217, 9 April 2014) 28.

[129] ibid.

[130] European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law (Publications Office of the European Union 2018) p.155. see also Article 29 Data Protection Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (WP 217, 9 April 2014).

[131] Recital 46, GDPR.

[132] EDPS, 'Opinion 7/2020 on the Proposal for Temporary Derogations from Directive 2002/58/EC for the Purpose of Combatting Child Sexual Abuse Online' (10 November 2020 Para. 16-21.

[133] Article 29 Data Protection Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (WP 217, 9 April 2014) 28.

crimes against the person through effective investigation and prosecution.[134] The CJEU has emphasised that such a positive obligation is "*all the more important when a child's physical and moral well-being is at risk*" (emphasis added).[135]

When tested against this requirement, the proposed regulation pursues both an objective of general interest recognised by the EU (in this case the effective prevention, detection and prosecution of related crimes, and the protection of victims of crime) and the need to protect the rights and freedoms of others (in this case the right to such protection and care as is necessary for their well-being of the child).[136]

The fight against CSA is a priority for the EU. As the Commission has aptly indicated, CSA online is a particularly serious crime that has wide-ranging and serious life-long consequences for victims. Sexual abuse of children is not only a serious violation of the human and fundamental rights of the child but also causes significant and long-term social harm.[137] In its 26 November 2019 resolution, the EP has observed that "child sexual abuse and exploitation online is a serious violation of the fundamental rights of children, resulting in enormous trauma and long-lasting harmful consequences for the child victims that can continue well into adulthood."[138]

Surveys also revealed that survivors of CSA online face perpetual feelings of shame, humiliation, vulnerability and powerlessness.[139] Therefore, sexual abuse is unquestionably a detestable type of wrongdoing with devastating effects on the victims from which children are entitled to State protection considering the threat to their physical and mental welfare and the vulnerability of their young age.

It must also be noted that the voluntary activities by certain NI-ICS providers "play a valuable role in enabling the identification and rescue of victims, and reducing the further dissemination of CSAM, while also contributing to the identification and investigation of offenders, and the prevention of child sexual abuse offences."[140] In 2019, for instance, Facebook alone reported 16 million CSAM online.[141]

There is no doubt that the processing of personal data by NI-ICS providers for the sole purpose of detecting, removing and reporting CSAM pursues a legitimate aim regardless of the scenarios identified. However, the fact that the measures would serve a serious and pressing social need does not necessarily mean that the measures are lawful under EU law. In order to be lawful under EU law, the measures envisaged must be reconciled with other human and fundamental rights affected by the measure.[142] The objectives of general interest and the requirements of necessity and

---

134 *La Quadrature du Net and Others v Premier ministre and Others*, Joined Cases C-511/18, C-512/18 and C-520/18, 6 October 2020, ECLI:EU:C:2020:791 Para.128.

135 ibid.

136 Article 24, the Charter.

137 EU strategy for a more effective fight against child sexual abuse, COM(2020) 607 final; On the exponential growth of CSAM online, see Elie Bursztein◊ and others, 'Rethinking the Detection of Child Sexual Abuse Imagery on the Internet' (2019).

138 European Parliament Resolution of 26 November 2019 on children's rights on the occasion of the 30th anniversary of the UN Convention on the Rights of the Child, 2019/2876(RSP).

139 Canadian Centre for Child Protection, 'Survivor's Survey' (full report 2017) <https://www.protectchildren.ca/pdfs/C3P_SurvivorsSurveyFullReport2017.pdf> accessed 14 December 2020.

140 Recital 5, Proposed Regulation.

141 EU strategy for a more effective fight against child sexual abuse, COM(2020) 607 final P.16.

142 *La Quadrature du Net and Others v Premier ministre and Others, Joined Cases C-511/18, C-512/18 and C-520/18, 6 October 2020, ECLI:EU:C:2020:791*, Para.130.

proportionality are closely linked. As such, the following sub-section examines the three scenarios against the 'necessity and proportionality' test.

D. Necessity and proportionality

The detection, reporting and removing of CSAM by NI-ICS providers, which necessarily involves the processing of personal data, could only be considered a justified restriction to the extent that it constitutes a strictly necessary and proportionate measure in a democratic society.[143]

Under Scenario 1, the transposition of the EECC would prevent NI-ICS providers from continuing their own measures on voluntary detection, removal and reporting of CSA online. As the practice would become illegal, there is no need for the balancing test for this scenario.

This section, therefore, focuses on whether and to what extent the proposed regulation meets these requirements under EU law. This analysis considers the EDPS guidelines on assessing the 'necessity' and 'proportionality' of measures that limit the fundamental rights to privacy and to the protection of personal data issued in 2017 and 2019. The caselaw of the CJEU requires that a lawful limitation on the exercise of the rights to privacy and data protection must be strictly necessary in view of the purpose pursued. In *Digital Rights Ireland*, for instance, the CJEU held that "so far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled caselaw, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary".[144] The proposed legislation should provide a clear and detailed description of the envisaged measures so as to assess whether such measures pass the 'strictly necessary' and 'proportionality' test under Article 52(1) of the Charter.[145]

The 'strictly necessary' test under Article 52(1) requires that the measures proposed must be the least intrusive compared to other options for achieving the same goal.[146] In other words, the proposed measures can be justified only if there are no other less intrusive, but equally effective, alternatives by which the general interest pursued can be achieved. For instance, if there are other alternative measures that can equally help fight CSAM by collecting lesser quantity of personal data compared to what is required in the envisaged measures, then the proposed regulation would fail to meet the strictly necessary test. Determining whether the proposed measure is the least intrusive is an empirical question in the sense that in order to answer it, all the alternative measures should be comprehensively identified with sufficient and detailed descriptions of the scope, extent and level of intrusiveness of the measure. Such alternative measures may include existing police capability such as online undercover investigation techniques often used to infiltrate paedophile rings. For instance, the Commission has recently confirmed that 'online undercover investigation techniques "have proven very effective in understanding offender behaviour and interaction on online service providers, and have ultimately facilitated the shutting down of communication channels used by these offenders, as well as their prosecution".[147] However, the proposed regulation

---

143 Art. 52 Charter See also Article 8(2) ECHR; Article 15(1), e-Privacy Directive.

144 *CJEU, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [GC], Joined cases C-293/12 and C-594/12, 8 April 2014* paragraphs 52; *La Quadrature du Net and Others v Premier ministre and Others, Joined Cases C-511/18, C-512/18 and C-520/18, 6 October 2020, ECLI:EU:C:2020:791*, Para.130.

145 EDPS, 'Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit' (11 April 2019) 9.

146 EDPS, 'Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit' (11 April 2017).

147 EU strategy for a more effective fight against child sexual abuse, 24.7.2020 COM(2020) 607 final, P.8.

is not accompanied by such a detailed explanation of the specific measures or the existence of other measures.

According to the Commission, the reason for not providing sufficient evidence to support the envisaged measures is the temporary nature of the measures and the fact that the Commission will propose comprehensive and long-term legislation in 2021. However, the temporary nature of the derogation should not be a justification to interfere with fundamental rights, especially if the Commission intends to incorporate the envisaged measures into the long-term legislation. For instance, there is no sufficient evidence to demonstrate that the current practices by NI-ICS providers are effective in fighting CSAM. The fact that the number of detected CSAM keep rising suggests that preventive measures should be prioritised instead of indiscriminate scanning of communications to detect, remove and report CSAM after harm is already done.[148] Therefore, without sufficient evidence to demonstrate that the current practices are effective in fighting CSAM and that there are no other less intrusive but equally (or more) effective alternatives, it is difficult to determine whether the measures envisaged by the proposed regulation would meet the strictly necessary and proportionate test.

The increasing use of decentralised or encrypted channels of communication by offenders is another factor that could undermine the effectiveness of the measures envisaged by the proposed regulation.[149] As the EU has recently recognised, "offenders have become increasingly sophisticated in their use of technology and technical capabilities including encryption and anonymity (e.g. peer-to-peer file sharing and the use of darknet)."[150] This would in turn expose children to additional risks of abuse because offenders would be out of reach from law enforcement authorities.

The proposed regulation repeatedly states that the derogations are proportional and strictly necessary for the sole purpose of detecting, removing and reporting CSAM online. For instance, Article 3 of the proposed regulation requires the rights and obligations provided under Article 5(1) and Article 6 of the e-Privacy Directive regarding the processing of personal and other data in connection with the provision of NI-ICS to be *"…strictly necessary for the use of technology for the sole purpose of removing child sexual abuse material and detecting or reporting child sexual abuse online…"*. While these requirements are commendable, the proposed regulation lacks clarity on how these requirements work in practice.

This lack of clarity is exacerbated by the uncertainties as to the specific technologies that are covered by the proposed regulation. Under Article 3(a) and Recital 11, the proposed regulation tries to specify the type of technologies that would benefit from the derogation, the scope and extent of their use, and their level of intrusiveness. Article 3(a) stipulates that the derogations should be "…limited to well-established technologies regularly used by providers of number-independent interpersonal communications services for that purpose before the entry into force of this Regulation, and that are in accordance with the state of the art used in the industry and are the least privacy-intrusive." According to this provision, the technologies used to process personal data for the purpose of detecting, removing and reporting CSAM by NI-ICS providers must be (i) well-established in the industry, (ii) regularly used by NI-ICS providers, (iii) used before the entry into force of the proposed regulation, and (iv) the least privacy-intrusive in accordance with the state of the art in the industry.

