Council of the European Union

Brussels, 26 April 2023
(OR. en)

8787/23

LIMITE

JUR 291
ENFOPOL 201
JAI 510

**OPINION OF THE LEGAL SERVICE**[1]

| | |
|---|---|
| From: | Legal Service |
| To: | Law Enforcement Working Party |
| Subject: | Proposal for a Regulation laying down rules to prevent and combat child sexual abuse – detection orders in interpersonal communications – Articles 7 and 8 of the Charter of Fundamental Rights – Right to privacy and protection of personal data – proportionality |

## I. INTRODUCTION

1. On 11 May 2022, the Commission submitted a Proposal for a Regulation laying down rules to prevent and combat child sexual abuse ("the proposed Regulation")[2]. The objective of the proposed Regulation is to establish uniform rules to address the use of information society services for online child sexual abuse in the internal market[3]. The legal basis for the proposed Regulation is Article 114 TFEU.

1 This document contains legal advice protected under Article 4(2) of Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, and not released by the Council of the European Union to the public. The Council reserves all its rights in law as regards any unauthorised publication.

2 COM(2022) 209 final.

3 Article 1(1) of the proposed Regulation.

2. The proposed Regulation establishes obligations on providers of information society services i) to assess the risk that their services are used for online child sexual abuse; ii) **to detect and report online child sexual abuse** and iii) to remove or disable access to child sexual abuse material on their services. It also establishes rules as regards the designation and functioning of the competent authorities of the Member States in charge of fighting online child sexual abuse and the cooperation between them. Finally, it sets up a new EU Agency, the EU Centre on Child Sexual Abuse.

3. During the discussions in the Law enforcement Working Party (LEWP) serious legal concerns were raised as regards, in particular, the **detection orders applied to interpersonal communication services**.[4]

4. The Council Legal Service (CLS) was requested to provide a written opinion on this matter. This opinion provides a legal analysis of the **conformity of the detection order applied to interpersonal communication services with Article 7 and 8 of the Charter of Fundamental Rights (the Charter) as interpreted by the relevant case law of the CJEU.** It is based on the oral interventions already made by the CLS representative in LEWP and focuses on the problematic aspects of the proposed Regulation in this respect. It is without prejudice to the legal analysis of other aspects of the proposed Regulation, including, in particular, the detection order obligations with regard to ***publicly available material on the internet***.

## II. LEGAL FRAMEWORK

5. Detection obligations and the procedure concerning the issuing of detection orders are provided for in Section 2, Articles 7 to 11, of the proposed Regulation. Its Article 44 on the role of the EU Centre (the new agency) in creating, maintaining and operating *"Databases of indicators"* is also relevant for the present analysis. The aspects of these provisions that are relevant for the purposes of the present analysis can be summarised as follows.

[4] The detection orders applied to material publicly available on the web as well as the removal, blocking and delisting orders were considered less problematic than the detection orders applied to interpersonal communications.

6. A **detection order** may be issued by a national judicial or independent administrative authority following a request of a Coordinating Authority (the authority designated by a Member State for the application and enforcement of the proposed Regulation), in order to require a service provider to detect online child sexual abuse. The detection order should include the specific service in respect of which the detection order is issued and, where applicable, the part or component of the service that would be affected (Article 8(1)(d)).

7. Information society services to which the proposed Regulation apply include **interpersonal communications services**[5].

8. The service providers to which a detection order is addressed would be required to detect **already known** child sexual abuse material (CSAM), **unknown** CSAM and **solicitation of children**. The detection orders concerning the solicitation of children would apply to interpersonal communications where one of the users is a child user (Article 7(8)).

9. A detection order can be issued when the issuing authority considers that the conditions referred to in Article 7(4) of the proposed Regulation are met. It would be **directed at a specific service** where *"there is evidence of a significant risk of the service being used for the purpose of online child sexual abuse"* and where such an order would be considered proportionate[6]. It would concern the communications of all the users of that service. The ultimate assessment of the "evidence", the "significant risk" and the proportionality of an order would lie with the competent national judicial authority or independent administrative authority issuing the order.

---

5 Article 2 of the proposed Regulation.
6 Article 7(4) of the proposed Regulation.

10. The CSAM would have to be detected by the service provider by **installing and operating technologies** to detect the dissemination of known or new child sexual abuse material or the solicitation of children, which would be based on the corresponding indicators provided by the EU Centre. Detection would imply, therefore, that content of all communications must be accessed and scanned, and be performed by means of available automated tools, the exact nature of which is not specified in the proposal, as the proposal's ambition is to remain technologically neutral.[7]

11. The proposed Regulation specifies that the technologies would have to be i) effective in detecting the dissemination of such material, ii) not be able to extract any other information from the relevant communications than the information strictly necessary to detect such material, iii) based on the use of the indicators in accordance with the state of the art in the industry and the least intrusive in terms of the impact on the users' rights to privacy and data protection, and iv) sufficiently reliable (limiting to the maximum extent possible the rate of errors). The technologies would have to be made available (but not conceived) by the EU Centre. Nevertheless, service providers would not be required to use any specific technology, including those made available by the EU Centre, as long as the requirements set out in the Regulation are met. Furthermore, the responsibility to comply with those requirements and for any decisions to be taken in connection to or as a result of the use of the technologies made available by the EU Centre would rest on the service providers.[8]

