19 October 2023

Legal opinion
commissioned by MEP Patrick Breyer, member of the Greens/EFA Group in the European Parliament

CHRISTOPHER VAJDA KC

RE:

THE 2022 PROPOSAL FOR AN EU REGULATION LAYING DOWN RULES TO PREVENT AND COMBAT CHILD SEXUAL ABUSE

OPINION

Introduction and summary of advice

1. I am asked to advise on the lawfulness of the provision on "detection orders" ("DOs") in the Commission's proposal dated 11 May 2022 for a Regulation ("the Regulation") laying down rules to prevent and combat child sexual abuse material ("CSAM"). This Opinion is divided into the following sections:
    a. Section A summarises the material aspects of the Regulation;
    b. Section B situates the Regulation within its factual context and considers how it may apply in practice;
    c. Section C summarises the conclusions of an Opinion from Professor Colneric regarding the Commission's proposed Regulation in 2020[1] to tackle child sexual abuse online; and
    d. Section D contains my legal analysis of the Regulation.

2. In summary, my conclusion is that the provision for DOs in the Regulation is likely to infringe Articles 7 and 8 of the EU Charter of Fundamental Rights ("the Charter"). Once a DO is made under the Regulation, the providers against whom the order has been made must implement a system of general and indiscriminate monitoring of extremely sensitive data, including the content of communications which may then be retained. Although much of this data may be illegal, there is no certainty that all of it will be. The

[1] This subsequently became 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 ("the 2021 Regulation").

general principle, as laid down by the CJEU, is that general and indiscriminate monitoring of data is only permitted in national security contexts. While the developing case law of the CJEU may provide a derogation from this general principle in a case where the data does not enable one to draw precise conclusions about a person's private life, I do not think such a derogation would be applicable to the Regulation. The Regulation enables the content of communications to be monitored which will inevitably enable precise conclusions to be drawn about a person's private life and also removes the safeguards of end-to-end encrypted communications. Yet the Regulation and the accompanying Explanatory Memorandum are silent on the justification for the removal of encryption, its feasibility and effectiveness, and any knock on effects on other networks which are not yet subject to a DO. Given the significance of such an interference with the right to privacy and data protection, the failure of the Regulation in these respects leads me to conclude that the provision for DOs in the Regulation is 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.

Section A: The Regulation

3. Article 1 of the Regulation provides:

"This Regulation lays down uniform rules to address the misuse of relevant information society services for online child sexual abuse in the internal market.

It establishes, in particular:

(a) obligations on providers of relevant information society services to minimise the risk that their services are misused for online child sexual abuse;

(b) obligations on providers of hosting services and providers of interpersonal communication services to detect and report online child sexual abuse;

(c) obligations on providers of hosting services to remove or disable access to child sexual abuse material on their services;

(d) obligations on providers of internet access services to disable access to child sexual abuse material;

(e) rules on the implementation and enforcement of this Regulation, including as regards the designation and functioning of the competent authorities of the Member

States, the EU Centre on Child Sexual Abuse established in Article 40 ('EU Centre') and cooperation and transparency." (emphasis added)

4. Article 1 makes clear that the Regulation is implementing a number of obligations. I am instructed to consider the issue of detection orders. The detection obligations are set out at section 2, at Articles 7-9.
5. The relevant definitions are set out at Article 2. Insofar as is relevant, they are as follows:

(a) 'hosting service' means an information society service as defined in Article 2, point (f), third indent, of Regulation (EU) .../... [on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC];

(b) 'interpersonal communications service' means a publicly available service as defined in Article 2, point 5, of Directive (EU) 2018/1972, including services which enable direct interpersonal and interactive exchange of information merely as a minor ancillary feature that is intrinsically linked to another service;

(c) 'software application' means a digital product or service as defined in Article 2, point 13, of Regulation (EU) .../... [on contestable and fair markets in the digital sector (Digital Markets Act)];

(d) 'software application store' means a service as defined in Article 2, point 12, of Regulation (EU) .../... [on contestable and fair markets in the digital sector (Digital Markets Act)];

(e) 'internet access service' means a service as defined in Article 2(2), point 2, of Regulation (EU) 2015/2120 of the European Parliament and of the Council49;

(f) 'relevant information society services' means all of the following services: (i) a hosting service;

(ii) an interpersonal communications service;

(iii) a software applications store;

(iv) an internet access service.