---

148 Alexander Hanff, "Why I don't support privacy invasive measures to tackle child abuse' (11 November 2020) available at <https://www.linkedin.com/pulse/why-i-dont-support-privacy-invasive-measures-tackle-child-hanff/>.

149 Alexander Hanff, "Why I don't support privacy invasive measures to tackle child abuse' (11 November 2020) available at <https://www.linkedin.com/pulse/why-i-dont-support-privacy-invasive-measures-tackle-child-hanff/>.

150 EU strategy for a more effective fight against child sexual abuse, 24.7.2020 COM(2020) 607 final, p.6.

The proposed regulation does not provide any criterion on how to determine whether a specific technology meets these requirements. For instance, it is not clear what constitutes "well-established technology" within the meaning of the proposed regulation. Even though the Commission has mentioned some examples of current technologies, they are not necessarily covered by the proposed regulation.[151]

Furthermore, the fact that a specific technology has been commonly used by the NI-ICS providers for the mentioned purposes does not sufficiently justify the envisaged measures. It is also unclear whether the Commission intends to preclude future technologies and rely only on previously deployed ones. While Article 3(a) provides that the derogations would apply to technologies that have been deployed "before the entry into force" of the proposed regulation, Recital 5 suggests that the Regulation does not intend to preclude "the further evolution of the technology in a privacy-friendly manner". Such lack of clarity on the type of technologies that would fall within the envisaged derogation risks legal uncertainty.

As previously indicated, the three types of technologies commonly used in industry are hashing technology for previously known images and videos, classifiers and artificial intelligence for previously unknown CSAM,[152] and grooming/solicitation detection techniques for text based CSAM. However, it is also important to note that these technologies are not the same in their function, accuracy, effectiveness, and level of intrusiveness with fundamental rights. This means that these technologies cannot equally meet the requirements set out under Article 3 of the proposed regulation. For instance, Article 3(b) provides that "the technology used is in itself sufficiently reliable in that it limits to the maximum extent possible the rate of errors regarding the detection of content representing child sexual abuse".

Hashing technology (PhotoDNA for images and videos) is the only technology that can sufficiently meet this criterion. PhotoDNA does not only have a high level of accuracy (its rate of false positives is estimated at no more than 1 in 50 billion) but is also the least privacy-intrusive technology because it involves only a one-way transformation of data to digital signatures of known CSAM, thus removing any personally identifiable information.

By contrast, the other commonly used technologies classifiers and artificial intelligence, and grooming detection techniques involve automated analysis and indiscriminate scanning of communications content and related traffic data. Such an automated and indiscriminate scanning of communications content and related traffic data by NI-ICS providers could not meet the requirement of necessity and proportionality under Article 52(1) of the Charter. In this regard, the EDPS argues that "Even if the technology used is limited to the use of "relevant key indicators", the deployment of such general and indiscriminate analysis is excessive." This argument is consistent with the caselaw of the CJEU. For instance, in La Quadrature du Net (C 511/18 and C 512/18), the CJEU held that "the automated analysis of that [communications] data can meet the requirement of proportionality only in situations in which a Member State is facing a serious threat to national security which is shown to be genuine and present or foreseeable, and provided that the duration

[151] Questions for written answer to the Commission by the EP rapporteur Birgit Sippel, S&D, and her shadows (28 September 2020) (file with authors) p.5.

[152] For details on this, see <https://getsafer.io/?__hstc=208625165.6e43b6ca1a24ae39c45825db9e93e751.1607863065103.1607863065103.1607863065103.1&__hssc=208625165.2.1607863065104&__hsfp=3312982632>.

[153] Missing Children Europe, *Intergroup Expert Meeting on EU Legislation on the Fight against Child Sex Abuse Online* (2020) <https://www.youtube.com/watch?feature=youtu.be&v=adY_uWfs90E&app=desktop> accessed 13 December 2020.

[154] EDPS, 'Opinion 7/2020 on the Proposal for Temporary Derogations from Directive 2002/58/EC for the Purpose of Combatting Child Sexual Abuse Online' (10 November 2020) para.26.

of that retention is limited to what is strictly necessary to protect national security and, more particularly, to prevent terrorism".[155]

Even though the proposal states that the techniques used to detect text based CSAM work based on relevant key indicators, there is no objective criterion that could help determine what these relevant indicators are. Under Article 3, the proposed regulation requires that:

"(c) the technology used to detect solicitation of children is limited to the use of relevant key indicators, such as keywords and objectively identified risk factors such as age difference, without prejudice to the right to human review;"

This provision risks the general and indiscriminate monitoring and analysis of communications content and related traffic data of innocent users. As the Commission has confirmed, the indicators used to detect text based CSAM may vary from one technology to another, therefore making it difficult to determine the exact indicators and keywords stipulated under Article 3(c). The techniques used to detect solicitation of children are not only disproportionate but also prone to errors. Therefore, when it comes to detecting text based CSAM and previously unknown images, the proposed regulation in its current format does not meet the 'strictly necessary' and 'proportionate' test under Article 52(1) of the Charter. In order to mitigate this uncertainty, this study recommends that additional safeguards be incorporated into the proposed regulation (Scenario 3).

Conclusion:

- The proposed regulation could affect a number of fundamental rights including children's rights, privacy and data protection of users, and freedom of expression. While the detection, removal, and reporting of CSAM by NI-ICS will have **a positive contribution to the protection of fundamental rights of the child, these measures will also negatively affect the fundamental rights of other users such as the right to privacy, data protection and the right to freedom of expression and confidentiality of communications.**
- By allowing NI-ICS providers to process personal data for the purpose of detecting, removing, and reporting CSAM online, the measures envisaged by **the proposed regulation constitute an interference with the exercise of fundamental rights to confidentiality of communications and protection of personal data regardless of the legitimate aim pursued.**
- It is necessary to consider the legal basis used for the voluntary processing of content or traffic data for the purpose of detecting, removing and reporting CSA online since the proposed regulation itself explicitly does not provide one. Articles 6(1)(a), 6(1)(b), 6(1)(c), and 6(1)(e) of the GDPR would not provide adequate protection to users if they are used as the legal basis. Only Articles 6(1)(d) (for vital interests) and 6(1)(f) (for legitimate interests) could serve as legal bases that would provide adequate protections. Therefore, **the proposed regulation must include clear and explicit language that limits the derogation to the e-Privacy Directive to those voluntary practices expressly conducted using Article 6(1)(d) or 6(1)(f) of the GDPR as their legal basis.** Any practices carried out by NI-ICS providers to combat CSA online using any other legal basis should not be able to avoid their duties and responsibilities under Article 5(1) and 6 of the e-Privacy Directive.

[155] *La Quadrature du Net and Others v Premier ministre and Others*, Joined Cases C-511/18, C-512/18 and C-520/18, 6 October 2020, ECLI:EU:C:2020:791, Para. 177, 178.

- The processing of personal data by NI-ICS providers for the sole purpose of detecting, removing and reporting CSAM pursues a legitimate aim. However, **the fact that the measures would serve a serious and pressing social need does not necessarily mean that they are lawful under EU law.** The measures envisaged must be reconciled with other human and fundamental rights affected by the measures.
- Without sufficient evidence to demonstrate that the current practices are effective in fighting CSAM and that there are no other less intrusive but equally effective alternatives, it is difficult to determine whether the measures envisaged by the proposed regulation would meet the strictly necessary and proportionality test. Furthermore, **the current technologies that would be covered by the proposed regulation are different in terms of accuracy, effectiveness, and level of intrusiveness.** Hashing algorithms used for images and videos are the least-intrusive technologies and can meet the proportionality test. By contrast, other technologies, especially text-based child grooming detection techniques involve automated analysis and indiscriminate scanning of communications content and related traffic data and are prone to errors and vulnerable to abuse. **Without clear and precise additional safeguards, these technologies could not meet the necessity and proportionality test under Article 52(1) of the Charter.**

5. Effective Remedies

This section aims at answering the fourth research question: What is the impact of the proposed regulation on the right to an effective remedy in accordance with Article 47 of the EU Charter of Fundamental Rights, if the users are not aware that the content of their private communications is scanned and potentially flagged up for human review?

5.1. Right to effective remedy

Article 47 of the Charter guarantees the right to an effective remedy before a court. The CJEU enshrined that right in its judgments as a general principle of EU law.[156] Furthermore, Article 47 of the Charter also provides for the right to a fair trial.

An effective remedy therefore entails that anyone alleging that their rights have been violated has recourse to justice, meaning having access to a court or tribunal that is competent to hear the alleged violation.

5.1.1. When would remedies be needed?

There are at least two types of (documented) instances when a remedy or access to justice may be needed following from the practices that fall within the remit of this proposed regulation:

a. When alleged CSAM is found on the services of a NI-ICS, the NI-ICS acting in line with its terms and conditions, suspends or blocks access to the account where the CSAM was found. Different consumer organisations[157] have reported an increase in reports by users whose accounts have been blocked without pre-notice and without the ability to save data. According to a Dutch consumer organisation, accounts can be blocked with the mere notification that the Microsoft service-agreement has been violated, without making it clear why this is the case, what the user can do and where they can find recourse. This was also the case in a recent Dutch case,[158] when a man whose Microsoft accounts were closed only found out why this was the case in court during interim proceedings ('kort geding').