12. The detection technologies would have to be based on the *"indicators"* of known CSAM, unknown CSAM and solicitation of children provided by the EU Centre. Two types of tools would need to be used. For any detection, the relevant providers would be compelled to implement **content verification tools** in order to analyse all content for the presence of known and unknown CSAM or for solicitation of children. Additionally, for detecting solicitation of children, they would have to use (unspecified) **age verification tools** to distinguish between adult and child users.[9]

---

7 Articles 10 and 46 of the proposed Regulation.
8 Articles 10(2), (3), and 50 of the proposed Regulation.
9 Articles 7, 10 and 44 of the proposed Regulation.

13. The period of application of detection orders would be *"limited to what is strictly necessary"* but should not exceed 24 months for the dissemination of known or new CSAM and 12 months for the solicitation of children.[10]

## III. LEGAL ANALYSIS

14. Article 52(1) of the Charter states, regarding the scope and interpretation of the rights guaranteed by it, that any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms. In observance of the principle of proportionality, limitations are only possible if they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.

15. As will be further explained in subsections 2 and 3 below, there is no doubt that, on the one hand, the detection order for interpersonal communications pursues an objective of general interest and, on the other hand, that it introduces significant limitations to the rights to privacy and personal data protection. The main legal concerns as to the compliance with the Charter as interpreted by the case law of the Court of Justice arise on the question whether those limitations are sufficiently regulated by law, compromise the essence of those fundamental rights, and are proportionate to the objective pursued. Subsections 1, 4 and 5 below will further elaborate on these aspects.

[10] Article 7(8)(c) and (9) of the proposed Regulation.

### 1. The limitations to the fundamental rights must be provided for by law

16. According to well-established case law of both the ECtHR and the Court[11], the requirement that any limitation on the exercise of a fundamental right must be *provided for by law* implies that the act which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned. Therefore, such requirement not only refers to the fact that the interference must have a basis "in law" – which is not at issue in the present case – but also implies that the legal act permitting the interference with those rights must itself define clearly and precisely the scope of the limitation. The measure at issue must be accessible and foreseeable and, as a result, allow for meaningful judicial control, even though it can be formulated in terms which are sufficiently open to be able to adapt to different scenarios and keep pace with changing circumstances[12].

17. Requirements of clarity, precision and completeness are all the more relevant with regard to the proposed Regulation, given the extent and seriousness of the interference with the fundamental rights that would be caused by the regime of detection orders in interpersonal communications. Indeed, given the significance of the interference with fundamental rights, the judicial review by the Court would be strict and not limited to manifest error, thereby reducing scope of discretion of the Union legislature.[13] This intensity of judicial review increases the importance of having clear, precise and complete legal provisions for the purposes of ensuring a legally sound approach.

---

11 See, ECtHR judgment of 25 May 2021, Big Brother Watch and Others v. United Kingdom, CE:ECHR:2021:0525JUD005817013, paragraph 333, and the case law cited. See, among others, judgment of 16 July 2020, Facebook Ireland and Schrems, C-311/18, EU:C:2020:559, paragraph 175, and the case law cited.

12 See judgment of 21 July 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, paragraph 114.

13 See judgments of 8 April 2014, Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 47 and 48 and case law cited therein.

18. In addition, this measure is a regulation *"directly applicable in all the Member States"*[14] and, unlike a directive, will not, in principle, require the adoption of any *transposition* measure of the detection order obligations applied to interpersonal communications in the national legal orders. This implies that, in case of judicial review, compliance with fundamental rights of the regime of detection orders would have to be assessed on the basis of its own merits, clarity and precision, as defined by the Union legislature. Therefore, in applying the principle of conform interpretation with those rights, it would not be possible to rely on the margin of discretion of Member States in transposing a directive.[15]

19. In the light of the above, it must be noted, first of all, that the proposed Regulation provides for a comprehensive set of rules concerning, in particular, the risk assessment, the risk mitigation, the risk reporting and the issuing of detection orders by judicial authorities or independent administrative authorities, which are significant elements supporting a conclusion that the first requirement of Article 52 of the Charter is complied with.

20. However, this conclusion is undermined in two important respects concerning, on the one hand, the key role and impact of the technology on the limitation of the fundamental rights at stake and, on the other hand, the lack of qualification of the substantive conditions concerning the issuance of a detection order.

21. On the **first** aspect, concerning technology, on a combined reading of Articles 7(1) and 10(1) of the proposed Regulation the detection order consists, in substance, of imposing on a specific service provider the obligation to install and operate a technology enabling the detection of CSAM. Nevertheless, in its Articles 7(1), (3)(a) and (8), 10(2) and (3), and 44, the proposed Regulation does not specify in sufficient detail the nature and the features of the technologies to be made available for this purpose.

