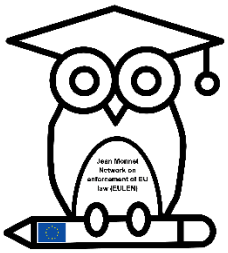

Jean Monnet Network on EU Law Enforcement

Working Paper Series

Conference:

Enforcement of European Union Law: New Horizons,

19-20 September 2024 at King's College London

Effective Enforcement or Excessive Surveillance?

New Technologies, New Crimes, and the Search for a New Equilibrium in EU Law Enforcement Illustrated by the Example of the Combat against Child Sexual Abuse

Charlotte Quaisser*

Abstract

The paper takes the ongoing discussion around the EU's ambition to fight Child Sexual Abuse (CSA) and the proposed Regulation to Prevent and Combat Child Sexual Abuse (COM/2022/209 final [CSAR]) as a cause to reflect on the challenges new technologies and the digitalisation and datafication of society pose for a (criminal) law enforcement. While there is a general consensus that CSA is amongst the most severe crimes and its combat is of paramount importance, the questions remain *what* instruments are legitimate and acceptable to this aim in the age of AI in an area founded in fundamental rights and the rule of law. The paper therefore outlines the new challenges of online CSA and the abilities and limitations of some of the technological counter measures proposed by the contentious CSAR, focusing on the obligation for providers to install and use software to screen all their content for child sexual abuse.

Keywords:

Enforcement, Criminal Law, Criminal Procedure, Artificial Intelligence, AI, Surveillance, CSAM, Chat Control

* Charlotte Quaisser is a Doctoral Researcher at the University of Luxembourg.

I. Introduction

New technologies provide new possibilities for offenders and law enforcement actors alike. Taking the example of child sexual abuse (CSA), on the one hand, digital technologies and online platforms provide new ways for offenders to obtain and disseminate child sexual abuse materials (CSAM) online, and to approach children for sexual abuse purposes in the digital space (so called 'grooming'). On the other hand, such crimes might be countered or even prevented using new automated detection tools such as image hashing or AI based filtering.

To this aim, the European Commission has proposed already in 2022 a Regulation to Prevent and Combat Child Sexual Abuse (COM/2022/209 final [CSAR]). Despite an unanimous consensus, including among the critics[1] of the Proposal, that the safeguard of children is a matter of utmost importance and action is required to effectively combat online child sexual abuse, the solution proposed by the CSAR has been highly contentious since its introduction. On the one side, supporters from child protection organisations and security circles have rallied in favour of the proposed regulations, hailing them as a long-overdue necessity in view of new risks through modern technological means,[2] some of them already calling for their extension to other areas.[3] On the other side, civil rights activists, privacy campaigners, data protection authorities and IT security experts have sharply criticised the proposal as an unbridled form of surveillance with fatal consequences for privacy and other fundamental rights. They have also questioned its practical effectiveness.[4] In particular, the difficult to fulfil obligation to detect new CSAM and grooming, and the impending abolition of end-to-end encryption with its ramifications for internet security are scrutinised.[5]

Continuous efforts by the outgoing Belgian Council Presidency to finally push through the proposed CSAR recently came to a temporary halt when the vote was pulled from the agenda on 21 June 2024.[6] However, the debate is far from over. Further efforts towards an adoption of the Regulation can be expected.[7] The new Hungarian Council Presidency has already taken first steps in this direction and submitted a compromise proposal.[8]

---

[1] Jürgen Bering and Svea Windwehr, 'Digitale Silver Bullets: Grundrechtswidrige Regulierungsvorhaben statt wirksamer Kinder- und Jugendschutz' (*VerfBlog*, 30 August 2024) <https://verfassungsblog.de/chat-kontrolle-effektiver-kinder-und-jugendschutz/> accessed 12 September 2024; Datenschutzkonferenz 'Geplante Chatkontrolle führt zu einer unverhältnismäßigen, anlasslosen Massenüberwachung!' (Press release of the Conference of [German] Independent Federal and State Data Protection Supervisory Authorities of 17 October 2023) <https://www.datenschutzzentrum.de/uploads/dsk/23-10-17_DSK-Pressemitteilung-Chatkontrolle.pdf> accessed 12 September 2024.

[2] Internet Watch Foundation, 'IWF voices support for European CSAM proposal in open letter to European Union' (1 June 2022) <https://www.iwf.org.uk/news-media/news/iwf-voices-support-for-european-csam-proposal-in-open-letter-to-european-union/> accessed 12 September 2024.

[3] Andre Meister, 'Politiker fordern Ausweitung der Chatkontrolle auf andere Inhalte' (*netzpolitik.org*, 6 October 2023) <https://netzpolitik.org/2023/ueberwachung-politiker-fordern-ausweitung-der-chatkontrolle-auf-andere-inhalte/?ref=COM(2023)777&lang=en> accessed 12 September 2024.

[4] EDRi, 'European Commission must uphold privacy, security and free expression by withdrawing new law, say civil society' (8 June 2022) <https://edri.org/our-work/european-commission-must-uphold-privacy-security-and-free-expression-by-withdrawing-new-law/> accessed 12 September 2024; EDPS, 'Opinion 8/2024 on the Proposal for a Regulation amending Regulation (EU) 2021/1232 on a temporary derogation from certain ePrivacy provisions for combating CSAM' (24 January 2024) <https://www.edps.europa.eu/system/files/2024-01/2023-1261_d0219_opinion_en.pdf> accessed 12 September 2024; Datenschutzkonferenz (n 1).

[5] Nena Decoster, 'The policing and reporting of online child sexual abuse material: a scoping review' (2024) 95(2) RIDP, 323 330.