The reason for closing the account was that PhotoDNA marked a photo on his OneDrive account, which he had (presumably) shared, as CSAM. While the court found that Microsoft was within its rights to shut down the account, it ordered Microsoft not to delete the plaintiff's data while awaiting main proceedings. Without going into whether or not the man in question was at fault (he claimed that the image was sent to him and that he did not share it), the fact remains that the account was completely blocked or suspended without any information as to why this was the case. The question is what sort of information or remedy should be given to a user.

For such cases, clear information and remedies should be in place. At this point, it seems that Microsoft's policy is to shut down an account with a mere notification that a violation has occurred, without clear information on redress. As such, Microsoft fails to provide a remedy in this matter. This is not questioning the reliability of the software but questioning the company policy in that regard.

---

156 Case 222/84 Johnston [1986] ECR 1651; see also judgment of 15 October 1987, Case 222/86 Heylens [1987] ECR 4097 and judgment of 3 December 1992, Case C-97/91 Borelli [1992] ECR I-6313.

157 https://www.consumentenbond.nl/digitaalgids/digitaalgids-uitgelicht/microsoft-blokkeert-account

158 Rechtbank Midden-Nederland C/16/504246 / KL ZA 20-163 [2020] ECLI:NL:RBMNE:2020:4348.

From a NI-ICS providers' perspective, giving information or reasons for blocking the account may be difficult, especially if the material has been forwarded to LEAs and is under investigation.

b. Alleged CSAM found on the services of a NI-ICS may be a leading, if not the leading, piece of electronic evidence in a trial of an alleged suspect. It is being argued in literature[159] that unless safeguards exist which ensure that electronic information (later to be used as evidence) is collected, stored and analysed in a way that no tampering with the evidence took place, the right to a fair trial may not be guaranteed in a later stage of the process. As the EDPS notes in paragraph 38, "in terms of quality and integrity requirements, additional safeguards should be implemented in order to guarantee that this information considered as digital evidence has been properly collected and preserved and would therefore be admissible before a court. Guarantees related to the supervision of the system and its use, in principle by law enforcement authorities, are decisive elements to comply with. Transparency and independent redress possibilities available to individuals are other essential elements to be integrated in such a scheme."[160]

5.2. Remedies in the proposed regulation

There is no reference to remedies for either of these instances in the proposed regulation. The Commission explains[161] that:

a. any person has a right to an effective remedy under the Charter rights;

b. where personal data may have been processed, remedies and access to DPAs also exist.

While the explanation of the Commission is correct, there are at least four considerations that shed doubt on the effectiveness of the Commission's explanations as remedies.

5.2.1. Access to court as effective remedy for acts of private actors:

Article 47 of the Charter, like Article 13 of the ECHR, applies primarily to acts committed by the administration or the executive against rights in the Charter or the ECHR. However, for acts of private actors, at least in the interpretation given by the ECtHR, to fall within the remit of Article 13, there must be a remedy where the State shares responsibility for such acts or has not taken the necessary measures concerning them.[162]

In the case of Scenario 1, the practices, if continued, are voluntary practices by NI-ICS providers and not an obligation by law, where the State shares no responsibility for the acts of private actors. Hence, following the current interpretation of the right to an effective remedy, a user whose account has been blocked, suspended or terminated cannot claim that their right to an effective remedy has been infringed as there is no such right for acts of private actors. Section 5.3 below will examine whether remedies under the GDPR can be used in this situation.

---

159 Stoykova, R. The Presumption of Innocence Evidentiary mechanisms in a digital context. *The International Journal of Evidence and Proof* (forthcoming) (accepted for publication).

160 European Data Protection Supervisor, Opinion7/2020 on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online, 10 November 2020, paragraph 38 https://edps.europa.eu/data-protection/our-work/publications/opinions/opinion-proposal-temporary-derogations-directive_en The EDPS also makes reference to his Opinion of the European Data Protection Supervisor on the proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, paragraph 15.

161 In Non-paper with explanations to the questions by the EP rapporteur Brigit Sippel, S&D, and her shadows dated 28 September 2020

162 *Plattform "Arzte für das Leben" v. Austria*, 1988, §§ 34-39) and *Paul and Audrey Edwards v. the United Kingdom*, 2002, § 101).

In the case of Scenario 2, under the proposed regulation the practices will remain voluntary practices and hence the current interpretation here too does not offer users a right to an effective remedy to acts carried out by private actors. Having no other specific remedy in the proposed regulation may leave a user at the mercy of private actors.

In the case of Scenario 3, new safeguards would need to be introduced anticipating the possible remedies for may be necessary for users, including the ability to access a court for actions carried out by a private actor.

5.2.2. Effective remedies in the context of online services

In the information sheet issued by the Council of Europe on Human Rights for Internet Users, the guidance notes:

"You have the right to an effective remedy when your human rights and fundamental freedoms are restricted or violated.[163] To obtain a remedy, you should not necessarily have to pursue legal action straight away. The avenues for seeking remedies should be available, known, accessible, affordable and capable of providing appropriate redress. Effective remedies can be obtained directly from Internet service providers, public authorities and/or national human rights institutions. Effective remedies can – depending on the violation in question – include inquiry, explanation, reply, correction, apology, reinstatement, reconnection and compensation."[164]

Following these guidance notes, access to court then can be seen as a last resort but other remedies should also be provided.

In the case of Scenario 1, the effective remedies mentioned in the guidance notes, that is, e.g., inquiry, explanation, reply, correction, apology, reinstatement, reconnection and compensation, will only be available to a user if the private actors voluntarily provide them. The chance that this happens voluntarily may be rather small. A user would therefore have no effective remedy.

In the case of Scenario 2, under the proposed regulation there is no reference to options of effective remedies. As in the case of Scenario 1, effective remedies are dependent on the NI-ICS voluntarily extending these remedies to the users.

In the case of Scenario 3, the proposed regulation would introduce provisions anticipating possible remedies for users that are not restricted to access to court but also include e.g., inquiry, explanation, reply, correction, apology, reinstatement, reconnection and compensation for actions carried out by a private actor. As noted by the EDPS in his opinion on this proposed regulation,[165] an example of possible measures can be found in the Proposal for a Regulation on preventing the dissemination of terrorist content online which provides for information to content providers (subject to derogation where competent authorities decide that for reasons of public security including in the context of an investigation, it is considered inappropriate or counter-productive to directly notify the content provider of the removal or disabling of content).[166]

---

163 This first sentence is in bold in the original text.

164 https://www.coe.int/en/web/freedom-expression/effective-remedies.

165 European Data Protection Supervisor, Opinion7/2020 on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online, 10 November 2020, paragraph 40 https://edps.europa.eu/data-protection/our-work/publications/opinions/opinion-proposal-temporary-derogations-directive_en.

166 Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, Brussels, 12.9.2018, COM(2018) 640 final. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52018PC0640.

5.2.3. Timeliness of the remedy

In particular, by focusing on a remedy which is dependent on court procedures, one can question whether this would in this context (of the online activity of users) be a timely remedy. Court procedures in different EU Member States may not be as fast as one would need e.g., for the unblocking of an account, reconnection, possible correction etc. Furthermore, the lack of information that may be made available to a user on the reasons for the termination of services may make legal action by the user rather difficult to explain to a court or make it challenging to claim the existence of unfairness, negligence or practices against the contractual relationship by the provider.

In the case of Scenario 1, the timeliness of any remedy is dependent on the good-will of the NI-ICS to provide information in a timely manner for a user to be informed and, if necessary, take further action.

In the case of Scenario 2, since there is no reference to any remedies under the proposed regulation, as in Scenario 1, the timeliness of any remedy is dependent on the good-will of the NI-ICS to provide information in a timely manner for a user to be informed and, if necessary, take further action.

In the case of Scenario 3, the proposed regulation would need to include time limits imposed on the NI-ICS for the provision of information or for the provision of any other remedy.

5.2.4. Ensuring a right to a fair trial

In line with Article 47 of the Charter and Article 6 of the ECHR, whenever there is a determination of rights and obligations or any criminal charge, a person is entitled to a fair trial. One can argue that given that the nature of these voluntary activities and of the proposed regulation are not ones based on criminal law, the considerations on the right to fair trial do not fall within the scope of the Charter or the ECHR. However, it is to be noted that when CSAM is found as a result of the voluntary practices allowed under this proposed regulation, criminal proceedings may follow. A recognition that a person subject to legal action following from these practices are entitled to the right to a fair trial can ensure that all persons affected by this proposal are aware of the rights that follow from these practices. Furthermore, persons who were mistakenly surveilled may be entitled to a right to a fair trial should criminal proceedings be started against them.

5.3. Remedies under the GDPR

Given that the practices of NI-ICS providers must meet GDPR requirements[167], it is important to consider what remedies may be available under the GDPR. Article 77 of the GDPR provides a right for every data subject to lodge a complaint with a supervisory authority if the data subject considers that the processing of personal data infringes the GDPR. In addition, Article 79 of the GDPR provides that a data subject has the right to an effective judicial remedy against a controller or a processor where the data subject considers that his or her rights under the Regulation have been infringed as a result of the processing of personal data in a way which is non-compliant with the GDPR.

For the exercise of both these rights in the context of voluntary practices of NI-ICS, the data subject needs to know that the decision of the NI-ICS providers to block or suspend access to their account is related or based on the processing of the data subject's personal data.