---

14 Article 288 TFEU.

15 See, judgment of 21 July 2022, Ligue des droits humains, C-817/19, paragraphs 87 to 89, where in order to assess the legality of the Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ 2016 L 119, p. 132) the Court in applying the principle of conformity relied also on the implementation of the directive by the Member States.

22. In particular, it is not specified what *"sufficiently reliable detection technologies"* means, and what would be the *"rate of errors"* regarding the detection that would be considered acceptable in terms of balance between *"effectiveness"* and the need to take the *"least intrusive measures"*. Furthermore, the *"indicators"* to be used to detect known CSAM, unknown CSAM and solicitation of children are to be elaborated and provided by the EU Centre at a later stage. The same goes for the unspecified tools needed to distinguish between adult and child users in the case of detection of solicitation of children (age verification tools). In these respects, the requirement of compliance with fundamental rights is not defined in the act itself but is left to a very large extent to the service provider, which remains responsible for the choice of the technology and the consequences linked to its operation.[16]

23. To provide one example, the choice of age verification technology (mass profiling and/or biometric identification and/or digital identity certificates) could greatly impact the degree of intrusiveness of the system, and therefore influence the further assessment of the conformity with the Charter of the detection orders regime as a whole.

24. On the **second** aspect, concerning the conditions for the issuance of a detection order, although its Article 7 sets out certain detailed requirements in this regard, the proposed Regulation does not set out the methodology by which the risk of use of the specific service for the purpose of child sexual abuse should be assessed, or specify a meaningful threshold of the level of risk that would justify the introduction of the detection order. Article 7(4) to (7) refer to the concepts of *"significant risk"*, *"negative consequences for the rights and legitimate interests"* of the users, *"fair balance between fundamental rights"*, *"mitigation measures"* or *"potential consequences"* for all the parties affected. Depending on whether the detection order concerns known, unknown CSAM, or solicitation of children, those concepts are, in turn, further defined by referring to other insufficiently precise concepts like the use *"to an appreciable extent"* of services or comparable services for the purposes of the dissemination of any CSAM and a *"significant number of reports"* available in this respect.

---

16 See judgment of 5 September 2012, Parliament v Council, C-355/10, EU:C:2012:516, paragraph 77.

25. The terms used – for instance the reference to the need for a measure to be *"effective"* – combined with the fact that the responsibility for the choice of "effective" technology lies ultimately with the service providers, raise serious doubts as to the foreseeability of the impact of these measures on the fundamental rights at stake.

26. In conclusion, the concepts used in the proposed Regulation to determine the limitations to the fundamental rights at stake that would derive from the use of detection orders, as well as the fact that those limitations would depend, in essence, on technologies and methodologies which are yet to be established, makes it challenging to assess the degree of interference with fundamental rights. In substance, the duty to further determine the extent of such interference would ultimately be upon those in charge of conceiving the relevant technology, the parameters for the indicators-based screenings and implementing the detection order on a case-by-case basis (EU Centre, national authorities, judges, service providers). The extent of discretion involved could give rise to a very broad range of possible different interpretations and concerns as regards compliance with fundamental rights.

27. In light of the above, the regime of detection orders, as currently provided for by the proposed Regulation, entails the risk of not being sufficiently clear, precise and complete, and therefore of not being in compliance with the requirement that limitations to fundamental rights must be provided for by law. The proposed Regulation should provide more detailed elements both on the limits to fundamental rights that the specific type and features of the technology to be used would entail and related possible safeguard measures.

## 2. Combating child sexual abuse as an objective of general interest

28. As to the question whether the detection orders established by the proposed Regulation **pursue an objective of general interest** recognised by the Union or the need to protect the rights and freedoms of others, the Court has affirmed that the fight against serious crime in order to ensure public security constitutes an objective of general interest.[17] Furthermore, the Court explicitly enumerates *"the sexual exploitation of children and child pornography"* among the offences that *"are inherently and indisputably extremely serious"*.[18] This is also reflected in the EU relevant legislation concerning child sexual abuse.[19]

29. The Court affirms that *"[…]as regards, in particular, effective action to combat criminal offences committed against, inter alia, minors and other vulnerable persons, it should be borne in mind that positive obligations of the public authorities may result from Article 7 of the Charter, requiring them to adopt legal measures to protect private and family life. Such obligations may also arise from Article 7, concerning the protection of an individual's home and communications, and Articles 3 and 4, as regards the protection of an individual's physical and mental integrity and the prohibition of torture and inhuman and degrading treatment."*

---

17 See judgments of 8 April 2014, Digital Rights Ireland and Others, C-293/12 and C-594/12, paragraph 42, of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, 125, EU:C:2020:79, paragraph 126. The Court notes, in this respect, that Article 6 of the Charter lays down the right of any person not only to liberty, but also to security. However, the Court specifies that since that provision applies to deprivations of liberty by a public authority, Article 6 of the Charter cannot be interpreted as imposing an obligation on public authorities to take specific measures to prevent and punish certain criminal offences.