...

(h) 'user' means any natural or legal person who uses a relevant information society service;

(i) 'child' means any natural person below the age of 18 years;

(j) 'child user' means a natural person who uses a relevant information society service and who is a natural person below the age of 17 years;

(k) ...

(l) 'child sexual abuse material' means material constituting child pornography or pornographic performance as defined in Article 2, points (c) and (e), respectively, of Directive 2011/93/EU;

(m) 'known child sexual abuse material' means potential child sexual abuse material detected using the indicators contained in the database of indicators referred to in Article 44(1), point (a);

(n) 'new child sexual abuse material' means potential child sexual abuse material detected using the indicators contained in the database of indicators referred to in Article 44(1), point (b);

(o) 'solicitation of children' means the solicitation of children for sexual purposes as referred to in Article 6 of Directive 2011/93/EU;

(p) 'online child sexual abuse' means the online dissemination of child sexual abuse material and the solicitation of children".

(i) What does a DO require?

6. Article 7 concerns the power to issue a DO and materially provides:

"1. The Coordinating Authority of establishment shall have the power to request the competent judicial authority of the Member State that designated it or another independent administrative authority of that Member State to issue a detection order requiring a provider of hosting services or a provider of interpersonal communications services under the jurisdiction of that Member State to take the measures specified in Article 10 to detect online child sexual abuse on a specific service."

7. Article 10 sets out what a DO requires of providers of hosting services ("Providers"). It states in material part:

"1. Providers of hosting services and providers of interpersonal communication services that have received a detection order shall execute it by installing and operating technologies to detect the dissemination of known or new child sexual abuse material

or *the solicitation of children, as applicable, using the corresponding indicators provided by the EU Centre in accordance with Article 46."* (emphasis added)

8. Article 10(2) states that Providers will have access, free of charge, to technology to implement the detection orders from the EU Centre in accordance with Article 50(1), but there is no requirement to use any specific technology provided the technology that is used meets the requirements set out in Article 10.

9. Article 10(3) sets out the relevant technological requirements:
   "The technologies shall be:
   (a) effective in detecting the dissemination of known or new child sexual abuse material or the solicitation of children, as applicable;
   (b) not be able to extract any other information from the relevant communications than the information strictly necessary to detect, using the indicators referred to in paragraph 1, patterns pointing to the dissemination of known or new child sexual abuse material or the solicitation of children, as applicable;
   (c) 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 private and family life, including the confidentiality of communication, and to protection of personal data;
   (d) sufficiently reliable, in that they limit to the maximum extent possible the rate of errors regarding the detection."

10. Article 7(8) provides *inter alia* that those requesting the issuance of a DO (or those issuing it) "*shall target and specify it*", thereby ensuring that "*where [the significant risk of the service being used for the purpose of online child sexual abuse] is limited to an identifiable part or component of a service, the required measures are only applied in respect of that part or component*." Recital 23 specifies this as "*a limitation to an identifiable part or component of the service where possible without prejudice to the effectiveness of the measure, such as specific types of channels of a publicly available interpersonal communications service, or to specific users or specific groups of users, to the extent that they can be taken in isolation for the purpose of detection*."

11. Although the issue of end-to-end encryption is central to the legal analysis of the Regulation and its compliance with the Charter[2], it is addressed only once, at recital 26, which provides:

"The measures taken by providers of hosting services and providers of publicly available interpersonal communications services to execute detection orders addressed to them should remain strictly limited to what is specified in this Regulation and in the DOs issued in accordance with this Regulation. In order to ensure the effectiveness of those measures, allow for tailored solutions, remain technologically neutral, and avoid circumvention of the detection obligations, those measures should be taken regardless of the technologies used by the providers concerned in connection to the provision of their services. Therefore, this Regulation leaves to the provider concerned the choice of the technologies to be operated to comply effectively with DOs and should not be understood as incentivising or disincentivising the use of any given technology, provided that the technologies and accompanying measures meet the requirements of this Regulation. That includes the use of end-to-end encryption technology, which is an important tool to guarantee the security and confidentiality of the communications of users, including those of children. When executing the DO, providers should take all available safeguard measures to ensure that the technologies employed by them cannot be used by them or their employees for purposes other than compliance with this Regulation, nor by third parties, and thus to avoid undermining the security and confidentiality of the communications of users". (emphasis added).