[6] Carl Deconinck, 'EU 'chat-control' plan goes back to drawing board' (*Brussels signal*, 20 June 2024) <https://brusselssignal.eu/2024/06/eu-chat-control-plan-goes-back-to-drawing-board/> accessed 12 September 2024.

[7] Alex Ivanovs, 'EU Council has withdrawn the vote on Chat Control' (*Stackdiary*, 20 June 2024) <https://stackdiary.com/eu-council-has-withdrawn-the-vote-on-chat-control/> accessed 12 September 2024; Felix Reda, Aufgeschoben ist nicht aufgehoben (*VerfBlog*, 26 June 2024) <https://verfassungsblog.de/aufgeschoben-ist-nicht-aufgehoben/> accessed 12 September 2024; Bering and Windwehr (n 1).

[8] Andre Meister, 'Ungarn nimmt neuen Anlauf zur Chatkontrolle', (*netzpolitik.org*, 4 September 2024) <https://netzpolitik.org/2024/staendige-vertreter-ungarn-nimmt-neuen-anlauf-zur-chatkontrolle/> accessed 12 September 2024.

The discussion has relevance beyond the areas of child protection and criminal law. Comparable technological measures for content moderation are also being discussed or are already being used to enforce provisions limiting illegal online content in other areas, such as terrorist content, anti-hate speech measures and the protection of intellectual property (in this context under the label 'upload filter'[9]).

It should be noted that some of the measures covered by the CSAR can already be implemented today on a voluntary basis. Companies such as Gmail and Facebook Messenger make use of an interim Regulation[10] that has recently been extended.[11] Even though, unlike in the CSAR Proposal, the monitoring of user content is not mandatory for providers, the same concern that the measures would amount to a general and indiscriminate monitoring of private communications without effective safeguards apply to the voluntary monitoring. For the question of a fundamental rights violation it is irrelevant whether the services are obligated or only authorised to undertake the measures.[12]

II. New technologies, new crimes, new solutions?

The aim of the CSAR is to prevent the sexual abuse of children via the internet. The proposed Regulation would make online service providers responsible to prevent the use of their hosting and messaging services for the dissemination of child sexual abuse material and the solicitation of children for sexual purposes. CSAM essentially includes any visual image or record of real or simulated sexually explicit activity that involves (apparent) minors pursuant to.[13] To this end, a new 'EU Centre' is to be set up to coordinate the EU's activities in the fight against child abuse and to both monitor and advise service providers in fulfilling their obligations under the Regulation. For their part, the service providers are obliged to carry out preventive 'risk assessments' and 'risk mitigations', and, upon receival of a so called 'detection order' from the competent authorities, inspect the content of their services. They are also subject to reporting duties.[14]

The need to combat online child sexual abuse is justified by the increasing prevalence and severity of the issue, exacerbated by new technologies and the digital environment.[15] New technologies have facilitated the rapid dissemination of child sexual abuse material, perpetuating the harm experienced by victims and providing offenders with new avenues to exploit children. E.g., a 2021 global study[16] revealed that over one-third of respondents had been asked to perform sexually explicit acts online during childhood, and more than half had experienced some form of online child sexual abuse. The pandemic further heightened children's exposure to unwanted online approaches, including solicitation into child sexual abuse. Despite existing laws in the area, the EU has struggled to protect children effectively, particularly in the online sphere.[17]

---

[9] See e.g. Ralf Müller-Terpitz, 'Urheberrechtsreform und Upload-Filter: Eine Gefahr für die Meinungspluralität?: Grundrechtliche Überlegungen zur deutschen Umsetzung von Art. 17' (*VerfBlog*, 2 November 2020, <https://verfassungsblog.de/urheberrechtsreform-und-upload-filter/> accesed 12 September 2024; Reda, Felix*:* 'Walking from Luxembourg to Brussels in two hours' (*VerfBlog*, 16 November 2020) <https://verfassungsblog.de/luxembourg-to-brussels-in-two-hours/> accessed 12 September 2024.

[10] Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse [2021] OJ L274.

[11] Decoster (n 5) 329; European Parliament, 'Child sexual abuse online: current rules extended until April 2026' (10 April 2024) <https://www.europarl.europa.eu/news/en/press-room/20240408IPR20311/child-sexual-abuse-online-current-rules-extended-until-april-2026> accessed 12 September 2024.

[12] Ninon Colneric, 'Legal opinion commissioned by MEP Patrick Breyer, The Greens/EFA Group in the European Parliament' (March 2021) <https://www.patrick-breyer.de/wp-content/uploads/2021/03/Legal-Opinion-Screening-for-child-pornography-2021-03-04.pdf> accessed 12 September; Decoster (n 5) 329; EDPS (n 4).

[13] C.f. Article 2 lit.(l) CSAR in conjunction with Article 2, points (c) and (e), respectively, of Directive 2011/93/EU; Decoster (n 5) 323.

[14] Cf. Chapter 2 CSAR.

[15] CSAR Recital 1 and 2.

[16] Economist Impact, 'Estimates of childhood exposure to online sexual harms and their risk factors: A global study of childhood experiences of 18-20 year olds' (WeProtect Global Alliance) <https://www.weprotect.org/economist-impact-global-survey/#report>accessed 12 September.

[17] CSAR Explanatory Memorandum.