18 See, judgment of 21 July 2022, Ligue des droits humains, C-817/19, paragraph 149.

19 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 (OJ 2011 L 335, p. 1, and corrigendum OJ 2012 L 18, p. 7).

30. The Court concludes, in this respect, that *"Articles 4 and 7 of the Charter, require, in particular, the adoption of substantive and procedural provisions as well as practical measures enabling effective action to combat crimes against the person through effective investigation and prosecution, that obligation being all the more important when a child's physical and moral well-being is at risk."*.[20]

31. It is noted that, on the one hand under its Article 1 (*subject matter and scope*), the objective of the proposed Regulation is *"to address the misuse of relevant information society services for online child sexual abuse in the internal market"*. On the other hand, in Article 2 (l) to (n) (definitions), the proposed Regulation refers to the definitions of CSAM included in Directive 2011/93/EU on combating children sexual abuse and sexual exploitation of children and child pornography, and not to the definition of the related criminal offences concerning sexual abuse provided for by that Directive. Therefore, the scope of the detection order provided for by the proposed Regulation is not limited to detecting criminal conduct.

32. In the light of the above, there is no doubt that the detection orders are meant to pursue the important objective of general interest of preventing, detecting, investigating and prosecuting child sexual abuse offences. Nevertheless, the scope of such detection, as defined by the proposed Regulation, is broader than the detection of criminal conduct. This is an aspect that needs to be taken into account in assessing the requirements referred to in Article 52 of the Charter as interpreted by the Court.

[20] See judgments of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, paragraph 128, of 20 September 2022, SpaceNet AG, C-793/19 and C-794/19, EU:C:2022:702, paragraphs 63 to 65.

### 3. The limitation on the rights to privacy and the protection of personal data

33. The screening of interpersonal communications as a result of the issuance of a detection order undeniably affects the fundamental right to respect for private life, guaranteed in Article 7 of the Charter, because it provides access to and affects the confidentiality of interpersonal communications (text messages, e-mails, audio conversations, pictures or any other kind of exchanged personal information). It is also likely to have a deterrent effect on the exercise of freedom of expression, which is enshrined in Article 11 of the Charter[21]. It does not matter in this respect whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference.[22]

34. Furthermore, such screening constitutes the processing of personal data within the meaning of Article 8 of the Charter and affects the right to protection of personal data provided by that provision.[23]

35. It must be noted, in this respect, that under settled case law the fact that the automated analysis based on predefined indicators would not, as such, allow all the users whose data is being analysed to be identified, does not prevent such data from being considered personal data, in so far as the automated analysis would allow the person or persons concerned by the data to be identified at a later stage. According to the definition of personal data in Article 4(1) of the General Data Protection Regulation (GDPR), information relating, inter alia, to an **identifiable person** constitutes personal data.[24] Therefore, screening of all communications in a given service, with the assistance of an automated operation, presupposes systematic access to and processing of all information and constitutes an interference with the right to data protection, regardless of how that data is used subsequently. In particular, the question whether that information is subsequently accessed by the competent authorities is irrelevant.

---

21 See judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, paragraph 173.

22 See judgment of 21 July 2022, Ligue des droits humains, C-817/19, paragraph 96.

23 See, by analogy, judgment of 21 July 2022, Ligue des droits humains, C-817/19, paragraphs 93 and 94.

24 See judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, paragraph 171.

36. As to the seriousness of the interference that the use of a detection order in interpersonal communications would entail, in *La Quadrature du Net*[25], the Court analysed the national legislation which, for the purpose of safeguarding national security including terrorism, required providers of electronic communications services to implement, on their networks, measures allowing for the automated analysis of traffic and location data.

37. In *La Quadrature du Net,* the Court considered that an automated analysis corresponding, *"[…] in essence, to a screening of all the traffic and location data retained by providers of electronic communications services, which is carried out by those providers at the request of the competent national authorities applying the parameters set by the latter"* as being a ***particularly serious interference*** since it covers, ***generally and indiscriminately***, the data of persons using electronic communication systems, is likely to reveal the nature of the information consulted online and applies also to persons with respect to whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with terrorist activities.[26]

38. The national measure assessed by the Court in paragraphs 171 to 180 of the judgement *La Quadrature du Net* is similar to the detection orders in the proposed Regulation. In both cases the providers are required to automatically screen the communication data. In both cases, the screening is based on the *"indicators"* provided by the public authorities. Both measures concern electronic communications services and are likely to reveal the nature of the information exchanged online. Furthermore, both measures apply also to persons with respect to whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with the criminal activities concerned.

---

25 See, judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, paragraphs 172 to 180.

26 See, judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, paragraph 174.

39. Nevertheless, for the purpose of assessing whether a detection order in interpersonal communication would entail a ***particularly serious interference*** in the light of this case law, it must be assessed, first, whether the detection order would cover *generally and indiscriminately* the data of persons using electronic communication systems within the meaning of that case law and, second, the type of data concerned.