12. This recital is to be contrasted with the current position as set out in the 2021 Regulation which does not mandate nor indeed permit interference with end-to-end encryption. The reason for this is explained in recital 25 which provides: *"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."*

[2] See further sections D(2) to (5) below.

13. The absence of this, or equivalent, language in recital 26 suggests that the Regulation is no longer preserving end-to-end encryption. Indeed the conclusion that I draw from the change in these recitals is that, unlike the 2021 Regulation, the Regulation does not preclude interference with end-to-end encryption This reading is supported by the Impact Assessment Report ("IAR"), which states that the obligation is to detect CSAM "*regardless of the technology used in online exchanges*".[3] The Commission goes on to state that it discarded the option of limiting the obligations to unencrypted services because such legislation would not be effective in achieving the Commission's objectives and may in fact detract from those objectives by "*unintentionally creating an incentive for certain providers to use technologies in their services to avoid the new legal obligations, without taking effective measures to protect children on their services and to stem the dissemination of CSAM*."[4]

14. In summary, a DO would impose a wide-ranging monitoring obligation on the Provider subject to the DO.[5] That general monitoring obligation is subject to the restrictions set out at Article 10(4) and 10(5).

15. Article 10(4) requires Providers to ensure that the measures it takes are for the sole purpose of complying with the DO and go no further than necessary, and that the decision-making is not entirely autonomous. Those obligations are to:

    (a) take all the necessary measures to ensure that the technologies and indicators, as well as the processing of personal data and other data in connection thereto, are used for the sole purpose of detecting the dissemination of known or new child sexual abuse material or the solicitation of children, as applicable, insofar as strictly necessary to execute the detection orders addressed to them;

[3] See page 73.

[4] See page 83 of the IAR. Cf further discussion of encryption at page 194. "*Safeguards would therefore also include not to generally weaken encryption and to ensure a high level of information security*".

[5] See Joint Opinion 4/2022 of the EDPB-EDPS of 28 July 2022 on the Regulation ("the Joint Opinion"): "In all three types of detection orders …, the technologies currently available rely on the automatic processing of content data of all affected users. The technologies used to analyze the content are often complex typically involving the use of AI. …the EDPB and EDPS consider that, in practice, the proposal could become the basis for de facto generalized and indiscriminate scanning of the content of virtually all types of electronic communications of all users in the EU/EEA. " (§§52 and 55). The same point is made by the EDRi position paper dated 19 October 2022 ("the EDRi Paper") which states "since it is impossible to differentiate between criminal content and legitimate content without analysing it, all content needs to be included in the assessment. such an order will thus constitute a "general monitoring obligation" which is unlawful, §3.4 at p.30.

(b) establish effective internal procedures to prevent and, where necessary, detect and remedy any misuse of the technologies, indicators and personal data and other data referred to in point (a), including unauthorized access to, and unauthorised transfers of, such personal data and other data;

(c) ensure regular human oversight as necessary to ensure that the technologies operate in a sufficiently reliable manner and, where necessary, in particular when potential errors and potential solicitation of children are detected, human intervention;

(d) establish and operate an accessible, age-appropriate and user-friendly mechanism that allows users to submit to it, within a reasonable timeframe, complaints about alleged infringements of its obligations under this Section, as well as any decisions that the provider may have taken in relation to the use of the technologies, including the removal or disabling of access to material provided by users, blocking the users' accounts or suspending or terminating the provision of the service to the users, and process such complaints in an objective, effective and timely manner;

(e) inform the Coordinating Authority, at the latest one month before the start date specified in the detection order, on the implementation of the envisaged measures set out in the implementation plan referred to in Article 7(3);

(f) regularly review the functioning of the measures referred to in points (a), (b), (c) and (d) of this paragraph and adjust them where necessary to ensure that the requirements set out therein are met, as well as document the review process and the outcomes thereof and include that information in the report referred to in Article 9(3)."

14. There are also obligations in place designed to ensure that users are informed about the Providers' obligations under DOs (see Article 10(5)).

(ii) What are the reporting obligations?

15. The reporting obligations at Articles 12 and 13 require Providers to report any information indicating potential online child sexual abuse on its services.