[167] See Legislative Train Schedule: Promoting our European Way of Life. Proposal for a Regulation on a temporary derogation from certain provisions of the e-Privacy Directive for the purpose of combating child sexual abuse online https://www.europarl.europa.eu/legislative-train/theme-promoting-our-european-way-of-life/file-temporary-derogation-from-the-e-privacy-directive-for-ott-services.

While this may be the case in some situations, as noted earlier NI-ICS providers are often not in a position, given potential legal investigations or proceedings by competent authorities, to explain the reasoning behind their decision to a user/data subject. The effectiveness of the remedies under the GDPR are thus reduced and rather limited for the situation of Scenario 1 and Scenario 2.

In other areas,[168] where due to the lack of information available on practices, it is close to impossible for a person to seek any remedy, the ECtHR considered that a supervisory machinery/mechanism may be sufficient for as long as the measures remain unable to be disclosed. This may be included in Scenario 3. In the current proposed regulation, no supervisory mechanism, other than potentially the supervisory authority responsible in line with the GDPR, is considered. If the measure of suspension has not been reached through non-compliance of the GDPR, the role of the supervisory authority under the GDPR is rather limited. As a result, a user/customer of the NI-ICS remains effectively without any legal remedies. Under Scenario 3, a supervisory machinery/mechanism can be introduced.

Conclusion:

- **The proposed regulation makes no reference to options for effective remedies.** Users are dependent on NI-ICS voluntarily introducing remedies.
- **Users who are not aware that the content of their private communications is scanned and potentially flagged up for human review cannot avail themselves of the rights provided for in Article 47 of the Charter.** In line with current interpretations of Article 47 of the Charter, the right to an effective remedy cannot be invoked against a private actor (e.g., NI-ICS) unless the State shares responsibility in the acts of the private actor.
- **The remedies provided in the GDPR** (Article 77 & Article 79) **are also not sufficient.** The exercise of both these rights is dependent on the user knowing that the decision of the NI-ICS providers to block or suspend access to their account is related or based on the processing of their personal data.
- To avoid users being dependent on voluntary remedies introduced by NI-ICS, **the proposed regulation should introduce provisions anticipating possible remedies for users that are not restricted to access to court** but also include e.g. inquiry, explanation, reply, correction, apology, reinstatement, reconnection and compensation for actions carried out by a private actor /or the setting up of a supervisory mechanism for as long as the measures taken by NI-ICS cannot be disclosed, for instance, pending legal investigations or proceedings by competent authorities.

[168] E.g. in situations of covert surveillance and personal data retention.

6. Proposing Additional Safeguards

Based on the analysis of the proposed regulation as it currently stands, along with Article 52(1) of the Charter (discussed in section 4 above), several additional safeguards can be suggested to ensure better protection for the rights of users of NI-ICS while simultaneously curbing the spread of CSAM and protecting children from abuse online.

6.1. Different safeguards for different types of technologies

To meet the requirements of the principles of necessity and proportionality, the safeguards provided in the proposed regulation under Article 3 are not sufficiently nuanced. This is due to the differences in the technologies used to detect, report and remove CSAM from interpersonal communications services. The conceptual additions to the safeguards are discussed below.

As discussed previously, there are two main types of technologies: (i) for images/videos, and (ii) for text conversations. Technologies dealing with the former use hashing algorithms (such as PhotoDNA, PDQ, TKM+PDQF and Safer) and are far more reliable and well-established than machine learning-based algorithms (such as Project Artemis, and Facebook's tools) that deal with the latter.

However, it should be noted that despite text-based technologies such as Project Artemis being less reliable than PhotoDNA and the lack of concrete evidence regarding their effectiveness, NCMEC insists in their open letter to EU Parliament Members that they are still effective in detecting child grooming attempts.[169] Further, text messaging is clearly a major vector in child abuse; NCMEC's in-depth analysis of CyberTipline reports shows that up to 34% of the reports had abusers engaging in text-based sexual conversation/role-play as a form of grooming.[170]

Furthermore, the nature of machine learning algorithms is such that it is hard to understand exactly how they work even if they work well,[171] and they keep getting more efficient over time.[172] Given the commitment of service providers in detecting, reporting and removing CSAM on their platforms (as can be seen through Project Protect, alluded to earlier), it is likely that their algorithms for text-based analysis will show more promise over the five-year life of the proposed regulation. It is necessary to provide additional safeguards for the use of such technologies when compared to image/video analysis. The most important of these safeguards have been discussed below.

6.2. Safeguards for the transfer of personal data to third countries

Under US federal law, NI-ICS providers are under a duty to report, as soon as reasonably possible after obtaining actual knowledge of CSAM, to NCMEC regardless of where the providers operate and irrespective of the location of where the users whose data is processed is.[173] NCMEC runs the main database of hashes and has the responsibility to determine whether specific material should be

[169] NCMEC, Letter to EU Parliament Members, available at: https://www.missingkids.org/content/dam/missingkids/pdfs/NCMEC%20letter%20to%20EU%20Parliament%20Members.pdf. Last accessed: 14/12/2020.

[170] NCMEC, The Online Enticement of Children: An In-Depth Analysis of CyberTipline Reports, available at: https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/Online%20Enticement%20Pre-Travel.pdf. Last accessed: 05/12/2020.

[171] Terrence J. Sejnowski, *The unreasonable effectiveness of deep learning in artificial intelligence*, Proceedings of the National Academy of Sciences Dec 2020, 117 (48) 30033-30038.

[172] OpenAI, *AI and Efficiency*, available at: https://openai.com/blog/ai-and-efficiency/. Last accessed: 14/12/2020.

[173] 18 U.S. Code § 2258A. Reporting requirements of providers. https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section2258A&num=0&edition=prelim.

included in the database as CSAM. For this reason, relevant EU LEAs rely largely on the reports they receive from NCMEC. For instance, the Commission confirmed that "NCMEC received over 725 000 such reports concerning the EU in 2019 which it forwarded to the relevant law enforcement agencies in the EU."[174]

As part of the duty to report, the NI-ICS providers pass on information about the involved individual, information relating to when and how a customer or subscriber of a provider uploaded, transmitted, or received content relating to the report and geographic location information of the involved individual.[175] This information could be on data subjects who are located in the EU. The NI-ICS provider would hence be transferring the personal data of data subjects who are in the EU to a non-governmental organisation, NCMEC, in third countries that possibly lack an adequate level of data protection essentially equivalent to EU law. The major NI-ICS providers that would fall under the scope of the proposed regulation are headquartered in the US and hence subject to US law and hence subject to this duty to report CSAM once they obtain actual knowledge of it.

Following recent caselaw,[176] it is important that the proposed regulation clarifies the legal basis for the transfer of data outside the EU in line with the GDPR. Whether the proposed regulation intends to create a new legal basis for the transfer of data to third countries is not clear. Considering this legal uncertainty, the proposed regulation should require NI-ICS providers to comply with the legal basis set out under Chapter V of the GDPR. When they transfer personal data to third countries or international organisations, NI-ICS providers should ensure that third countries have a level of protection essentially equivalent to that guaranteed by EU law. The proposed regulation should also require NI-ICS providers to incorporate the type and volume of data transferred to third countries and the legal basis used for such transfers as part of the periodic reporting obligations stipulated under Article 3(e).

6.3. Prior Consultation with DPAs for the use of technical measures

Given the potential impact on the right to privacy and data protection of technical measures used to detect CSAM and keeping in mind that technical measures evolve over time, it is important to take into account measures to review the use of technical measures by NI-ICS providers. What is suggested in this situation is that the proposed regulation makes specific reference to Article 35 of the GDPR to be followed before a technical measure is used and to Article 36 of the GDPR requiring prior consultation. The EDPS recommends the introduction, also with a view of providing legal certainty, of an explicit requirement of carrying out a DPIA within the meaning of Article 35 GDPR in relation to any processing that falls within the scope of the proposed derogation.[177]

Article 35 of the GDPR makes it mandatory for service providers to carry out a data protection impact assessment if their processing is "likely to result in a high risk to the rights and freedoms of natural persons". The systemic filtering and scanning of communications content and related traffic data by

---

174 COM(2020) 607 final EU strategy for a more effective fight against child sexual abuse p.2 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf.

175 18 U.S. Code § 2258A. Reporting requirements of providers.

176 Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650; and C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* ECLI:EU:C:2020:559.

177 European Data Protection Supervisor, Opinion7/2020 on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online, 10 November 2020, paragraph 46 https://edps.europa.eu/data-protection/our-work/publications/opinions/opinion-proposal-temporary-derogations-directive_en.

NI-ICS providers for the purpose of detecting, removing and reporting CSA online could result in it being classed as 'high risk' within the meaning of the GDPR.

As highlighted above, the techniques used to detect unknown CSAM and scanning for the solicitation of children may risk the general and indiscriminate monitoring of communications of all users. Furthermore, the processing operation involves special categories of data (such as a natural person's sex life or sexual orientation) within the meaning of Article 9 of the GDPR. The processing of such data triggers a mandatory prior Data Protection Impact Assessment (DPIA) under Article 35(3)(b). Therefore, the proposed regulation should incorporate explicit provisions that would require NI-ICS providers to carry out a DPIA prior to the deployment of any technology.