The current approach is not deemed effective because of a lack of communication and standardisation between different stakeholders that currently operate isolated and according to their differing agendas. Since online CSA is not constrained to one geographic area or one organisation, there is a need to harmonise cross-stakeholder collaboration. [18] The cross-border nature of online services makes national regulations insufficient and fragmented.[19] Currently, providers face the burden of complying with diverse national rules, leading to unequal conditions and potential loopholes. Voluntary measures taken by some service providers have proven insufficient, with significant disparities in the quality and quantity of reports to law enforcement authorities.[20]

But where technology offers more opportunities for criminals, it also offers opportunities to fight crime and adapt to the changed profiles of cybercrimes. Automatic detection tools can be used to detect, identify and remove potential CSAM on platforms to prevent redistribution.[21] This is also the approach to which the CSAR Proposal is aimed: At the heart of the proposed Regulation is the introduction of an obligation for providers to proactively detect known and new CSAM and instances of grooming on their platforms upon issuance of a so called 'detection order'.[22] Without going into the mechanism of issuing a detection order in more detail, it should be noted that the circle of addressees and the requirements for a detection order are so broad that they ultimately aim at all services that enable the exchange of messages, images or videos may be affected, as they generally have a significant risk of being used for the exchange of child pornography content.[23] This applies regardless of the actual extent of online CSA on the service.[24]

Once a detection order has been issued, the providers are obliged to report any information indicating potential online CSA on its services (Articles 12 and 13). Article 10(3) sets out the relevant technological requirements: The technologies must reliably recognise known and new CSAM, and grooming, while keeping the error rate low. At the same time, they should not be able to extract any information other than what is absolutely necessary and interfere as little as possible with the fundamental rights of users in accordance with the state of the art in the industry. Although the draft claims to be technology-neutral, these requirements along with the sheer volume of content that must be supervised, means that this can only be achieved by means of a comprehensive and indiscriminate automated screening of all content, including private communications.[25] To provide support to the providers for the implementation of obligations imposed, access to reliable sets of indicators of online CSA that in turn provide means to use reliable automated detection technologies, and to free-of-charge automated detection technologies, is assured.[26] The EU Centre is to provide these indicators that should allow technologies to detect the dissemination of either the same material (known material) or of different child sexual abuse material (new material), or the solicitation of children, as applicable.[27]

III. The technological implementation

To realise the aforementioned requirements set out by Article 10(3) CSAR, the following technological aspects in particular are being discussed according to the current state of the art:

[18] Decoster (n 5) 359.
[19] CSAR Recital 3.
[20] CSAR Explanatory Memorandum.
[21] Decoster (n 5) 324.
[22] Article 10 CSAR.
[23] Cf. Article 7(4) lit.(a) CSAR.
[24] CSAR Recitals 20 and 21.
[25] Paul Zurawski 'EU-Kommission: Vorschlag „Chatkontrolle" – Verhältnisse der Überwachung' (2022) ZD-Aktuell 01240.
[26] CSAR Explanatory Memorandum.
[27] Article 44 CSAR; Recital 61.

(1) *Image Hashing*

One of the technologies most commonly used to automatically detect CSAM is the so called hashing system. A hash value is often compared to a digital fingerprint. It is calculated from a file though an algorithm and can be used to identify it. It is however not possible to in return reconstruct the underlying file from the hash value. A hash-based detection mechanism compares the hash values of the files present on the hosting service with the hash values of known CSAM that are stored into databases. This allows for the rapid scanning of large volumes of data and for the quick removal of detected CSAM.[28]

In the perceptual hashing variant, the technology is also robust against minor changes such as rescaling and colour changes. In this case, the hash value is not calculated from the entire file, but from certain structural properties of the image material it contains. However, this increase in robustness also means that the technology is more susceptible to false positives.[29]

The scope of application of hash-based removal is however limited to already known CSAM. A hash value-based detection approach cannot be used to detect new, as yet unknown CSAM, as there is no possibility of matching them.

(2) *AI-based filtering*

Self-learning algorithms are another detection method. The algorithms identify patterns in training data and apply them to the content available on the hosting service. In contrast to image hashing, this allows them to detect also new CSAM, as well as grooming patterns. The strategies used by perpetrators to manipulate minors for abuse and to guarantee subsequent secrecy are not identical but often show parallels that can be used to their detection and thus the prevention of abuse.[30]

Such algorithms are much more flexible and robust against modifications than hash-based tools. With this method, however, a much higher number of false positive classifications is to be expected compared to hashing. This number might be reduced by refining the analysis technique, but is unlikely to be eliminated. The categorisation of content as CSAM may depend on the context in which it was produced and disseminated. Complex considerations may be necessary to evaluate, for example, whether content is to be categorised as a work of art.[31]

Estimations on the accuracy that can be achieved by machine learning based algorithms vary.[32] The accuracy indicates the proportion of correct classifications in the total number of classification processes. The accuracy of a classification model indicates the ratio of correct classifications in relation to the total number of classification processes. In the process of designing the algorithms, it is typically necessary to adjust it either for high precision[33] or for high recall[34] rate. For example, if a detection system is set to recognise as many CSAM as possible (high recall), it will typically classify more harmless materials as false positives (low precision). For grooming in

[28] Decoster (n 5) 343 f.
[29] Harold Abelson et al, 'Bugs in our Pockets: The Risks of Client-Side Scanning' [2024] 10(1) Journal of Cybersecurity; Matthias Bäcker and Ulf Buermeyer, 'Mein Spion ist immer bei mir: Anmerkungen zu der geplanten Inpflichtnahme von Internet-Diensteanbietern zur Bekämpfung sexualisierter Gewalt gegen Kinder („Chatkontrolle")' (*VerfBlog*, 11 August 2022), <https://verfassungsblog.de/spion-bei-mir/> accessed 12 September.
[30] On the varying mechanisms of cybergrooming of children see Maria Gahn, 'Abuse process including (cyber) grooming and online sexual solicitation' [2024] 95(2) RIDP 299.
[31] Bäcker and Buermeyer (n 29).
[32] EDPB-EDPS, 'Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse' (28 July 2022) <https://www.edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202204_csam_en_0.pdf> accessed 12 September, no 60 ff; Laura Kabelka, 'EU assessment of child abuse detection tools based on industry data' (*Euraktiv*, 5 October 2022) <https://www.euractiv.com/section/digital/news/eu-assessment-of-child-abuse-detection-tools-based-on-industry-data/> accessed 12 September.
[33] *Precision* is the ratio of correctly positive classifications to all positive classifications. A higher precision means that fewer innocuous images or conversation are wrongly labelled as CSAM or grooming (lower number of false positives).
[34] *Sensitivity* or *recall* indicates the proportion of correctly positive classifications among the actual positives. A higher sensitivity means that fewer cases of CSAM or grooming go undetected (lower number of false negatives).