16. Article 12(1) provides that where a Provider becomes aware "*in any manner other than through a removal order issued in accordance with this Regulation of any information*

indicating potential online child sexual abuse on its services, it shall promptly submit a report thereon to the EU Centre in accordance with Article 13."

17. Article 13 sets out the details which the report "*shall include*". These details are as follows:

> *"(a) identification details of the provider and, where applicable, its legal representative;*
>
> *(b) the date, time stamp and electronic signature of the provider;*
>
> *(c) all content data, including images, videos and text;*
>
> *(d) all available data other than content data related to the potential online child sexual abuse; (e) whether the potential online child sexual abuse concerns the dissemination of known or new child sexual abuse material or the solicitation of children;*
>
> *(f) information concerning the geographic location related to the potential online child sexual abuse, such as the Internet Protocol address;*
>
> *(g) information concerning the identity of any user involved in the potential online child sexual abuse;*
>
> *(h) whether the provider has also reported, or will also report, the potential online child sexual abuse to a public authority or other entity competent to receive such reports of a third country and if so, which authority or entity;*
>
> *(i) where the potential online child sexual abuse concerns the dissemination of known or new child sexual abuse material, whether the provider has removed or disabled access to the material;*
>
> *(j) whether the provider considers that the report requires urgent action;*
>
> *(k) a reference to this Regulation as the legal basis for reporting."*

18. The reporting obligations therefore require the reporting of personal data including *inter alia* the relevant IP address, identity of the user involved, and all content data.

(iii) Who can make a DO?

19. Article 25 establishes Coordinating Authorities for child sexual abuse issues. Member States must designate one or more competent authorities responsible for the application and enforcement of the Regulation (see Article 25(1)). That Coordinating Authority shall

be responsible for all matters related to the application and enforcement of the Regulation in the Member State concerned (see Article 25(2)). There are certain requirements (concerning *inter alia* independence) as to who can be a Coordinating Authority, these requirements are in Article 26.

20. As described in more detail below, Coordinating Authorities can investigate whether a DO is needed and request that one be made if they consider that the legal conditions are met, but a Coordinating Authority cannot make a DO itself. A DO can only be made either by a judicial authority or an independent administrative authority specified by the Member State (see Article 7(4)).

(iv) In what circumstances can a DO be made?

21. Pursuant to Article 7(2), a DO cannot be made until the Coordinating Authority has investigated and assessed whether the conditions in Article 7(4) are met. Further, the DO cannot be made unless the competent judicial authority or independent administrative authority considers that the conditions in Article 7(4) are met. There are two conditions:

> *"(a) there is evidence of a significant risk of the service being used for the purpose of online child sexual abuse, within the meaning of paragraphs 5, 6 and 7, as applicable;*
>
> *(b) the reasons for issuing the detection order outweigh negative consequences for the rights and legitimate interests of all parties affected, having regard in particular to the need to ensure a fair balance between the fundamental rights of those parties."* (emphasis added).

22. Paragraphs 5, 6 and 7 referred to in Article 7(4)(a), provides that the "*significant risk"* exists despite any voluntary mitigation measures taken by the Provider or which the Provider will take.

23. A DO in respect of the dissemination of known or new CSAM shall not exceed 24 months, and DOs concerning the solicitation of children cannot exceed 12 months (Article 7(9)).

24. The Regulation specifies the contents and template of DOs (see Article 8(1)), and also makes provision for the right to challenge a DO before the courts (see Article 9(1)). That right extends to both Providers and "*users affected by the measures taken to execute [the DO]*".

Section B: the application of the Regulation in practice

25. As I understand it, once a DO is made the Provider is under a legal obligation to install one or more technologies which scan all data passing through that Provider's network and which then extract from that data information pointing to the potential dissemination of known or new CSAM or the grooming of children.

26. A DO order would require a Provider to carry out a two-stage exercise. At the first stage, the Provider is, as I understand it, screening all communications within the scope of the DO in order to identify potential CSAM. This initial screening stage can be regarded as "stage 1". This screening process applies to all communications within the scope of the DO regardless of their individual characteristics. By contrast, the retention of data is limited to data which has been identified as potential CSAM or grooming. This can be regarded as "stage 2". Data which is assessed as suspected CSAM or grooming is then retained for a longer period in order for the Provider to fulfil its reporting obligations.