40. **First**, the fact that a detection order would be addressed to a specific service provider and not to all interpersonal communications services does not seem, as such, a relevant argument to consider that the measure would not be of ***general and indiscriminate*** nature.

41. It must be noted that in assessing ***targeted*** versus ***general and indiscriminate*** measures, the Court takes into account the specific nature of the measure.[27] In particular, the relevant factor that is taken into account by the Court in its case law concerning retention of communication of *metadata* is whether the automated processing of data is limited on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, or whether other objective and non-discriminatory criteria may be considered in order to establish a connection, at least indirectly, between serious criminal acts and the persons whose data are processed.[28] The need for such *connection*, established by the Court in the context of the retention of *metadata* (traffic and location data) should be appreciated differently in relation to access to content data (content of interpersonal communications), which constitutes a more significant interference with fundamental rights.

---

27 See, for example, judgment of 26 January 2023, Ministerstvo na vatreshnite raboti, C-205/21, EU:C:2023:49, paragraph 129.

28 See judgment of 20 September 2022, SpaceNet AG, C-793/19 and C-794/19, paragraphs 75, 83 to 84, 112 and 113.

42. The obligations in the detection orders provided for by the proposed Regulation, while addressed to a specific service provider, would imply that content of all interpersonal communications concerning that service (or the affected part or component where applicable)[29] must be accessed and scanned by means of automated tools. Therefore, such processing of data would not be limited to the interpersonal communications of persons in respect of whom there are reasonable grounds to believe that these persons are in any way involved in committing, or have committed a child sexual abuse offence, or presenting a connection, at least indirectly, with sexual abuse offences.

43. The proposed legislation requires the general screening of the data processed by a specific service provider without any further distinction in terms of persons using that specific service. The fact that the detection orders would be directed at specific services where there is evidence of a significant risk of the service being used for the purpose of online child sexual abuse would be based on a connection between that service and the crimes of child sexual abuse, and not, even indirectly, on the connection between serious criminal acts and the persons whose data are scanned. The data of all the persons using that specific service would be scanned without those persons being, even indirectly, in a situation liable to give rise to criminal prosecutions, the use of that specific service being the only relevant factor in this respect.

44. With this regard, it must be taken into consideration that interpersonal communication services are used by almost the entire population and may also be used for the dissemination of CSAM and/or for solicitation of children. Detection orders addressed to those services would entail a variable but in almost all cases very broad scope of automated analysis of personal data and access to personal and confidential information concerning a very large number of persons that are not involved, even indirectly, in child sexual abuse offences.

[29] See Article 8(1)(d) of the proposed Regulation.

45. This concern is further confirmed by the fact that the proposed Regulation does not provide any substantive safeguards to avoid the risk that the accumulated effect of application of the detection orders by national authorities in different Member States could lead to covering all interpersonal communication services active in the Union.

46. Furthermore, since issuing a detection order with regard to a specific provider of interpersonal communication services would entail the risk of encouraging the use of other services for child sexual abuse purposes, there is a clear risk that, in order to be effective, detection orders would have to be extended to other providers and lead *de facto* to a permanent surveillance of all interpersonal communications.

47. In the light of the above, even though the detection order is addressed to a single service provider with regard to a specific interpersonal communication service or a part or component of it, it is highly probable that in case of judicial review, a data screening obligation such as that provided by the obligations in the detection orders would be considered as *general and indiscriminate*, and therefore not *targeted* processing of data.

48. Given its general and indiscriminate nature, such screening obligation would, therefore, entail a ***particularly serious interference*** with fundamental rights in the light of the case law referred to above in paragraphs 36 and 37.

49. **Second**, such conclusion is further confirmed by the significance of the interference, which is more acute in the detection order than in *La Quadrature du Net* in view of the categories of data concerned. In *La Quadrature du Net*, the generalised screening concerned the *metadata* (traffic and location data), while the detection order would concern screening of the *content of communications*. The processing of metadata is less intrusive than similar processing of content data.

50. Moreover, the screening of content of communications would need to be effective also in an encrypted environment, which is currently widely implemented in the interpersonal communication environment. That would imply that the providers would have to consider (i) abandoning effective end-to-end encryption or (ii) introducing some form of "back-door" to access encrypted content or (iii) accessing the content on the device of the user before it is encrypted (so-called "client-side scanning").[30]

51. Therefore, it appears that the generalised screening of content of communications to detect any kind of CSAM would require *de facto* prohibiting, weakening or otherwise circumventing cybersecurity measures (in particular end-to-end encryption), to make such screening possible. The corresponding impact on cybersecurity measures, in so far as they are provided by economic operators on the market, even under the control of competent authorities, would create a stronger interference with the fundamental rights concerned and could cause an additional interference with other fundamental rights and legitimate objectives such as safeguarding data security.