particular, it is assumed that the deployment of AI based tools might lead to a high number of false positive classifications due to the complex assessment of the content and context of the communication that it requires.[35]

(3) '*Chat-Control*'

One particularly controversial aspect of the Proposal is the extension of the detection obligation to *interpersonal communications services* which became known under the term *chat control*[36]. From a technical perspective, centralised, decentralised or hybrid solutions are possible.

With a centralised solution, the detection system is comparatively secure against unauthorised attacks. However, centralised scanning on the service provider's server is not possible if the communication is *end-to-end encrypted*. Here, the service provider does not have access to the content of the interpersonal communication.[37] End-to-end-encryption is a widespread industry standard to ensure the security of communications.[38]

A supposedly secure alternative is put forward in the form of *client-side scannin*g. This means that all or part of the detection takes place on the user's own devices before the content is encrypted.[39] However, the feasibility of this is questioned given the hardware performance and storage required on the end device.[40] In addition, client-side scanning equally weakens encryption. Since most user devices have vulnerabilities, the monitoring and control capabilities of the client-side scanning technology can be abused by adversaries. And the opacity of mobile operating systems makes it difficult to verify that the measures only target undisputedly illegal material. Content can be sent either encrypted and private or not, including on the user's own device.[41] The fact that the proposal would undermine encryption was first publicly acknowledged by the EU Commission on 20 June 2024, after having long claimed that it would be able maintained encryption by using a decentralised technology.[42]

(4) Age Verification

Another approach is aimed at age verification. It could for example be used to determine whether the persons depicted in an image are minors. As part of grooming detection, it could be used to identify whether the people contacted are children.

A rough distinction can be made between two different approaches: Age verification through data matching on the one hand and (AI-based) age estimation based on biometric data or insights into user behaviour on the other. The first involves identification via (electronic) identity documents. This method poses risks for the security and misuse of the data queried and collected in this way, especially as such identity checks are regularly outsourced to external service providers. In addition, anonymity on the internet would be abolished.[43]

When analysing biometric data, especially sensitive data is affected. Another challenge with AI-based approaches in this constellation is that it is often unclear exactly how the model arrived at its assessment. This is particularly problematic if misjudgements are made on the basis of such technologies and particularly young-looking adults or people with unusual user behaviour are excluded from accessing certain apps or websites.[44]

---

[35] Bäcker and Buermeyer (n 29).
[36] Or, rebranded in the course of the Belgian efforts to push through the draft, as 'uplodad moderation', see Ivanovs (n 7).
[37] Bäcker and Buermeyer (n 29).
[38] Datenschutzzentrum (n 1).
[39] Bering and Windwehr (n 1).
[40] Bäcker and Buermeyer (n 29).
[41] Abelson et al (n 29); Markus Reuter, 'Berühmte IT-Sicherheitsforscher:innen warnen vor Wanzen in unserer Hosentasche' (*netzpolitik.org*, 16 October 2021) <https://netzpolitik.org/2021/client-side-scanning-beruehmte-it-sicherheitsforscherinnen-warnen-vor-wanzen-in-unserer-hosentasche/> accessed 12 September.
[42] Ivanovs (n 7).
[43] Bering and Windwehr (n 1).
[44] Bering and Windwehr (n 1).

Currently, age verification-based access restrictions to digital platforms and services are also increasingly being discussed as an alternative approach to minimise specific risks for children online.[45]

IV. Assessment: Effectivity and Proportionality

Due to the technical limitations just described, there are doubts about the technological feasibility of some of the requirements that the proposal imposes on providers. As discussed above, these relate in particular to the reliable detection of new materials and behaviour that can be classified as grooming. Due to the vast amount of data being searched, even a small percentage of false positives results in a high number of false suspicions. As detection is linked to a reporting obligation, there is a risk of intrusive law enforcement action that will infringe on fundamental rights and bind law enforcement resources.[46] Even correctly classified, the sheer number of automated reports threatens to flood authorities and have the opposite of the desired effect, while non-digital CSA issues lose visibility.[47] In fact, these resources are already so strained that even known abusive images are not always systematically removed.[48]

On the other hand, false negatives can lead to a false sense of security and systematic overlooking of online CSA, assuming that classification errors are likely not independent of each other. There is also the likelihood that tech-savvy offenders will not use a system that can detect online CSA. In this respect, there is a risk of displacement effects towards networks that are not compliant with the obligations.