6.4. Internal review mechanism

Service providers typically have internal review mechanisms – whether automated or human – that apply to content published on their platform. The extent to which these review mechanisms apply to interpersonal communications services is unclear. Facebook, for example, has published community standards and content moderation guidelines that apply across its services.[178] These rules may therefore be applicable to Facebook Messenger as well, as long as it is not covered by end-to-end encryption, since this encryption would make the content of messages sent on Facebook's messaging services unavailable for moderation by Facebook. Instagram has similar rules in place, but their enforcement in direct messages is unclear. At the moment, Facebook Messenger and Instagram's direct messaging services are not end-to-end encrypted, so it is possible that content on these services is being monitored for CSAM.[179] Similar rules do not exist for WhatsApp since it is end-to-end encrypted.

The general rules set out by Facebook and Microsoft's Xbox Live[180] provide for an appeal process if users contest decisions taken during Facebook's review. However, these appeals processes are triggered once an account has been banned or locked. The process cannot be triggered by users if they believe that their privacy has been infringed through automated content moderation when their accounts have not been banned.

Greater safeguards related to such internal redress mechanisms may go a long way towards protecting innocent users' rights. As discussed in Section 5.2.2 of this study, these could include mechanisms that provide users with the right to request an inquiry, an explanation, a reply, a correction, an apology, and also notification, reinstatement, reconnection and compensation from the NI-ICS provider if a user's data was incorrectly flagged as containing CSAM. Therefore, the proposed regulation should incorporate explicit provisions that require NI-ICS to put in place clear and transparent procedures to ensure that users have appropriate redress when their communications are mistakenly flagged as CSAM or their account blocked. The proposed regulation should also require NI-ICS to report on such internal redress mechanisms as part of the transparency and accountability obligation under Article 3(e).

---

[178] Facebook Community Standards, available at: https://www.facebook.com/communitystandards. Last accessed: 05/12/2020.

[179] For example, content moderators at Facebook have reported vetting private chats on the platform. *See* Hern, A. (2019), "Revealed: catastrophic effects of working as a Facebook moderator", *The Guardian*, 17 September [online]. Available at: https://www.theguardian.com/technology/2019/sep/17/revealed-catastrophic-effects-working-facebook-moderator (Accessed: 5 December 2020).

[180] Microsoft Support, "Learn why your account was banned or suspended from Xbox Live", available at: https://support.microsoft.com/en-us/account-billing/learn-why-your-account-was-banned-or-suspended-from-xbox-live-87d8f88a-d45f-1955-d39f-deb3a64bd6cd. Last accessed: 05/12/2020.

6.5. Human Oversight

The use of indiscriminate automated analysis of data, as already mentioned in section 4, is very intrusive and the CJEU in its caselaw[181] seems to only permit this automated analysis in particular circumstances.

While Microsoft's Project Artemis requires human oversight for any text conversation triggered by the machine learning algorithm that detects CSAM before they are forwarded to LEAs, this is not in itself a sufficient safeguard. Individual re-examination by non-automated means before an individual measure adversely affecting the persons concerned is adopted[182] should be included in the proposed regulation regarding all automated text analysis technologies used by NI-ICS providers.

This may ensure the reduction of false positives. Note that due to COVID-19, some service providers such as Facebook have reduced their reliance on human oversight[183] which may create a greater risk of infringements of users' fundamental rights given the lower reliability of text-based analysis. The proposed regulation should require human oversight before a report is sent to LEAs and NGOs acting in the public interest against CSA. Article 3(c) of the proposed regulation makes reference to human review[184] but does not establish parameters for the right to human review. A specific requirement would ensure that human moderators are involved in every critical decision that could affect human and fundamental rights.

6.6. Data retention

Some technologies such as Microsoft's Project Artemis depend on the analysis of historical chat conversations to detect child grooming incidents. Therefore, chat conversations need to be retained for some length of time and are deleted only after analysis is conducted and they are found to be free of CSAM. This requires the retention of data which is contrary to Article 3(d) of the proposed regulation, under which any data where CSA is not "detected and confirmed" must be erased immediately. Instead of banning the retention of any data where CSA is not yet detected, as the language of Article 3(d) currently states, safeguards related to data retention should be more nuanced and in line with the CJEU's judgments regarding the Data Retention Directive, so that data retention is allowed to the extent that it is strictly necessary for the detection of CSA, for a limited time and subject to effective review (either judicial or administrative).[185] This would allow algorithms used for the detection of text-based child grooming to function as intended – subject to all other safeguards outlined in this section.

---

[181] See for example, Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v Premier ministre and Others ECLI:EU:C:2020:791* Para.172-182.

[182] As suggested in Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v Premier ministre and Others ECLI:EU:C:2020:791* Para. 182.

[183] Facebook, Keeping People Safe and Informed About the Coronavirus, available at: https://about.fb.com/news/2020/12/coronavirus/. Last accessed: 05/12/2020.

[184] Article 3(c) of the Proposed Regulation states "the technology used to detect solicitation of children is limited to the use of relevant key indicators, such as keywords and objectively identified risk factors such as age difference, without prejudice to the right to human review;". The Proposed Regulation thus considers that that there may be situations where human review takes place but does not specify the conditions under which this right would arise.

[185] *See* Judgment of the Court (Grand Chamber) of 6 October 2020, C-623/17, Privacy International, ECLI:EU:C:2020:790, *and* Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others, ECLI:EU:C:2020:791.

6.7. Encryption

The proposed regulation should specifically state that its scope does not include end-to-end encryption. Without such a safeguard, it is possible that Member States may compel service providers to institute backdoors into the encryption using the proposed regulation as the legal basis. While it is true that end-to-end encryption may hinder the detection of CSAM online, expanding the scope into this territory will result in extended debate and negotiations, negating the Commission's need for urgency.

6.8. Transparency and accountability

Under Article 3(e) and Recital 14, the proposed regulation would require NI-ICS providers to publish annual reports in respect of the activities undertaken pursuant to the derogation. This is the only transparency and accountability mechanism envisaged by the proposed regulation. Even though this transparency and accountability mechanism should be considered as a positive step, it is not adequate for at least two reasons.

First, there is a lack of information as to the NI-ICS providers that are involved in the voluntary practice and the type of technology they deploy. For instance, the Commission has confirmed that it is not possible to provide the complete list of all the companies involved in the practice of detecting, removing and reporting CSAM in the EU. For this reason, the *ex-post* periodic report may not be sufficient to ensure meaningful transparency and accountability. This uncertainty could be addressed by requiring NI-ICS providers to request prior authorisation from the DPAs. The NI-ICS providers should also be required to include, in addition to the information listed under Article 3(e), the list of NGOs to which CSAM have been reported.

Second, what makes the envisaged transparency and accountability mechanism inadequate is the dependence on public interest organisations that are established outside the EU. As highlighted above, NCMEC is not only operating the main databases for hashes, it also unilaterally decides whether and how to report CSAM to relevant authorities outside the US. It is not clear whether there are EU-based NGOs acting in the public interest against CSA. Therefore, the establishment of a public register of such organisations, as proposed by the EP Rapporteur, should be considered as additional mechanism of ensuring transparency and accountability.

6.9. Additional safeguards addressing the issue of indiscriminate monitoring

The study found that the techniques used to detect text-based child grooming involve indiscriminate monitoring and automated analysis of the private messages of all users. These techniques are not only disproportionate but also prone to errors, while being vulnerable to abuse. Owing to their intrusive and indiscriminate nature, these techniques (such as Microsoft's Project Artemis) should be subject to strict requirements, in addition to the safeguards discussed above. The proposed regulation should apply strict scope and time limitations to techniques that analyse private messages, as well as periodic review by DPAs. Instead of using these techniques to monitor all private messages, their use should be limited to private messages of persons already under suspicion of soliciting child abuse or distributing CSAM.

Conclusion:

Based on the analysis of the Proposed Regulation as it currently stands, along with Article 52(1) of the Charter (discussed in section 4 above), **several changes should be made to ensure better safeguards to the rights of users of NI-ICS while simultaneously curbing the spread of CSAM and protecting children from abuse online**. This includes adding nuance by differentiating between safeguards based on the type of technology in use; protecting personal data that is transferred to third countries; receiving prior authorisation from DPAs; adding a more elaborate internal review mechanism; expanding human oversight before reports are sent to LEAs; adding safeguards for data retention; clearly carving out end-to-end encryption from the Proposed Regulation; and improving transparency and accountability.

7. Main Findings

This targeted human rights impact assessment examined the following research questions:

1. What are the impacts of the proposed regulation on EU privacy and data protection rights (e-Privacy Directive and GDPR) as well as EU fundamental rights and the ECHR human rights of persons affected?
2. Does the proposed regulation comply with the principle of proportionality and the principle of subsidiarity, which includes an 'EU added value' test?
3. Are the safeguards provided for in the proposed regulation sufficient to ensure compliance with Article 52(1) of the EU Charter, taking account of the current case law of the CJEU and GDPR rules?
4. What is the impact of the proposed regulation on the right to an effective remedy in accordance with Article 47 of the EU Charter of Fundamental Rights, if the users are not aware that the content of their private communications is scanned and potentially flagged up for human review?