52. Furthermore, the screening of audio or written communications in order to detect solicitation of children would necessarily require age assessment/verification generalised to all users of the service concerned. In fact, without establishing the precise age of all users, it would not be possible to know that the alleged solicitation is directed towards a child. Such process would have to be done either by (i) mass profiling of the users or by (ii) biometric analysis of the user's face and/or voice or by (iii) digital identification/certification system. Implementation of any of these measures by the providers of communication services would necessarily add another layer of interference with the rights and freedoms of the users.

---

30 See also, in this respect, request for a preliminary ruling from the Landgericht Berlin (Germany) lodged on 24 October 2022 – Criminal proceedings against M.N., in pending Case C-670/22, concerning the use of evidence obtained from the interception of enabled end-to-end encrypted communication telecommunications, including content of communications, covering all the users subscribed to a communications service, without concrete evidence of the commission of serious criminal offences by those individual users.

53. It follows from the above that the application of detection orders to interpersonal communications, as proposed, would entail a particularly serious interference with fundamental rights.

### 4. The essence of the right to privacy and protection of personal data

54. In this context the question could also arise whether, in the light of the case law the interference entailed by the proposed detection orders applied to interpersonal communication could even compromise **the essence** of the right[31] to the respect for private and family life as well as the right to the protection of personal data.

55. Indeed, the Court has ruled that, *"legislation permitting the public authorities to* ***have access on a generalised basis to the content of electronic communications*** *must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter"*.[32] Furthermore, it can be inferred from the case law that the interference entailed by such legislation in the fundamental rights enshrined in Articles 7 and 8 of the Charter is considered as being very far-reaching, particularly serious and likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance.[33]

---

31 The obligation to respect the essence of the rights concerned is one of the conditions foreseen by Article 52(1) of the Charter for the lawfulness of a limitation on the exercise of the rights and freedoms recognised by the Charter.

32 See judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 94.

33 See judgments of 8 April 2014, Digital Rights Ireland and Others, C-293/12 and C-594/12, paragraph 39; of 6 October 2015, Schrems, C-362/14, paragraph 94; of 21 December 2016, Tele2 Sverige and Watson and Others, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 100 and 101.

56. In so far as the detection which may be authorised would entail generalised access to and further processing of the content of interpersonal communications, the right to confidentiality of correspondence would become ineffective and devoid of content, since it would not impose any limitation in terms of either content or persons concerned to be complied with by a service provider. In the light of the above-mentioned case law, such interference entails, therefore, the serious risk even of compromising the essence of the fundamental right to respect for private life.

57. It is true that, under Article 10(3)(b) of the proposed Regulation, the technology to be made available and used by the services provider *"shall not be able to extract any other information from the relevant communications than the information strictly necessary to detect* [CSAM]*"*, and *"shall be in accordance with the state of the art in the industry and the least intrusive in terms of the impact on the users' rights to privacy and family live as well as data protection"*. Nevertheless, it must be recalled in this respect that not extracting irrelevant communication does not exclude, *per se*, the need to screen, through an automated analysis, all the interpersonal communication data of every user of the specific communication service to which the order is addressed, including to persons with respect to whom there would be no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with child sexual abuse offences.

58. In the light of the above, it can be concluded that the detection order regime provided for by the proposed Regulation as regards interpersonal communications entails a serious risk that it would be found to compromise the essence of the rights to privacy and data protection enshrined in Article 7 and 8 of the Charter, in so far as it would seek to authorise access on a generalised basis, through automated and systemic screening surveillance, to the content of electronic communications and personal data of all users of a specific service, irrespective of their direct or indirect link with child sexual abuse criminal activities.[34]

[34] See by analogy, judgment of 21 July 2022, Ligue des droits humains, C-817/19, paragraphs 92 to 111.

## 5. Compliance with the principle of proportionality

59. Notwithstanding the foregoing, in the event that the measures at stake are considered to respect the essence of fundamental rights, their compliance with the Charter would have to be assessed from the perspective of proportionality in so far as they entail, in any case, ***particularly serious*** limitations of/interferences with those rights, as outlined in paragraphs 33 to 53 above.

60. Under settled case law, the principle of proportionality requires that the limitations which may, in particular, be imposed by acts of EU law on rights and freedoms enshrined in the Charter do not exceed the limits of what is **appropriate and necessary** in order to meet the legitimate objectives pursued or the need to protect the rights and freedoms of others; where there is a choice between several appropriate measures, recourse must be had to the least onerous, and the disadvantages caused must not be disproportionate to the aims pursued. Moreover, where several fundamental rights and principles enshrined in the Treaties are at issue, the assessment of observance of the principle of proportionality must be carried out in accordance with the need to reconcile the requirements of the protection of those various rights and principles at issue, striking a fair balance between them.[35]

61. The need to ensure that the interference to privacy and data protection is limited to what is strictly necessary is all the greater where personal data are subjected to automated processing, particularly where there is a significant risk of unlawful access to those data. This consideration would apply especially where the protection of the category of personal data concerns sensitive data.[36] This is clearly the case for the data contained in the content of interpersonal communications.

