EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of European Lawyers

Rue Joseph II, 40/8 - B-1000 Brussels
+32 (0)2 234 65 10 | ccbe@ccbe.eu | www.ccbe.eu

CCBE position on the proposal for a regulation laying down rules to prevent and combat child sexual abuse

25/11/2022

Introduction and executive summary

On 11 May 2022, the European Commission presented a proposal for a regulation laying down rules to prevent and combat child sexual abuse[1]. The proposal provides for obligations on providers of hosting services, interpersonal communication services, software application stores, internet access services, and other relevant services regarding the detection, reporting, removal, and blocking of known and new online child sexual abuse material ("CSAM"), as well as the solicitation of children (called "grooming").

The CCBE considers that child sexual abuses are particular serious and heinous crimes and fully support the objectives to combat such crime and the adoption of specific measures to prevent and fight it; however, the CCBE has serious concerns, shared by the European Data Protection Board ("EDPB") and the European Data Protection Supervisor ("EDPS")[2], over the threats posed by the proposal on the right to privacy, the protection of professional secrecy and legal professional privilege ("PS/LPP").

In particular, the CCBE concludes that:

- **The necessary safeguards to ensure the protection of fundamental rights, including the confidentiality of communications, have been discarded in the proposal. The very essence of the right to confidentiality is undermined by the proposal which lacks legal clarity, as a legal basis to the detection obligation, and proportionality regarding the interferences and limitations to fundamental rights.**
- **The procedural safeguards and the complexity of the process leading to the adoption of a detection order cannot replace substantive safeguards to ensure the confidentiality of communications and the protection of PS/LPP.**
- **The EU legislator have to adopt clear legal provisions and safeguards to ensure that fundamental rights of all citizens are properly ensured and well balanced. In this regard, the CCBE is strongly opposed to the approach where the protection of fundamental rights is partly or fully delegated to private parties.**
- **The proposed measures enabling the detection and identification of contents by service providers should be removed from the proposal, in the absence of clear legal provisions and proper safeguards to ensure that the fundamental rights of individuals are respected and well balanced.**
- **The proposal should not prevent lawyers from adequately protecting the confidentiality of their communications through encryption methods. The EU legislator should provide for the protection of "end to end encryption" ("E2EE") and ensure that the provisions of the proposal could not weaken E2EE in any way.**

[1] COM(2022) 2096 final

[2] EDPB-EDPS Joint Opinion 4/2022 on the proposal for a regulation of the European Parliament an of the Council laying down rules to prevent and combat child sexual abuse, 28 July 2022, page 5

- **The proposal should specify and limit the circumstances and purposes under which the EU Centre may forward reports to Europol. Any transfer of personal data to Europol should be adequate, relevant and limited to what is strictly necessary, while ensuring data quality and reliability. Moreover, the exchange of personal data between the EU Centre and Europol should only take place on a case-by-case basis, following an explicit and duly assessed request.**

I. Detection obligation

The CCBE notes that article 7 to 10 of the proposed regulation provide for an obligation for providers of hosting and interpersonal communication services to detect CSAM and grooming communication when a judicial or an independent administrative authority has issued a detection order under the conditions laid down in articles 7 and 8. In this regard, providers should use technologies to detect dissemination of CSAM or grooming communication under the conditions specified in article 10.

A. The necessity to guarantee PS/LPP

1. A specific protection

The CCBE recalls that for lawyers to be effective in defending their clients' rights, there must be confidence that communications between them are kept confidential. Most legal systems share a common understanding that if the right of the citizen to safeguard confidentiality, i.e. the right of the citizen to be protected against any divulging of his/her communication with his/her lawyer, were to be denied, people may be denied access to legal advice and to justice. PS/LPP are thus seen as instruments by which access to justice and the maintenance of the rule of law can be achieved.

The European Court of Human Rights ("ECtHR") has repeatedly linked the respect for PS/LPP to the observance of **Articles 6 and 8 of the European Convention on Human Rights** ("ECHR"), stating that "*the right of everyone to a fair trial*"[3] *is dependent upon the "relationship of trust between [the lawyer and the client]*" and repeatedly highlighting that undermining PS/LPP may violate Article 8, which protects the right to respect for private and family life. Indeed, **Article 8 "*affords strengthened protection to exchanges between lawyers and their clients*"**. The Court specifies that "*this is justified by the fact that lawyers are assigned a fundamental role in a democratic society, that of defending litigants. Yet they cannot carry out this essential task if they are unable to guarantee to those they are defending that their exchanges will remain confidential*" [4].

The protection of confidentiality of lawyer-client communications has also been recognised as a **general principle of EU law** by the European Court of Justice[5] and has a **legal basis in the EU Charter of Fundamental Rights within its articles 7 on the right to privacy and 47 on the right to a fair trial**.