27. Providers would be required to monitor and retain the information necessary to comply with their reporting obligations, which includes IP addresses and other location information, user identity, and the content of the communications which – in the case of suspected grooming – may include significant exchanges of text. This is clearly highly sensitive data which would reveal the nature of data transmitted online and hence involve a significant interference with an individual's rights to privacy and data protection.

28. The Regulation is not prescriptive as to the technological methods used to implement DOs, nor does it specify the features of the technology it will make freely available to Providers. Therefore, it is not clear from the Regulation itself what technological steps Providers will be required to take under a DO. It is assumed that Providers will use the latest available technology to comply with a DO in the least intrusive manner. If that is the case, I understand that different technologies will be used in order to detect (i) known CSAM; (ii) new CSAM; and (iii) grooming. In respect of (i) and (ii), I understand that the relevant technology will be required to scan images and videos. In the case of (iii), the technology will be required to scan text. The Commission considers that most of this material is

"*manifestly illegal content*" and is therefore to be considered analogously to material that constitutes a copyright infringement or defamation.[6]

29. I set out below my understanding of some of the technologies currently available to implement a DO.

30. 'Hashing' is the most commonly used technology to detect known CSAM. A hash is a unique digital fingerprint. The appropriate authorities hold databases of CSAM material, with each photograph or video in the database being given a 'hash'. Those hashes are made available to Providers. When a photograph or video is transmitted by a user, the Provider can scan that image to identify whether it matches the 'hash' of the known CSAM. If the hash does not match, the data is not retained. The technology does not identify the individuals in the image or video and does not analyse the context.[7]

31. The detection of new CSAM typically relies upon an algorithm which uses indicators to rank the similarity of a new image to pre-existing known images of CSAM. The algorithm thereby identifies the likelihood of an image or video constituting CSAM. As with images of known CSAM, the algorithm is unable to extract any identifying information (such as identity or location data). However since the detection of new content is more complex than the detection of known content it requires systematic human review to ascertain its potential illegality. The accuracy rate is said to lie "significantly above 90%".[8]

32. The detection of grooming typically relies on an algorithm which uses content indicators (e.g. keywords in the conversation) and metadata (e.g. frequency or other patterns in communication to determine any age differences between the users and the likely involvement of a child in the communication) to rank the similarity of an online exchange to online exchanges reliably identified as grooming. The algorithm can thereby determine the likelihood of an online exchange constituting grooming. The classifiers are not able to use the substance of the content of the communication but are solely able to detect patterns which point to possible grooming. The algorithms are unable to extract any other information from the content of the conversation such as identifying specific persons or locations. The accuracy rate is stated to lie around 90%, and the process requires systematic

6 See Box 9 at page 51 of the IAR accompanying the Regulation.
7 See Box 14 at page 71 of the IAR.
8 See Box 16 at pages 78-79 of the IAR. This appears to be based upon an example given at page 282 of the IAR, of Thorn's Safer tool. This is a CSAM detection tool which can be set at a 99.9% precision rate.

human review to ascertain its potential illegality.[9] The source of this figure, namely Microsoft, does not recommend relying on it, as it "*relates to a single English-language technique trained on a small data set of known instances of solicitation within historic text-based communications, and in all cases merely serves to flag potential solicitation for human review and decision as part of a wider moderation process*."[10]

33. As I have already indicated, I proceed on the basis that the Regulation is intended to be broad enough for a DO to impose an obligation on a Provider to break end-to-end encryption.[11] As to whether this is technologically possible to do this, the Joint Opinion has doubts about its effectiveness:

> *"As regards the possibility of circumventing CSAM detection, it should be noted that at present there seems to be no technological solution to detect CSAM that is shared in an encrypted form. Therefore any detection activity - even client-side scanning intended to circumvent end-to-end encryption offered by the provider - can be easily circumvented by encrypting the content with the help of a separate application prior to sending it or uploading it. Thus the detection measures envisaged by the Proposal might have a smaller impact on the dissemination CSAM on the Internet than one might hope for."*[12]

34. In the IAR the Commission has considered potential technological solutions to the application of DOs to end-to-end encrypted services, so as "*not to generally weaken encryption and to ensure a high level of information security"*[13]. A group of experts commissioned by the Commission have considered a number of technological solutions.