---

35 See judgment of 17 December 2020, Centraal Israëlitisch Consistorie van België and Others, C-336/19, EU:C:2020:1031, paragraph 64.

36 See judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, cited, paragraph 132.

62. In its case law to date, the Court has not directly discussed the proportionality of a mandatory screening of *content of interpersonal communications* for law enforcement purposes such the one provided for by the proposed Regulation, for the obvious reason that no such measure has yet been enacted by the Union or by any of its Member States. Comparative law is also of limited assistance.[37] The outcome of the proportionality test may however be inferred from a number of rulings concerning, in particular, internal market legislation (Article 15 of the e-Privacy Directive[38]), where the proportionality of measures related to communication data was at stake. This case law is all the more relevant here as the proposed Regulation, like the above-mentioned directive, is based on Article 114 TFEU.

63. The methodology developed by the Court to assess the proportionality of particularly serious interferences to fundamental rights in the context of data retention or access to *metadata* is relevant for the purposes of assessing the measures at stake.

64. In this context, with regard to Articles 7, 8, 11 and Article 52(1) of the Charter, the Court stated, **first of all**, that those provisions do not preclude legislative measures that, for the purposes of combating serous crime and preventing serious threats to public security, provide for the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary.[39]

---

37 However, see the discussion on the scanning of communication data under the US legislation (judgments of 6 October 2015, Schrems, C-362/14, cited and of 16 July 2020, Facebook Ireland and Schrems, C-311/18, cited). Regarding different, but connected issue of bulk interception of communications by intelligence services for national security purposes see ECtHR judgment of 25 May 2021, Big Brother Watch and Others v. United Kingdom, CE:ECHR:2021:0525JUD005817013 and Centrum för Rättvisa v. Sweden, CE:ECHR:2021:0525JUD003525208.

38 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.

39 See judgment of 20 September 2022, SpaceNet AG, C-793/19 and C-794/19, cited, paragraph 75.

65. However, the Court specified that even the positive obligations which may arise, depending on the circumstances, from Articles 3, 4 and 7 of the Charter and which relate to the establishment of rules to facilitate effective action to combat criminal offences, cannot have the effect of justifying interference that is as serious as that entailed by legislation providing for the retention of traffic and location data with the fundamental rights to privacy and personal data protection, in circumstances where the data of the persons concerned are not liable to disclose a link, at least an indirect one, between those data and the objective pursued.[40]

66. In the light of this case law, and taking into account the considerations referred to in paragraphs 39 to 47 above, there is a serious risk of non-compliance with the principle of proportionality in so far as the detection orders would require the *general and indiscriminate access* to the content of personal communications by a specific service provider, and would apply without any distinction to all the persons using that specific service, without those persons being, even indirectly, in a situation liable to give rise to criminal prosecution.

[40] See judgments of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, cited, paragraph 145, and of 20 September 2022, SpaceNet AG, C-793/19 and C-794/19, cited, paragraph 24. It must be noted, in this respect, that the Court accepted the conformity with the Charter of provisions that make it possible, with regard to a person in respect of whom there are reasonable grounds to believe that is involved in serious criminal offences, to secure the effective and rapid collection of data in the context of a criminal procedure and following an individual assessment of their necessity and proportionality (see, judgments of 15 December 2015, WebMindLicenses, C-419/14, EU:C:2015:832, paragraph 69, and of 16 February 2023, HYA e.a., C-349/21, EU:C:2023:102, paragraph 49).

67. It must be noted, in this respect, that establishing *a link, at least an indirect one,* between the content of interpersonal communications and the objective pursued by the measures at stake is further affected by the fact that, in the light of paragraph 31 above, the detection orders are not limited to criminal content. Directive 2011/93/EU on combating children sexual abuse and sexual exploitation of children and child pornography establishes minimum rules concerning the definition of the relevant offences and leaves the Member States the task of defining several elements constituting the relevant criminal offences in national law (see, in particular the "age of sexual consent" below which it is prohibited to engage in sexual activities with a child). As a result, the screening at EU level may cover material which would not always constitute or lead to child sexual abuse offences in all the Member States.

68. Moreover, the risk of non-compliance with the principle of proportionality would be further aggravated by the fact that the detection order, unlike the measures addressed in the case law referred to in paragraph 64, would concern the content of interpersonal communications and not the traffic and location data.

69. **Second**, the Court stated that EU law does not preclude, for the purposes of combating crime in general, the **generalised retention of data relating to civil identity and IP addresses**.[41]

[41] Data related to civil identity concern purchase of a means of electronic communication, such as a pre-paid SIM card being subject to a check of official documents establishing the purchaser's identity and the registration, by the seller, of that information, with the seller being required, should the case arise, to give access to that information to the competent national authorities. IP addresses are part of traffic data, they are generated independently of any particular communication and mainly serve to identify, through providers of electronic communications services, the natural person who owns the terminal equipment from which an Internet communication is made. See judgment of 20 September 2022, SpaceNet AG, C-793/19 and C-794/19, cited, paragraph 99.