2. Limited interferences

According to article 52(1) of the EU Charter, interference with fundamental rights must be provided for by law, respect the essence of those rights and, subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. Furthermore, the rights contained in the Charter

[3] ECtHR, Michaud v. France (12323/11), 2012, §§117-118
[4] ECtHR, Kopp v. Switzerland (23224/94), 1998
[5] ECJ, AM&S v. Commission, (155/79), 1982, §18

corresponding to the rights guaranteed by the ECHR should have the same meaning and scope. This applies to the right to confidentiality of communications as it is guaranteed by article 7 of the Charter and article 8 of the ECHR. The right protected under article 8 ECHR might be subject to interference which should be in accordance with the law, pursue a legitimate aim and be necessary in a democratic society to achieve the aim concerned.

However, as stated above, the ECtHR affords a strengthened protection under article 8 ECHR to communications falling with the protection of PS/LPP. Moreover, the CCBE recalls that although the article 8 right is qualified, the right to a fair trial according to Article 6 ECHR is absolute and not a qualified one[6]. **Therefore, if a legally privileged communication, or a communication protected by an obligation of professional secrecy does fall within the scope of article 6 ECHR, then, given the absolute nature of the protection afforded by this article, there should be no possibility of interception being permitted**.

In this regard, it is noteworthy that in the transitional provisions of the **Regulation (EU) 2021/1232**[7], adopted to modify the e-privacy directive[8] to fight against CSAM, pending the adoption of the current proposal, the EU legislator has explicitly provided for a **clause on the protection of PS/LPP**, considering that **the temporary rules to detect online child sexual abuse should be "*without prejudice to the rules on professional secrecy under national law, such as rules on the protection of professional communications, between doctors and their patients, between journalists and their sources, or between lawyers and their clients, in particular since the confidentiality of communications between lawyers and their clients is key to ensuring the effective exercise of the rights of the defence as an essential part of the right to a fair trial*"**. Unfortunately, such general clause has not been repeated by the European Commission in the new proposal.

The following analysis of the proposal reveals that the necessary safeguards to ensure the protection of fundamental rights, including the confidentiality of communications, have been discarded. The CCBE considers that the very essence of the right to confidentiality is undermined by the proposal which lacks legal clarity, as a legal basis to the detection obligation, and proportionality regarding the interferences and limitations to fundamental rights.

B. The lack of sufficient safeguards in the proposal

1. The procedural safeguards and the role of private actors

The CCBE notes that a complex procedure leads to the issuance of a detection order, starting with a risk assessment carried out by the service provider and possible mitigation measures. In case a "*significant risk*" remains, the concerned national public authority, the so-called coordinating authority, shall launch the procedure for the adoption of a detection order. Before requesting such an order to the competent judicial or administrative authority, the coordinating authority must exchange with the service provider.

The conditions for requesting the issuance of a detection order are laid down in article 7(4) which requires the existence of a "*significant risk*" that the service is used for the purpose of online child sexual abuse. The assessment of the existence of such risk is provided for in article 7(5), (6) and (7) for each category of detection order (concerning the dissemination of known CSAM, new CSAM and the solicitation of children).

[6] ECtHR, Niemietz v. Germany, (13710/88), 1992, §375

[7] Regulation (EU) 2021/1232 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, 14 July 2021

[8] Directive 202/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 12 July 2002

Despite the supplement provisions of article 7(5)-(7), the prerequisites for adoption of a detection order, relying on the demonstration of a significant risk, are based on broad and vague concepts, lacking the necessary legal clarity for the proper implementation of the proposal and balance of the rights at stake. Indeed, the issuance of a detection order does not require a concrete suspicion and is not related to individual cases. The determination of a "*significant risk*" is enough and the latter "*shall be deemed to exist*" when the service is "*likely*" used for the dissemination of CSAM or for grooming. As indicated by the EDPB and the EDPS, **such vague provisions and legal uncertainty make it difficult to apply the legal requirements of the proposal in a predictable and non-arbitrary manner, by concerned service providers and courts or independent authorities issuing the order, and will lead to "*considerable divergences on the concrete implementation of the proposal across the Union*"**[9].

The CCBE is also deeply concerned by the involvement of private actors to identify, collect and forward content information while they are not subject to any obligation of professional secrecy nor to democratic control. As raised by European data protection bodies, targeted providers and authorities enjoy a wide margin of appreciation in balancing the fundamental rights of individuals. Service providers might have a consequent influence in the whole process leading to the issuance of a detection order. They should carry out the initial risk assessment (article 3), adopt mitigation measures having "*due regard*" to the "*potential consequences*" for the exercise of fundamental rights of all parties affected (article 4), before reporting and interacting with the coordinating authority which will decide to request or not a detection order.