At the same time, the extension of the detection requirements to encrypted services threatens the *de facto* abolition of these secure communication channels. The German *Bundesamt für Sicherheit in der Informationstechnik* (Federal Office for Information Security) recommends that private internet users use end-to-end encryption to ensure the confidentiality, authenticity and integrity of transmitted data.[49] This is the only way to ensure that the messages or data can be recognised solely by the person for whom they are intended. The identity of the sender is verified and the message cannot be altered unnoticed by third parties. There is a risk that providers would offer fewer encrypted services in order to better comply with the obligations, thus weakening the role of encryption in general and undermining the respect for fundamental rights and the trust in digital services.[50] The European Court of Human Rights recently ruled in *Podchasov v. Russia*[51] that end-to-end encryption is a fundamental right and that it is unlawful to undermine this protection preventively.[52] At the same time, some commentators have suggested that encrypted communications play little role in the distribution of CSAM or grooming of children.[53]

---

[45] See e.g. Aleesha Rodriguez, 'Australia's dummy spit over kids on social media isn't the answer. We need an internet for children' (*The Guardian*, 10 September 2024) <https://www.theguardian.com/commentisfree/article/2024/sep/10/australias-dummy-spit-over-kids-on-social-media-isnt-the-answer-we-need-an-internet-for-children> accessed 12 September; Oceane Duboust, 'Macron in favour of Europe-wide social media age restriction for teens under 15' (*Euronews*, 27 April 2024) <https://www.euronews.com/next/2024/04/27/macron-in-favour-of-europe-wide-social-media-age-restriction-for-teens-under-15> accessed 12 September.

[46] Bäcker and Buermeyer (n 29); Chris Köver, 'Zahl der falschen Verdächtigungen stark gestiegen' (*netzpolitik.org* 18 June 2024) <https://netzpolitik.org/2024/chatkontrolle-zahl-der-falschen-verdaechtigungen-stark-gestiegen/> accessed 12 September.

[47] Zurawski (n 25).

[48] Erik Tuchtfeld, '"Vielen Dank, Ihre Post ist unbedenklich": Wie die Europäische Kommission das digitale Briefgeheimnis abschaffen möchte' (*VerfBlog*, 25 May 2022) <https://verfassungsblog.de/vielen-dank-ihre-post-ist-unbedenklich/> accessed 12 September 2024; Robert Bongen, 'Pädokriminelle Bilder im Netz: EU-Abgeordnete fordern Aufklärung' (*Tagesschau*, 28 January 2022) <https://www.tagesschau.de/investigativ/panorama/missbrauch-kinder-bilder-bka-europol-101.html> accessed 12 September 2024.

[49] Bundesamt für Sicherheit in der Informationstechnik, 'Verschlüsselt kommunizieren im Internet' (*Bundesamt für Sicherheit in der Informationstechnik*) <https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesselt-kommunizieren/verschluesselt-kommunizieren_node.html#doc504778bodyText1> accessed 12 September.

[50] EPDP, 'Statement 1/2024 on legislative developments regarding the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse' (13 February 2024) <https://www.edpb.europa.eu/system/files/2024-02/edpb_statement_202401_proposal_regulation_prevent_combat_child_sexual_abuse_en.pdf> accessed 12 September.

[51] Podchasov v Russia, App no 33696/19 (ECtHR, 13 February 2024).

[52] Bering and Windwehr (n 1).

[53] Dpa, 'Kinderschutzbund gegen anlasslose Scans verschlüsselter Nachrichten' (*EU-Info.Deutschland*, 8 May 2022) <https://www.eu-info.de/dpa-europaticker/316232.html> accessed 12 September; Carla Siepmann, 'Jugendschutz bedeutet

However, even hashing-based detection of non-encrypted content, which is sometimes regarded as minimally invasive, [54] represents a paradigm shift in the fight against crime: All the above mentioned detection methods amount to a preventive general and indiscriminate surveillance without any initial suspicion of a crime. This undermines one of the traditional limits of law enforcement measures.[55] Further protection mechanisms are circumvented by the fact that the surveillance is carried out by private actors. Government surveillance measures are subject to strict control and enforcement requirements that do not apply to companies. It is also easier for users to take legal action against government measures. As soon as private individuals are given a free licence for surveillance, many of these safeguards no longer apply or only apply to a limited extent. For example, no court decides when content is scanned, as is usually the case with state surveillance measures.[56] This is illustrated by the case of a German user challenging the monitoring of personal chats by 'F-Messenger' on the basis of the provisional regulation, in which the *Landgericht Kiel* held that the Irish courts have international jurisdiction.[57]

It is questionable whether such far reaching measures are proportionate, especially in view of the interpersonal communication covered. The interference with Article 7 (Respect for private and family life) and Article 8 (Protection of personal data) of the Charter of Fundamental Rights[58] is substantial, it goes 'far beyond any interference that has so far been considered by the CJEU',[59] including in its recent *La Quadrature du Net II*[60] decision. Previous decisions only concerned metadata. With chat control, there is now access to the actual communication content. The fact that further processing only takes place in the event of a hit does not change the preceding general and indiscriminate interference if all communications are included in the screening.[61] Whether this can be considered 'strictly necessary and proportionate' is doubtful.

In addition to the effects on the privacy and security of communication, indirect effects on numerous other fundamental rights are to be expected. The more reliance is placed on automated tools, the greater the risk of excessive censorship. Increased filtering and monitoring of content in advance can lead to an undesirable restriction of users' fundamental freedoms and rights.[62] There is a threat of self-censorship and 'chilling effects', the restraint of (legal) statements or actions for fear of them being recognised by the state or third parties. This could have a major impact on freedom of expression and freedom of the media (especially for confidential source work).[63] The loss of privacy and autonomy therefore also harbours risks for the foundations of democracy.[64] There is a risk that social media platforms will make decisions with significant consequences for individuals and democracy without proper accountability.[65]

In view of the fact that the aim of the Proposal is to protect children, it should be noted that this also affects the of children who are active online. Their fundamental rights to informational self-determination, privacy and autonomy are equally restricted. Mass intrusion into the privacy of communication endangers the healthy

Datenschutz' (*netzpolitik.org*, 25 May 2022) <https://netzpolitik.org/2022/schuelerin-ueber-chatkontrolle-jugendschutz-bedeutet-datenschutz/> accessed 12 September.

[54] Decoster (n 5) 347.