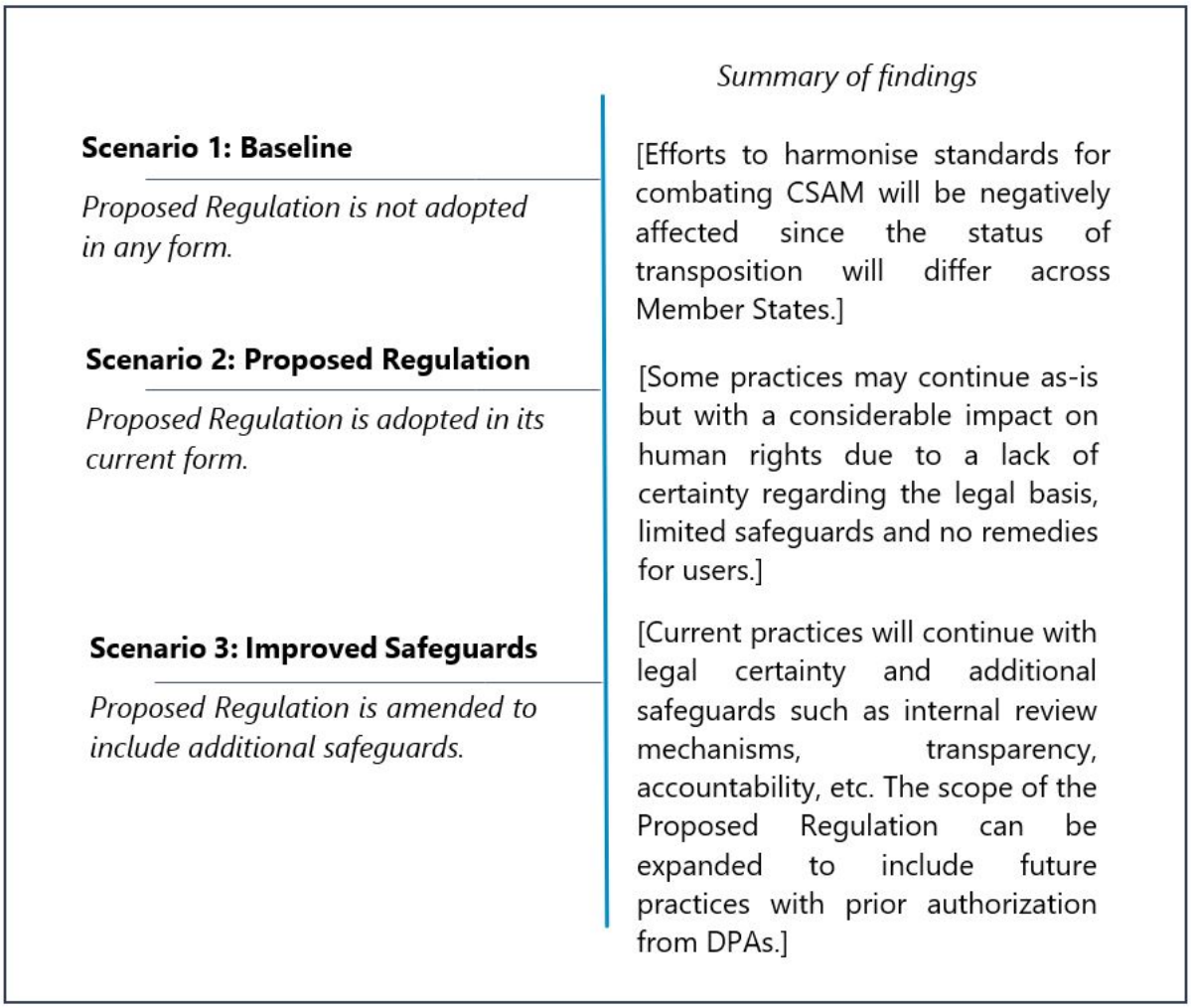
In order to answer these four questions, the study set the context for the proposed regulation and outlined three main scenarios in the following manner: a baseline scenario where the proposed regulation is not adopted (Scenario 1); a scenario where the proposed regulation is adopted in its current form (Scenario 2); and a scenario where the proposed regulation is amended to include further clarity in the text and additional safeguards for protecting fundamental human rights (Scenario 3).

The study then devoted a section each to the main issues identified in the proposed regulation: the EU's competence to adopt the proposed regulation (Section 2); whether the proposed regulation allows the technologies currently used to combat child sexual abuse to continue to be used (Section 3); the impact of the proposed regulation and current technologies on fundamental human rights (Section 4); the availability of remedies to those affected by the current technologies and the proposed regulation (Section 5); and finally, additional remedies and safeguards that should be included in the proposed regulation to ensure clarity and protection of the fundamental human rights of all users, including children (Section 6). All of the main findings in these respective sections were then put into the context of the four research questions above.

Based on the analysis in this study, it has been found that the proposed regulation takes major steps forward in the fight against child sexual abuse online and the proliferation of child sexual abuse material online. This comes at the cost of major direct and indirect consequences for the human and fundamental rights of all of the users of those services, since the proposed regulation creates an exception to the confidentiality of communications and traffic data otherwise granted by Articles 5(1) and 6 of the e-Privacy Directive. In creating such an exception, the proposed regulation should ensure that the impact on human and fundamental rights is alleviated through clear and precise language that meets the objective of combating CSAM, as well as robust safeguards that are in line with the current EU policy framework. **This study finds that the proposed regulation should be amended to add clarity to the text, as well as additional safeguards and remedies for the protection of fundamental human rights.** This is because the objective of the proposed regulation has not been completely met due to a lack of clarity regarding the legal basis for the processing of personal data using those technologies, as well as having the unintended effect of not covering algorithms that are either novel (such as perceptual hashing) or not well-established (such as machine learning). Thus, a baseline scenario (where the proposed regulation is not adopted, Scenario 1) has a negative impact on the fight against CSA but adopting the proposed regulation in its current form (Scenario 2) maintains the status quo, missing out on the

opportunity to create a much more positive impact on the fight against child sexual abuse while protecting the rights of users (Scenario 3). A summary of the findings for each scenario introduced in this study are presented in Fig. 2. The specific findings of the study are presented below the figure.

Figure 2. Summary of findings for each scenario



1. <u>Impact on fundamental human rights including privacy (first research question)</u>:

The proposed regulation could affect a number of fundamental rights including children's rights, the privacy and data protection of users, and freedom of expression. While the detection, removal, and reporting of CSAM by NI-ICS will have a positive contribution to the protection of the fundamental rights of the child, these measures will also negatively affect the fundamental rights of other users, such as the right to privacy, data protection and the right to freedom of expression and confidentiality of communications.

The proposed regulation constitutes an interference with the exercise of the fundamental rights to confidentiality of communications and protection of personal data. Such interference exists regardless of whether the processing is carried out by public authorities or private entities, and whether it is carried out on a voluntary basis or is required by law. The fact that the measures would serve a serious and pressing social need does not necessarily mean that they are lawful under EU law. The measures envisaged must be reconciled with other human and fundamental rights affected by the measures.

2. <u>The legality of Union action (second research question)</u>:

The proposed regulation meets the requirements of the principles of subsidiarity and proportionality (as relating to the test of EU competence). It also adds value by being adopted at the EU level. While there are concerns about the lack of additional safeguards and clarity in the language of the proposed regulation, acting at the EU level through a regulation ensures that policies regarding the effective detection, reporting and removal of CSAM online by NI-ICS providers are not fragmented. It also allows the EU to set a higher standard for the protection of the rights of both children and other users than that which may be set by individual Member States.

3. <u>Compliance of the proposed regulation with Article 52(1) of the Charter (third research question)</u>:

Article 52(1) of the Charter sets out specific criteria that must be met by any legislation that seeks to limit the exercise of the rights and freedoms provided by the Charter. These criteria are that: 1) the limitation must be provided for by law; 2) it must respect the essence of the rights; 3) it must genuinely meet the objectives of general interest recognised by the Union; and 4) it must be necessary and proportionate. This study examines whether the proposed regulation meets these criteria, since it does interfere with the fundamental rights to confidentiality of communications and the protection of personal data.

For the first criterion, it is necessary to consider the legal basis used for the voluntary processing of content or traffic data for the purpose of detecting, removing and reporting CSA online since the proposed regulation itself explicitly does not provide one. One of the six specified grounds set out in Article 6(1) of the General Data Protection Regulation (GDPR) could serve as alternative legal basis for voluntary processing of content or traffic data by NI-ICS providers for the purpose of detecting CSA online under the proposed regulation. Articles 6(1)(a), 6(1)(b), 6(1)(c), and 6(1)(e) of the GDPR would not provide adequate protection to users if they are used as the legal basis. Only Articles 6(1)(d) (for vital interests) and 6(1)(f) (for legitimate interests) could serve as legal bases that would provide adequate protections. Therefore, **the proposed regulation must include clear and explicit language that limits the derogation to the e-Privacy Directive to those voluntary practices expressly conducted using Article 6(1)(d) or 6(1)(f) of the GDPR as their legal basis.** Any practices carried out by NI-ICS providers to combat CSA online using any other legal basis should not be able to avoid their duties and responsibilities under Article 5(1) and 6 of the e-Privacy Directive.

The second criterion of 'respecting the essence of the rights' tests whether the right is in effect emptied of its basic content, effectively preventing the individual from exercising the right. Due to the specific standards and safeguards set out under Article 3, the proposed regulation respects the essence of the rights.