In this regard, the CCBE notes that, regarding the risk assessment, a list of elements must be taken into account by the providers according to article 3(2)(a) to (e), such as what is prohibited or restricted in their terms and conditions; the manner users use the service; the manner the service is used or likely to be used by children; age groups and risk of solicitation of age group; existing functionalities to establish contacts. Regarding mitigation measures to be taken, article 4 requires the adoption of measures such as the adaptation of the provider's content moderation or recommender systems.

However, as indicated by the EDPS and the EDPB, criteria of articles 3 and 4 might seem relevant but leave a broad marge of interpretation and appreciation by using abstract, vague and generic terms. The CCBE agrees that "***these criteria do not meet the legal certainty and foreseeability criteria needed to justify an interference with the confidentiality of communications between private individuals which constitutes a clear interference with the fundamental rights to privacy and freedom of expression***"[10].

Moreover, with regards to Recital (17) which stipulates that providers should be able to indicate their willingness and preparedness to the issuance of a detection order, during the phase of reporting the risk to the competent public authority, it appears that their views on the possible adoption of an order will be heard while "***it cannot be assumed that each and every provider will seek to avoid the issuance of a detection order in order to preserve the confidentiality of communications of its users by applying the most effective, but least intrusive measures […]***"[11]. Thus, targeted providers will have a significant role in balancing the rights at stake, in particular the confidentiality of communications. This involvement is quite disturbing following the recent data leaks and scandals which showed the inability of certain providers to properly process highly sensitive content. Despite regulatory frameworks, supposedly robust in Europe, large platforms have bypassed data protection and privacy laws for years, demonstrating the ineffectiveness of regulatory mechanisms to guaranty the confidentiality of communications and data protection.

In this regard, the procedural safeguards and the complexity of the process leading to the adoption of a detection order are not enough and cannot replace substantive safeguards[12] to ensure the confidentiality of communications and the protection of PS/LPP. Also, the CCBE is strongly opposed to the approach where the protection of fundamental rights is partly or fully delegated to private parties.

[9] EDPB-EDPS Joint Opinion 4/2022, §37
[10] *Ibid*., §27
[11] *Ibid*., §29
[12] *Ibid*., §30

It is up to the EU legislators to adopt clear legal provisions and safeguards to ensure that fundamental rights of all citizens are properly ensured and well balanced.

2. Technologies used to detect CSAM and grooming

Following Article 10 of the proposal, targeted service providers receiving a detection order shall execute it by installing and operating technologies to detect the dissemination of known or new CSAM or grooming. Such technologies shall not be able to extract any other information from the relevant communications than the information strictly necessary to detect, in accordance with the state of the art in the industry and least intrusive in terms of the impact on the users' rights to privacy and the confidentiality of communications.

However, the CCBE notes that, as pointed out by the EDPS and the EDPB, "*the technologies currently available rely on the **automated processing of content data of all affected users*** […]. *Moreover, the technologies currently available, especially those for detecting new CSAM or grooming, are known to have **relatively high error rates**"*[13]. This is all the more alarming whereas "*the general conditions for the issuance of a detection order under the Proposal, i.e. applied to an entire service and not just to selected communications, the duration up to 24 months for known or new CSAM and up to 12 months for grooming, etc. may lead to a very broad scope of the order in practice. **As a result, the monitoring would actually be general and indiscriminate in nature, and not targeted in practice**".*

Also, in the previous impact assessment prepared by the European Parliamentary Research Service ("EPRS") on the temporary rules to fight against CSAM and grooming of the Regulation (EU) 2021/1232, the EPRS concluded that "***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**"*[14]**.**

The CCBE shares the EPDB-EDPS conclusions that "*the proposal could become the basis for de facto generalised and indiscriminate scanning of the content of virtually all types of electronic communications of all users in the EU/EEA. **As a result, the legislation may lead people to refrain from sharing legal content out of fear that they could be targeted based on their action***"[15].

The CCBE considers that the technologies at stake, as well as the conditions for their use, do not provide for sufficient safeguards in order to ensure the protection of PS/LPP and the confidentiality of communications. By applying to all users and operating an automated analysis of all communications, in an unproportionate manner, such technologies may enable the flagging and interception of privileged communications shared by clients and their lawyers, leading to breaches of PS/LPP. Beyond their lack of proportionality, the CCBE stresses that in all cases services providers should be required to ensure that the technology they used guarantees that there is no interference with any kind of data or communication protected by PS/LPP. They should be required to deploy technological means that safeguard that privileged material will not be accessed.

In view of the above developments, the CCBE concludes that the proposed measures enabling the detection and identification of contents by service providers should be removed from the proposal, in the absence of clear legal provisions and proper safeguards to ensure that the fundamental rights of individuals are respected and well balanced.