[55] Christoph Burchard, '(Was bleibt vom) Strafrecht in der Big Data-Überwachungsgesellschaft?' (2023) 135(4) ZStW 793, 815 ff.

[56] Bering and Windwehr (n 1).

[57] LG Kiel, Urteil vom 4.4.2024 – 13 O.

[58] Charter of Fundamental Rights of the European Union [2012] OJ C 326.

[59] Christopher Vajda, 'Legal opinion commissioned by MEP Patrick Breyer, member of the Greens/EFA Group in the European Parliament' (19 October 2023) <https://www.patrick-breyer.de/wp-content/uploads/2023/11/Vajda-Legal-Opinion-ChatControl-CSAR-2023-11-19.pdf> accessed 12 September, no 71.

[60] Case C-470/21 *La Quadrature du Net II* (30 April 2024).

[61] BVerfG, Order of the First Senate of 18 December 2018 - 1 BvR 142/15 – (*Automatic number plate recognition II*).

[62] Costica Dumbrava, 'Die Hauptrisiken sozialer Medien für die Demokratie Risiken durch Überwachung, Personalisierung, Desinformation, Moderation und Mikrotargeting' (*EPRS*, December 2021) <https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698845/EPRS_IDA(2021)698845_DE.pdf> accessed 12 September 2024, 24.

[63] Zurawski (n 25).

[64] Dumbrava (n 62).

[65] Dumbrava (n 62) 34 f.

development and communication behaviour of children, whose privacy and protected spaces are being invaded.[66] There is a serious risk that, of all people, children will be targeted by law enforcement agencies by the very rules designed to protect them. The automatic detection could for example make consensual 'sexting' between minors a trigger for criminal investigations.[67] Protecting children and young people also means ensuring that they have the privacy they need to feel safe and secure. In this respect, there is already a tension within the protected interest, which makes the interference even more difficult to justify.[68]

V. Alternative approaches to combat online CSA

There are alternative approaches to combating child abuse using new automated technologies. E.g. automated search of seized data carriers could make criminal investigations more effective and make them possible in the first place in cases with large amounts of data that can no longer be handled by humans.[69] CSAM detection tools can supplement the manual evaluation of (potential) evidence, which is resource-intensive and particularly psychologically stressful for law enforcement officers in child sexual abuse cases. The use of an algorithm can even have privacy enhancing effects due to possibility to limit the scope of the search in advance. The limitations of accuracy are also less important here. A relatively high number of false positive classifications is not detrimental. It is beneficial in a criminal investigation to show the investigators rather more legal images than miss CSAM. The algorithm can be optimised accordingly in favour of a high recall rate. However, the results always require human review. Random checks must also be carried out on misclassified negatives.[70]

Another important factor is prevention through education of children and their parents. They need to be taught media skills and age-appropriate guidance should be provided for children online. Children need to be aware of the consequences of disclosing information, sharing pictures and videos, and even more so of the possibility of meeting strangers. Children need to understand as early as possible what actions of others platform users are not appropriate and be empowered to set boundaries. They must have the opportunity to report illegal content to contact points within the network and directly to the competent authorities, and to seek help from parents or other trusted persons. In this regard, it is crucial for parents to signal to their children that it is always better to speak up, even if the children themselves are behaving inappropriately.[71]

Services and applications used by children should be designed in such a way that they can navigate the digital world safely. It must be avoided that children are too easily contacted by a perpetrator and, above all, isolated. Many social networks offer the possibility to exclude contact with strangers, to limit the visibility of content or to create accounts that allow for parental supervision. Less content in children's profiles and disclosures about their age and preferences can limit their selection as victims.[72]

In addition, traditional prevention approaches are also suitable for combating online CSA, such as general prevention via programmes aimed at non-offenders who feel attracted to children.[73]

VI. Conclusions: No effective enforcement, but excessive surveillance

There is no question that children need to be protected from sexual abuse. However, the means envisaged in the proposed CSAR are extremely questionable. In particular, the extension of surveillance obligations to interpersonal communications constitutes a serious interference with fundamental rights. If this includes the undermining of end-to-end encryption, then there are additional serious security concerns. In this regard, there seems to be

[66] Siepmann (n 53).
[67] Dpa (n 53); Dominik Brodowski, Markus Hartmann and Christoph Sorge, 'Automatisierung in der Strafrechtspflege' (2023) NJW 587.
[68] Zurawski (n 25).
[69] Dpa (n 53); Dominik Brodowski, 'Durchsuchung, Durchsicht und Beschlagnahme bei informationstechnischen Systemen' (2024) 79 JZ 750, 754.
[70] Brodowski (n 69) 754.
[71] Gahn (n 30) 315 f.; Bering and Windwehr (n 1).
[72] Gahn (n 30) 309 ff.; Bering and Windwehr (n 1).
[73] Gahn (n 30) 309.

increasing resistance from providers of software particularly,[74] who have an interest in ensuring the user has confidence in the safety and reliability of their products. Beyond the fundamental rights impact, there are already doubts about the feasibility and effectiveness of the measures.

A legal opinion also comes to the conclusion that the provisions laying down the monitoring obligation are 'likely to be unlawful on grounds of proportionality, lack of reasoning, legal certainty as well as the requirement that such interferences should be provided by the law'.[75] The Proposal 'enables the content of communications to be monitored which will inevitably enable precise conclusions to be drawn about a person's private life'.[76] This also applies to the current legal situation under the interim Regulation, according to which providers are permitted but not obliged to implement the aforementioned surveillance measures voluntarily.[77] As regards the disproportionate nature of the infringement of user's fundamental rights, there is no difference, regardless of whether the private companies that ultimately carry out the surveillance are obliged or merely authorised to do so. The interference lies in granting the permission.[78]

The increasing importance of private individuals for law enforcement in this context harbours its own pitfalls. There are fundamental concerns when, as is the case here, private individuals increasingly fulfil functions that originally belong to the state's monopoly on law enforcement. The private service providers, through their automated content surveillance, take over tasks that were traditionally the responsibility of public authorities. This allows law enforcement authorities to profit from the masses of data that are generated by private companies for their own economic interests. This surveillance in public-private cooperation not only reaches an unprecedented scale, but also takes on a new quality that threatens to undermine the fundamental principles of criminal procedure and could lead to an erosion of the safeguards that limit the powers of the state in criminal proceedings. This includes, but is not limited to, the circumvention of the requirements for criminal investigation measures or the elimination of legal remedies.