The proposed regulation also satisfies the third criterion of genuinely meeting an objective of general interest. In this case, the objective is the effective prevention, detection, and prosecution of child sexual abuse online, and the protection of victims of this offence. It also provides the protection necessary for the well-being of the child.

It should be noted that meeting the second and third criteria does not necessarily mean that the limitations to the exercise of rights and freedoms provided by the proposed regulation are lawful under EU law. These limitations must also meet the fourth criterion of necessity and proportionality. The proposed regulation is not accompanied by a detailed explanation of the specific measures or the existence of other possible measures. Without sufficient evidence to demonstrate that the current practices are effective in fighting CSAM and that there are no other less intrusive, but equally effective alternatives, it is difficult to determine whether the measures envisaged by the proposed regulation would meet the strictly necessary and proportionate test.

Furthermore, the current technologies that would be covered by the proposed regulation are different in terms of accuracy, effectiveness, and their level of intrusiveness. Hashing algorithms, which use one-way techniques to transform personally identifiable information into irrevocably randomised identifiers (or cryptographic hashes), are used to convert images and videos into hashes that are stored in a database. Instead of using the original images and videos, comparisons are done against this database. Thus, they are the least-intrusive technologies, meeting the proportionality test.

By contrast, other technologies, especially text-based child grooming detection techniques, involve the automated analysis and indiscriminate scanning of the original content of communications and related traffic data. At the same time, they are also prone to errors and vulnerable to abuse. Without clear and precise additional safeguards, these technologies will not meet the necessity and proportionality test under Article 52(1) of the Charter.

This can be rectified by adding safeguards that are not currently present in the proposed regulation: these include adding nuance by differentiating between safeguards based on the type of technology in use; protecting personal data that is transferred to third countries; receiving prior authorisation from Data Protection Authorities; adding a more elaborate internal review mechanism; expanding human oversight before reports are sent to law enforcement; adding safeguards for data retention; clearly carving out end-to-end encryption to ensure that the proposed regulation is not used to circumvent it; and improving transparency and accountability.

4. <u>Effective remedies for users (fourth research question)</u>:

The proposed regulation makes no reference to options for effective remedies. Users are dependent on NI-ICS voluntarily introducing remedies. Users who are not aware that the contents of their private communications are being scanned and potentially flagged up for human review cannot avail themselves of the rights provided for in Article 47 of the Charter. In line with the current interpretation of Article 47, the right to an effective remedy cannot be invoked against a private actor (e.g., NI-ICS) unless the state shares responsibility in the acts of that private actor. In addition, the **remedies provided in the GDPR** (Article 77 – to lodge a complaint with a supervisory authority and Article 79 – right to effective judicial remedy against a controller or a processor) **are also not sufficient** to protect users who are not aware that the content of their private communications is being scanned and potentially flagged up for human review. The exercise of both of these rights is dependent on the user knowing that the decision of the NI-ICS providers to block or suspend access to their account is related or based on the processing of their personal data.

To avoid users being dependent on voluntary remedies introduced by NI-ICS, **the proposed regulation should introduce provisions anticipating possible remedies for users that are not restricted to access to court but also include, for e.g., inquiry, explanation, reply, correction, apology, reinstatement, reconnection and compensation for actions carried out by a private actor and/or the setting up of a supervisory mechanism for as long as the measures taken by NI-ICS cannot be disclosed (for instance, pending legal investigations or proceedings by competent authorities).**

8. References

List of Cases:

Case law of the European Court of Justice

Case C-222/84 *Johnston v Chief Constable of the Royal Ulster Constabulary* ECLI:EU:C:1986:206.

Case 14/83 *Von Colson and Kamann* [1984] ECR 1891.

Case C-222/86 *Union nationale des entraîneurs et cadres techniques professionnels du football (Unectef) v Georges Heylens and others* ECLI:EU:C:1987:442.

Case C-97/91 *Oleificio Borelli SpA v Commission of the European Communities* ECLI:EU:C:1992:491.

Case C212/04 *Adeneler* [2006] ECR 1-6057.

Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen* ECLI:EU:C:2010:662.

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* ECLI:EU:C:2014:238.

Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650.

Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* ECLI:EU:C:2020:790.

Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* ECLI:EU:C:2020:559.

Joined Cases C-511/18, C-512/18 and C-520/*18 La Quadrature du Net and Others v Premier ministre and Others* ECLI:EU:C:2020:791.

Case C-61/19 *Orange România SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)* EU:C:2020:901.

Case law of the European Court of Human Rights

K.U. v. Finland, application ECHR 2008-V 1581.

Paul and Audrey Edwards v. the United Kingdom ECHR 2002-II 303, § 101.

Plattform "Arzte für das Leben" v. Austria (1988) Series A no. 139, §§ 34-39.

S and Marper v the United Kingdom ECHR 2008-V 1581.

Satakunnan Markkinapörssi Oy and Satamedia Oy V Finland App no 931/13 (ECtHR, 27 June 2017).

Other Case law

Judgement of 27.03.2019 - BVerwG 6 C 2.18. Para. 45-46. Available at <https://www.bverwg.de/270319U6C2.18.0>.

Rechtbank Midden-Nederland C/16/504246 / KL ZA 20-163 [2020] ECLI:NL:RBMNE:2020:4348.

Bibliography:

Legislation and treaties

Charter of Fundamental Rights of the European Union OJ C 326, 26.10.2012, p. 391–407.

Consolidated version of the Treaty on European Union OJ C 202 7.6.2016, p. 13.

Consolidated version of the Treaty on the Functioning of the European Union OJ C 326, 26.10.2012, p. 47–390.

Consolidated version of the Treaty on the Functioning of the European Union Protocol (No 2) On the application of the principles of subsidiarity and proportionality OJ C 202, 7.6.2016, p. 206–209.

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

of such data, and repealing Directive 95/46/EC (General Data Protection Regulation OJ L 119, 4.5.2016, p. 1–88.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') OJ L 178, 17.7.2000, p1–16.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, p 37–47.

Directive 2006/24/EC of the European Parliament and of the Council 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 and amending Directive 2002/58/EC OJ L 105, 13.4.2006, p. 54–63.

Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (codified version).
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02010L0013-20181218&from=EN.

Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA [2011] OJ L 335, 17.12.2011, p1-14.

Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) OJ L 321, 11.12.2018, p36-214.

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention of Human Rights).

18 U.S. Code § 2258A. Reporting requirements of providers.
https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section2258A&num=0&edition=prelim.

Documents by EU institutions and other EU bodies

Article 29 Data Protection Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (3 October 2017).

Article 29 Data Protection Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (WP 217, 9 April 2014).

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, EU strategy for a more effective fight against child sexual abuse, 24.7.2020 COM (2020) 607 final.

Council of Europe (2019), Member state responses to prevent and combat online child sexual exploitation and abuse. Baseline mapping. Report prepared by Victoria Baines https://rm.coe.int/191120-baseline-mapping-web-version-3-/168098e109.

Data Protection Commission of Ireland, 'Guidance on Legal Bases for Processing Personal Data' (December 2019).

EDBP, 'Guidelines 3/2019 on processing of personal data through video devices Version 2.0' (29 January 2020).

EDPB Opinion 5/2019 on the interplay between the e-Privacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities (12 March 2019).

EDPS, 'Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit' (11 April 2017).

EDPS, 'Guidelines on Assessing the Proportionality of Measures That Limit the Fundamental Rights to Privacy and to the Protection of Personal Data' (19 December 2019).

EDPS, 'Opinion 7/2020 on the Proposal for Temporary Derogations from Directive 2002/58/EC for the Purpose of Combatting Child Sexual Abuse Online' (10 November 2020).

EU strategy for a more effective fight against child sexual abuse, COM (2020) 607 final.

European Commission (2011) *The added value of the EU budget,* Brussels: EC. Available at: https://ec.europa.eu/budget/library/biblio/documents/fin_fwk1420/working_paper_added_value_EU_budget_SEC-867_en.pdf (Accessed: 4 December, 2020).

European Parliament (2020), *Online Platforms' Moderation of Illegal Content Online*. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652718/IPOL_STU(2020)652718_EN.pdf. (Accessed: 4 December 2020).

European Parliament Resolution of 26 November 2019 on children's rights on the occasion of the 30th anniversary of the UN Convention on the Rights of the Child, 2019/2876(RSP).

European Parliament, Report on the proposal for a regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards as the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online (COM(2020)0568 – C9 0288/2020 – 2020/0259(COD)), 11 December 2020.

European Parliament, Draft report on the proposal for a regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards as the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online, PE661.791v01-00, 27 November 2020.

European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law (Publications Office of the European Union 2018).

Europol (2020), Internet Organised Crimes Threat Assessment 2020, October 2020 https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf.

Flash Eurobarometer 469 – Report Illegal content online. Fieldwork June 2018 Publication September 2018 https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/83669.

Legislative Train Schedule: Promoting our European Way of Life. Proposal for a Regulation on a temporary derogation from certain provisions of the e-Privacy Directive for the purpose of combating child sexual abuse online https://www.europarl.europa.eu/legislative-train/theme-promoting-our-european-way-of-life/file-temporary-derogation-from-the-e-privacy-directive-for-ott-services.

Opinion 5/2016 Preliminary EDPS Opinion on the review of the e-Privacy Directive (2002/58/EC).

Literature and other online sources

Bird&Bird, *European Electronic Communications Code* [Online], Bird&Bird. Available at: https://www.twobirds.com/en/in-focus/european-electronic-communications-code/eecc-tracker. (Accessed: 4 December 2020).