70. The Court has confirmed, in this respect, that the retention of the IP addresses of all natural persons who own terminal equipment permitting access to the Internet might be the only means of investigating offences committed online, inter alia, in cases involving particularly serious child pornography offences, such as the acquisition, dissemination, transmission or making available online of child pornography, within the meaning of Article 2(c) of Directive 2011/93/EU on combating children sexual abuse and sexual exploitation of children and child pornography. However, the Court specified, on the one hand, that the civil identity of users of electronic communications systems, does not provide, apart from the contact details of those users, such as their addresses, any information on the communications sent and, consequently, on the users' private lives. Thus, the interference entailed by the retention of that data cannot, in principle, be considered as serious, On the other hand, concerning IP addresses, although they are part of traffic data, they do not, as such, disclose any information about third parties who were in contact with the person who made the communication. That category of data is therefore less sensitive than other traffic data.[42]

71. This case law can therefore not serve as a basis to conclude that the particularly serious interference with privacy and data protection entailed by the detection order obligations in interpersonal communications would be necessary and proportionate, in so far as they would impose the screening of information which the Court, contrary to the above-mentioned case law, considered as very sensitive (content of interpersonal communications).

[42] See judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, cited, paragraphs 152 to 158.

72. **Third**, in *La Quadrature du Net*, the Court stated that the particularly serious interference that is constituted by the general and indiscriminate automated analysis of traffic and location 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 of that retention is limited to what is strictly necessary. The Court specified that it is only in these circumstances that a general and indiscriminate screening of data which is likely to reveal the nature of the information consulted online and applies irrespective of a link, even an indirect or remote one, with terrorist activities, may be considered to be justified in the light of the requirements stemming from Articles 7, 8 and 11 and Article 52(1) of the Charter.[43]

73. However, it is difficult to see how this case law can serve as a basis to justify a measure which aims at combating criminal offences, which are indisputably serious, but are not related to threats to national security.

74. In this regard, the Court has held that the objective of protecting national security corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society through the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities. Such a threat is therefore distinguishable, by its nature, its seriousness, and the specific nature of the circumstances of which it is constituted, from that of serious criminal offences being committed. The Court concludes, in this respect, that crime, even of a particularly serious nature, cannot be treated in the same way as a threat to national security.[44]

---

43 See, judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, cited, paragraphs 172 to 180.

44 See judgments of 5 April 2022, Commissioner of An Garda Síochána and Others, C-140/20, EU:C:2022:258, paragraphs 61 62, and of 20 September 2022, SpaceNet AG, C-793/19 and C-794/19, cited, paragraphs 92 to 94.

75. Therefore, if the screening of communications *metadata* was judged by the Court proportionate only for the purpose of safeguarding *national security*, it is rather unlikely that similar screening of *content* of communications for the purpose of *combating crime* of child sexual abuse would be found proportionate, let alone with regard to the conduct not constituting criminal offences.

76. It follows from all of the above that the regime of the detection order with regard to interpersonal communications entail a serious risk of exceeding the limits of what is appropriate and necessary in order to meet the legitimate objectives pursued, and therefore of failing to comply with the principle of proportionality.

## IV. CONCLUSION

77. The CLS concludes that, in the light of the case law of the Court of Justice at this stage, the regime of the detection order, as currently provided for by the proposed Regulation with regard to interpersonal communications, constitutes a particularly serious limitation to the rights to privacy and personal data protection enshrined in Article 7 and 8 of the Charter.

78. Such regime entails a serious risk of:

a) not being sufficiently clear, precise and complete, notably in view of the expected intensity of the judicial review of a measure interfering with fundamental rights, and therefore as not being in compliance with the requirement that the limitations to the fundamental rights must be provided for by law as regards the points referred to in paragraphs 20 to 26;

b) compromising the essence of the above-mentioned fundamental rights in so far as it would permit generalised access to the content of interpersonal communications, or, in the alternative;

c) not being in compliance with the proportionality requirement in so far as

– it would require the general and indiscriminate screening of the data processed by a specific service provider, and apply without distinction to all the persons using that specific service, without those persons being, even indirectly, in a situation liable to give rise to criminal prosecution;

– it would not concern traffic and location data, but the content of interpersonal communications;

– it would pursue the general objective of fighting child sexual abuse crimes which, although they are serious crimes, do not constitute threats to national security.

79. If the Council were to decide to maintain interpersonal communications within the scope of the regime of the detection order, the regime should be targeted in such a way that it applies to persons in respect of whom there are reasonable grounds to believe that they are in some way involved in, committing or have committed a child sexual abuse offence, or have a connection, at least indirectly, with the commission of sexual abuse offences. Furthermore, the draft Regulation should provide more detailed and substantive elements with respect to the technology to be used and the extent of limitations to fundamental rights that it could entail, as well as further precisions concerning the conditions for issuance of a detection order and related possible safeguard measures.