[74] Ivanovs (n 7); See e.g. Meredith Whittacker, 'New Branding, Same Scanning: "Upload Moderation" Undermines End-to-End Encryption' (17 June 2024) <https://signal.org/blog/pdfs/upload-moderation.pdf> accessed 12 September.
[75] Vajda (n 59) 2.
[76] Vajda (n 59) 2.
[77] Colneric (n 12) 33 f.
[78] Colneric (n 12) 33 f.

VII. Bibliography

1. Legislation

Charter of Fundamental Rights of the European Union [2012] OJ C 326

Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse [2021] OJ L274

2. Case law

Case C 470/21 La Quadrature du Net II (30 April 2024)

Podchasov v Russia, App no 33696/19 (ECtHR, 13 February 2024)

BVerfG, Order of the First Senate of 18 December 2018 - 1 BvR 142/15 – (Automatic number plate recognition II).

LG Kiel, Urteil vom 4.4.2024 – 13 O 40/23

3. Literature

Abelson H, Anderson R, Bellovin SM, Benaloh J, Blaze M, Callas J, Diffie W, Landau S, Neumann PG, Rivest RL, Schiller JI, Schneier B, Teague V, Troncoso C, 'Bugs in our Pockets: The Risks of Client-Side Scanning' [2024] 10(1) Journal of Cybersecurity 1

Bäcker M and Buermeyer U, 'Mein Spion ist immer bei mir: Anmerkungen zu der geplanten Inpflichtnahme von Internet-Diensteanbietern zur Bekämpfung sexualisierter Gewalt gegen Kinder („Chatkontrolle")' (*VerfBlog*, 11 August 2022), <https://verfassungsblog.de/spion-bei-mir/> accessed 12 September

Bering J and Windwehr S, 'Digitale Silver Bullets: Grundrechtswidrige Regulierungsvorhaben statt wirksamer Kinder- und Jugendschutz' (*VerfBlog*, 30 August 2024) <https://verfassungsblog.de/chat-kontrolle-effektiver-kinder-und-jugendschutz/> accessed 12 September 2024

Brodowski D, 'Durchsuchung, Durchsicht und Beschlagnahme bei informationstechnischen Systemen' (2024) 79 JZ 750

Brodowski D, Markus Hartmann and Christoph Sorge, 'Automatisierung in der Strafrechtspflege' (2023) NJW 587

Burchard C, '(Was bleibt vom) Strafrecht in der Big Data-Überwachungsgesellschaft?' (2023) 135(4) ZStW 793

Decoster N, 'The policing and reporting of online child sexual abuse material: a scoping review' (2024) 95(2) RIDP 323

Gahn M, 'Abuse process including (cyber) grooming and online sexual solicitation' (2024) 95(2) RIDP 299

Müller-Terpitz R, 'Urheberrechtsreform und Upload-Filter: Eine Gefahr für die Meinungspluralität?: Grundrechtliche Überlegungen zur deutschen Umsetzung von Art. 17' (*VerfBlog*, 2 November 2020, <https://verfassungsblog.de/urheberrechtsreform-und-upload-filter/> accesed 12 September 2024

Reda F, 'Aufgeschoben ist nicht aufgehoben' (*VerfBlog*, 26 June 2024) <https://verfassungsblog.de/aufgeschoben-ist-nicht-aufgehoben/> accessed 12 September 2024

Reda F, 'Walking from Luxembourg to Brussels in two hours' (VerfBlog, 16 November 2020) <https://verfassungsblog.de/luxembourg-to-brussels-in-two-hours/> accessed 12 September 2024

Zurawski P 'EU-Kommission: Vorschlag „Chatkontrolle" – Verhältnisse der Überwachung' (2022) ZD-Aktuell 01240

4. Other Sources

Bongen R, 'Pädokriminelle Bilder im Netz: EU-Abgeordnete fordern Aufklärung' (*Tagesschau*, 28 January 2022) <https://www.tagesschau.de/investigativ/panorama/missbrauch-kinder-bilder-bka-europol-101.html> accessed 12 September 2024

Bundesamt für Sicherheit in der Informationstechnik, 'Verschlüsselt kommunizieren im Internet' (*Bundesamt für Sicherheit in der Informationstechnik*) <https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesselt-kommunizieren/verschluesselt-kommunizieren_node.html#doc504778bodyText1> accessed 12 September.

Colneric N, 'Legal opinion commissioned by MEP Patrick Breyer, The Greens/EFA Group in the European Parliament' (March 2021) < https://www.patrick-breyer.de/wp-content/uploads/2021/03/Legal-Opinion-Screening-for-child-pornography-2021-03-04.pdf> accessed 12 September

Datenschutzkonferenz 'Geplante Chatkontrolle führt zu einer unverhältnismäßigen, anlasslosen Massenüberwachung!' (Press release of the Conference of [German] Independent Federal and State Data Protection Supervisory Authorities of 17 October 2023) <https://www.datenschutzzentrum.de/uploads/dsk/23-10-17_DSK-Pressemitteilung-Chatkontrolle.pdf> accessed 12 September 2024

Deconinck C, 'EU 'chat-control' plan goes back to drawing board' (*Brussels signal*, 20 June 2024) <https://brusselssignal.eu/2024/06/eu-chat-control-plan-goes-back-to-drawing-board/> accessed 12 September 2024

Dpa, Kinderschutzbund gegen anlasslose Scans verschlüsselter Nachrichten (*EU-Info.Deutschland*, 8 May 2022) <https://www.eu-info.de/dpa-europaticker/316232.html> accessed 12 September

Duboust O, 'Macron in favour of Europe-wide social media age restriction for teens under 15' (*Euronews*, 27 April 2024) <https://www.euronews.com/next/2024/04/27/macron-in-favour-of-europe-wide-social-media-age-restriction-for-teens-under-15> accessed 12 September.