Berman G. and Albrights K. Children and the data cycle: rights and ethics in a big data world, Office of Research – Innocenti Working Paper WP-2017-05, June 2017.

Barnard, C. and Peers, S. (2014), European Union Law. Oxford University Press.

Brkan, M. (2019), 'The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning' 20 German Law Journal pp. 864–883.

Bursztein, Elie et al (2019), Rethinking the Detection of Child Sexual Abuse Imagery on the Internet. WWW '19: The World Wide Web Conference May 2019 Pages 2601–2607 https://doi.org/10.1145/3308558.3313482.

Canadian Centre for Child Protection, 'Survivor's Survey' (full report 2017) Available at: https://www.protectchildren.ca/pdfs/C3P_SurvivorsSurveyFullReport2017.pdf (Accessed 14 December 2020).

Craig, P. and De Búrca, G. (2015), EU Law. 6th ed. Oxford: Oxford University Press.

Davis, A. and Rosen, G. (2019), "Open-Sourcing Photo- and Video-Matching Technology to Make the Internet Safer", *Facebook,* 1 August [online]. Available at: https://about.fb.com/news/2019/08/open-source-photo-video-matching/ (Accessed: 4 December 2020).

Dodd, V. 'Facebook's encryption plans could help child abusers escape justice, NCA warns, *The Guardian*, 23 November [online]. Available at: https://www.theguardian.com/uk-news/2020/nov/23/facebooks-encryption-plans-could-help-child-abusers-escape-justice-nca-warns. (Accessed: 4 December 2020).

ECPAT International (2018), "Trends in online child sexual abuse material", April 2018, Bangkok: ECPAT International https://www.ecpat.org/wp-content/uploads/2018/07/ECPAT-International-Report-Trends-in-Online-Child-Sexual-Abuse-Material-2018.pdf.

Farid, H. (2019) 'Fostering a Healthier Internet to Protect Consumers', *House Committee on Energy and Commerce,* 16 October [online]. Available at: https://www.congress.gov/116/meeting/house/110075/witnesses/HHRG-116-IF16-Wstate-FaridH-20191016.pdf (Accessed: 4 December 2020).

Faustomorales (2019), 'Show HN: Perceptual hashing tools for detecting child sexual abuse material', *YCombinator News*, 4 November [online blog] Available at: https://news.ycombinator.com/item?id=21445448. (Accessed: 4 December 2020).

Greenberg, A. (2020) 'Facebook Says Encrypting Messenger by Default Will Take Years', *Wired*, 10 January [online]. Available at: https://www.wired.com/story/facebook-messenger-end-to-end-encryption-default/. (Accessed: 4 December 2020).

Gregoire, C. (2020), "Microsoft shares new technique to address online grooming of children for sexual purposes", *Microsoft*, 9 January [online]. Available at: https://blogs.microsoft.com/on-the-issues/2020/01/09/artemis-online-grooming-detection/ (Accessed: 4 December 2020).

Hern, A. (2019), "Revealed: catastrophic effects of working as a Facebook moderator", *The Guardian*, 17 September [online]. Available at: https://www.theguardian.com/technology/2019/sep/17/revealed-catastrophic-effects-working-facebook-moderator (Accessed: 5 December 2020)

Interpol (2020), Threats and Trends Child Sexual Exploitation and Abuse COVID-19 Impact, September 2020 https://www.interpol.int/en/content/download/15611/file/COVID19%20-%20Child%20Sexual%20Exploitation%20and%20Abuse%20threats%20and%20trends.pdf.

Ith, T. (2015) 'Microsoft's PhotoDNA: Protecting children and businesses in the cloud', *Microsoft*, 15 July [online]. Available at: https://news.microsoft.com/features/microsofts-photodna-protecting-children-and-businesses-in-the-cloud/ (Accessed: 4 December 2020).

Langston, J. (2018) 'How PhotoDNA for Video is being used to fight online child exploitation', *Microsoft,* 12 September [online]. Available at: https://news.microsoft.com/on-the-issues/2018/09/12/how-photodna-for-video-is-being-used-to-fight-online-child-exploitation/. (Accessed: 4 December 2020).

Lee, HE. Ermakova, T., Ververis, V., and Fabian, B. Detecting child sexual abuse material: A comprehensive survey. Forensic Science International: Digital Investigation 34 (2020) https://doi.org/10.1016/j.fsidi.2020.301022.

Macaulay, T. (2020) 'New AI tool detects child sexual abuse material with '99% precision', *TheNextWeb*, 31 July [online] Available at: https://thenextweb.com/neural/2020/07/31/new-ai-tool-detects-child-sexual-abuse-material-with-99-accuracy/ (Accessed: 4 December 2020).

Microsoft, *PhotoDNA*. [online] Available at: https://www.microsoft.com/en-us/photodna (Accessed: 4 December 2020).

Missing Children Europe, Intergroup Expert Meeting on EU Legislation on the Fight against Child Sex Abuse Online (2020) Available at:

https://www.youtube.com/watch?feature=youtu.be&v=adY_uWfs90E&app=desktop (Accessed 13 December 2020).

Ofcom, Internet users' experience of harm online: summary of survey research. Conducted by Kantar Media. Fieldwork June-July 2018 www.ofcom.org.uk › Internet-harm-research-2018-report.

Ofcom, Internet users' experience of potential online harms: summary of survey research. Fieldwork: January/February 2020 https://www.ofcom.org.uk/__data/assets/pdf_file/0024/196413/concerns-and-experiences-online-harms-2020-chart-pack.pdf.

Rubio, E. (2011) *The "added value" in the EU budgetary debates: one concept, four meanings,* Notre Europe, Paris: Institut Jacques Delors.

Schütze, R. and Tridimas, T., 2017. Oxford Principles of European Union Law Volume 1: The European Union Legal Order. Oxford: Oxford University Press.

Sejnowski, T.J. (2020), The unreasonable effectiveness of deep learning in artificial intelligence, Proceedings of the National Academy of Sciences, 117 (48) 30033-30038.

Stalford, H. and Drywood, E. (2009) 'Coming of Age?: Children's Rights in the European Union', Common Law Market Review, 46, 143-172.

Stoykova, R. The Presumption of Innocence Evidentiary mechanisms in a digital context. *The International Journal of Evidence and Proof* (forthcoming) (accepted for publication).

Sullivan, J. (2020) '*Preventing Unwanted Contacts and Scams in Messenger*', *Messenger*, 21 May [online]. Available at: https://messengernews.fb.com/2020/05/21/preventing-unwanted-contacts-and-scams-in-messenger/ (Accessed: 4 December 2020).

Technology Coalition (2020), *A Plan to Combat Online Child Sexual Abuse*, 10 June [online] Available at: https://www.technologycoalition.org/2020/05/28/a-plan-to-combat-online-child-sexual-abuse/ (Accessed: 4 December 2020).

Thorn, *How Safer's detection technology stops the spread of CSAM*. [online] Available at: https://www.thorn.org/blog/how-safers-detection-technology-stops-the-spread-of-csam/ (Accessed: 4 December 2020).

Thorn, *Perception Benchmarking*. [online] Available at: https://perception.thorn.engineering/en/latest/examples/benchmarking.html (Accessed: 4 December 2020).

UNICEF and GISMA (2016) Notice and Takedown: Company policies and practices to remove online child sexual abuse material. Available at: https://www.gsma.com/publicpolicy/wp-content/uploads/2016/05/UNICEF_GSMA2016_Guidelines_NoticeAndTakeDown_PoliciesAndPractices ToRemoveOnlineChildSexualAbuseMaterial.pdf (Accessed 15 December 2020).

Weatherill, S. (2011). The Limits of Legislative Harmonization Ten Years after Tobacco Advertising: How the Court's Case Law has become a "Drafting Guide". German Law Journal, 12(3), 827-864.

Zuckerberg, M. (2019) *A Privacy-Focused Vision for Social Networking*, 6 March [Facebook]. Available at: https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/ (Accessed: 4 December 2020).

OA-02-21-024-EN-N

On 10 September 2020, the European Commission presented a proposal (COM(2020) 568 final) on the temporary derogation from Articles 5(1) and 6 of the e-Privacy Directive, which protect the confidentiality of communications and traffic data. This proposal is targeted at ensuring the continuation of voluntary practices conducted by providers of 'number-independent interpersonal communications services' for the detection, reporting and removal of child sexual abuse material online after the European Electronic Communications Code has entered into force at the end of December 2020.

The European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) raised concerns over the proposal's potential impact on the human and fundamental rights of the users of those services, and requested that the European Parliamentary Research Service (EPRS) carry out a targeted impact assessment to this end, in the absence of a European Commission impact assessment accompanying this proposal.

The assessment finds that while the EU has the competence to adopt the proposed regulation per Article 5 of the Treaty on European Union, the impact of such practices on human and fundamental rights has not been adequately addressed. It should provide a clear legal basis for these practices, along with effective remedies for users. Some technologies covered by the proposed regulation have a disproportionate impact, and thus require additional safeguards unavailable in the proposal in its current form.

This is a publication of the Ex-ante Impact Assessment Unit
EPRS | European Parliamentary Research Service

PDF ISBN 978-92-846-7691-0 | doi:978-92-846-7691-0 | QA-02-21-024-EN-N