[13] *Ibid*., §52

[14] EPRS Study on the Commission proposal on the temporary derogation from the e-Privacy Directive for the purpose of fighting online child sexual abuse – Targeted substitute impact assessment, February 2021, page 37

[15] EDPB-EDPS Joint Opinion 4/2022, §55

II. Preventing attempts to jeopardise encryption

In addition, the CCBE notes that, as raised by the EDPB and the EDPS, the proposal might have an impact on the use of end-to-end encryption ("E2EE"). Recital 26 of the proposal states that providers have the choice of the used technologies to comply with detection orders, which should not be understood as incentivising or disincentivising the use of any given technology, providing that the technologies and accompanying measures meet the requirements of the proposed regulation, including end-to-end encryption technology. As explained by the EDPB and the EDPS, "*the mere possibility that a detection order might be issued is likely to weigh heavily on the technical choices made by providers, especially given the limited timeframe they will have to comply with such an order and the heavy penalties they would face for failing to do so. In practice, this might lead certain providers to stop using E2EE*".

Furthermore, it is astonishing to note that the **clause on the protection of end-to-end encryption**, provided for in Regulation (EU) 2021/1232, has not been repeated in the proposal of the European Commission as well as the clause on the protection of professional secrecy[16].

The CCBE considers that the proposal should not prevent lawyers from adequately protecting the confidentiality of their communications through encryption methods. The CCBE has stressed the particular vulnerability of lawyers to unlawful attacks by the government or private hackers, due to the fact that they keep sensitive information provided to them by clients in confidence that may not be disclosed[17]. This requires adequate cryptographic protection. Therefore, the CCBE calls the EU legislator to provide for the protection of E2EE and to ensure that the provisions of the proposal could not weaken E2EE in any way.

III. The cooperation between the new EU Centre and Europol

Finally, the CCBE notes that Chapter IV establishes an EU Centre on Child Sexual Abuse as a new decentralised agency to ensure the implementation of its provisions. The EU Centre should work in close cooperation with Europol, with a shared location, wide access to databases and information systems. According to Article 48, the EU Centre should forward to Europol and the competent national authorities reports that are not manifestly unfounded to investigate or prosecute potential child sexual abuse. Also, Article 53 requires that "*Europol and the EU Centre shall provide each other with the **fullest possible access to relevant information and information systems**, where necessary for the performance of their respective tasks and in accordance with the acts of Union law regulating such access*"'.

The CCBE has previously commented and expressed its concerns over the powers granted to Europol in its new mandate concerning the collection, processing and exchange of personal data. It considered that clear and precise provisions should govern the justifications for the collection, processing and exchange of personal data by Europol, which shall not bypass essential guarantees such as the need for prior judicial authorisation as well as the independent and impartial oversight system. In its position, the CCBE specified that any transfer of personal data to private parties made by Europol must respect essential guarantees (clear

[16] Recital (25) of Regulation (EU) 2021/1232: "*End-to-end encryption is an important tool to guarantee the security and confidentiality of the communications of users, including those of children. Any weakening of encryption could potentially be abused by malicious third parties. Nothing in this Regulation should therefore be interpreted as prohibiting or weakening end-to-end encryption*"

[17] CCBE Recommendations on the protection of client confidentiality within the context of surveillance activities, p. 20

legal basis, necessity and proportionality, independent judicial oversight and effective remedies)[18]. Furthermore, as raised by the EDPB and the EDPS, Europol's mandate is limited to support and strengthen actions by competent national authorities and their mutual cooperation in preventing and combating cross-border serious crime[19], and Union bodies providing information to Europol should determine the purpose or purposes for which that information needs to be processed by the latter and in which conditions[20].

Therefore, the CCBE considers that the forwarding of reports to Europol cannot take place on a general and automated basis. The CCBE supports the recommendation of the EDPB and the EDPS that the proposal should specify and limit the circumstances and purposes under which the EU Centre may forward reports to Europol. It should also require that any transfer of personal data to Europol should be adequate, relevant and limited to what is strictly necessary, while ensuring data quality and reliability[21]. Regarding the mutual access to relevant information systems between the EU Centre and Europol, the CCBE notes that the proposal does not specify the criteria nor the specific safeguards to enable such access to highly sensitive personal data. In this regard, the CCBE supports the recommendations of the EDPB and EDPS which consider that the exchange of personal data between the EU Centre and Europol should only take place on a case-by-case basis, following an explicit and duly assessed request[22].

[18] CCBE Position Paper on the Proposal for Regulation amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation, 6 May 2021

[19] Regulation (EU) 2016/794, Article 3

[20] *Ibid*., Article 19

[21] EDPB-EDPS Joint Opinion 4/2022, §126

[22] *Ibid*., §§129-133