Dumbrava C, 'Die Hauptrisiken sozialer Medien für die Demokratie Risiken durch Überwachung, Personalisierung, Desinformation, Moderation und Mikrotargeting' (*EPRS*, December 2021) <https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698845/EPRS_IDA(2021)698845_DE.pdf> accessed 12 September 2024

Economist Impact, 'Estimates of childhood exposure to online sexual harms and their risk factors: A global study of childhood experiences of 18-20 year olds' (*WeProtect Global Alliance*) <https://www.weprotect.org/economist-impact-global-survey/#report> accessed 12 September

EDPB-EDPS, 'Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse' (28 July 2022) <https://www.edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202204_csam_en_0.pdf> accessed 12 September

EDPS, 'Opinion 8/2024 on the Proposal for a Regulation amending Regulation (EU) 2021/1232 on a temporary derogation from certain ePrivacy provisions for combating CSAM' (24 January 2024)

<https://www.edps.europa.eu/system/files/2024-01/2023-1261_d0219_opinion_en.pdf> accessed 12 September 2024

EDRi, 'European Commission must uphold privacy, security and free expression by withdrawing new law, say civil society' (8 June 2022) <https://edri.org/our-work/european-commission-must-uphold-privacy-security-and-free-expression-by-withdrawing-new-law/> accessed 12 September 2024

EPDP, 'Statement 1/2024 on legislative developments regarding the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse' (13 February 2024) <https://www.edpb.europa.eu/system/files/2024-02/edpb_statement_202401_proposal_regulation_prevent_combat_child_sexual_abuse_en.pdf> accessed 12 September.

European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse' (*COM(2022) 209 final - 2022/0155(COD)* 11 May 2022)

European Parliament, 'Child sexual abuse online: current rules extended until April 2026' (10 April 2024) <https://www.europarl.europa.eu/news/en/press-room/20240408IPR20311/child-sexual-abuse-online-current-rules-extended-until-april-2026> accessed 12 September 2024

Internet Watch Foundation, 'IWF voices support for European CSAM proposal in open letter to European Union' (1 June 2022) <https://www.iwf.org.uk/news-media/news/iwf-voices-support-for-european-csam-proposal-in-open-letter-to-european-union/ accessed> 12 September 2024

Ivanovs A, 'EU Council has withdrawn the vote on Chat Control' (*Stackdiary,* 20 June 2024) <https://stackdiary.com/eu-council-has-withdrawn-the-vote-on-chat-control/> accessed 12 September 2024

Kabelka L, 'EU assessment of child abuse detection tools based on industry data' (Euraktiv, 5 October 2022) <https://www.euractiv.com/section/digital/news/eu-assessment-of-child-abuse-detection-tools-based-on-industry-data/> accessed 12 September.

Köver C, 'Zahl der falschen Verdächtigungen stark gestiegen' (*netzpolitik.org* 18 June 2024) <https://netzpolitik.org/2024/chatkontrolle-zahl-der-falschen-verdaechtigungen-stark-gestiegen/> accessed 12 September

Meister A, 'Politiker fordern Ausweitung der Chatkontrolle auf andere Inhalte' (*netzpolitik.org,* 6 October 2023) <https://netzpolitik.org/2023/ueberwachung-politiker-fordern-ausweitung-der-chatkontrolle-auf-andere-inhalte/?ref=COM(2023)777&lang=en> accessed 12 September 2024

Meister A, 'Ungarn nimmt neuen Anlauf zur Chatkontrolle', (*netzpolitik.org,* 4 September 2024) <https://netzpolitik.org/2024/staendige-vertreter-ungarn-nimmt-neuen-anlauf-zur-chatkontrolle/> accessed 12 September 2024.

Reuter M, 'Berühmte IT-Sicherheitsforscher:innen warnen vor Wanzen in unserer Hosentasche' (*netzpolitik.org,* 16 October 2021) <https://netzpolitik.org/2021/client-side-scanning-beruehmte-it-sicherheitsforscherinnen-warnen-vor-wanzen-in-unserer-hosentasche/> accessed 12 September

Rodriguez A, 'Australia's dummy spit over kids on social media isn't the answer. We need an internet for children' (*The Guardian*, 10 September 2024) <https://www.theguardian.com/commentisfree/article/2024/sep/10/australias-dummy-spit-over-kids-on-social-media-isnt-the-answer-we-need-an-internet-for-children> accessed 12 September

Siepmann C, 'Jugendschutz bedeutet Datenschutz' (*netzpolitik.org,* 25 May 2022) <https://netzpolitik.org/2022/schuelerin-ueber-chatkontrolle-jugendschutz-bedeutet-datenschutz/> accessed 12 September.

Vajda C, 'Legal opinion commissioned by MEP Patrick Breyer, member of the Greens/EFA Group in the European Parliament' (19 October 2023) <https://www.patrick-breyer.de/wp-content/uploads/2023/11/Vajda-Legal-Opinion-ChatControl-CSAR-2023-11-19.pdf> accessed 12 September