35. The group has considered the option of on-device hashing with server side matching, feasible in the short term, rated its compliance with the need to safeguard privacy and security as "*medium-low*":

> "*user data (hashes) are visible to the ESP. The possible security issues (compromise and manipulation of detection tools) may introduce vulnerabilities that could decrease*

---

9 See Box 17 at pages 81-82 of the IAR. See also §41 of the Joint Opinion and pages 282-283 of the IAR providing an example of Microsoft's Project Artemis tool. Microsoft reported that, in its own deployment of this tool in its services, its accuracy was 88%.

10 Microsoft Position Paper on the Regulation, September 2022, page 5.

11 See §§11-13 above.

12 §45.

13 See page 194 of the IAR and consideration of specific technological solutions at pp. 287, and 291-308.

the privacy of the communication. … the hashing algorithm in the device could be subverted and compromised/reverse engineered to not detect or report child sexual abuse (in particular in devices without trusted execution environments). It could also be manipulated to introduce false positives to inundate the reporting systems (e.g. NCMEC) with them. Also, the hash database in the ESP server could be manipulated to introduce non-CSAM hashes. The possible leak of detection tools (e.g. hashing algorithm), could reduce the effectiveness of similar detection tools elsewhere. Also to consider is the possibility that tech-savvy offenders (who may compromise the solution) would not use any system that allows the detection of CSA. These solutions are more likely to be used by non tech-savvy offenders (as is the case of most CSA detected and reported today)."[14]

36. This option is considered, amongst others, to be a promising solution but the group cautioned that some further research was required.[15]

Section C: Professor Colneric's Opinion on the 2021 Regulation

37. In March 2021 Professor Colneric provided an Opinion to those instructing me on the Commission proposal for the 2021 Regulation.[16] Unlike the Regulation, the 2021 Regulation took the form of a derogation from the obligations set out in Directive 2002/58/EC ("the **2002 Directive**"). Specifically, Article 3 of the 2021 Regulation suspended the application of the obligations set out in Article 5(1) and Article 6 of the 2002 Directive.[17]

38. Under Article 5(1) of the 2002 Directive there is an obligation for Member States to ensure the confidentiality of communications through national legislation. The provision prevents listening, tapping, storage and other kinds of interception or surveillance of

[14] See page 296-297 of the IAR.
[15] See page 309 of the IAR.
[16] 10 September 2020, COM (2020) 568, 2020/0259 (COD) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0568&from=EN. This became the 2021 Regulation, see fn. 1 above.
[17] https://edps.europa.eu/sites/edp/files/publication/dir_2002_58_en.pdf

communications. [18] Article 6 of the 2002 Directive concerns '*traffic data'*[19] and provides that it must be erased or made anonymous when it is no longer needed for the purpose of transmission of the communication, unless it is needed for billing, marketing (with consent).

39. Professor Colneric concluded that the 2021 Regulation did not comply with the Charter on the basis that it involved:

> *"the general and indiscriminate screening of all private correspondents for "child pornography". The very content of the communication is affected. Therefore, the interference is at least as serious as the retention and automating analysis of traffic and location data on the basis of the CJEU's case law, it must be concluded that although the purpose is fighting the serious crime of "child pornography", general and indiscriminate screening exceeds the limit of what is strictly necessary*".[20]

Section D: Analysis as to whether the Regulation complies with EU law

(i) Legal Framework: the Charter and CJEU case law

40. The relevant Charter rights are as follows.

a. Article 7: Respect for private and family life, which provides "*everyone has the right to respect for his or her private and family life, home and communications*".

b. Article 8: Protection of personal data, which provides:

---

[18] "*Member states shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality"* (emphasis added).

[19] Defined at Article 2(b) of the 2002 Directive as "*any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof*".

[20] Page 29. She relied in particular on the judgment of the CJEU in Joined Cases C-511 and 512/18 *La Quadrature du Net* (*" Quadrature 1")* EU:C:2020:791
which interprets the Charter as laying down a general prohibition on general and indiscriminate monitoring of traffic and location data emanating from electronic communications other than for the purposes of national security, a concept that does not extend to the detection of child sexual material, see §§134-151 and 172-181.

"1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

c. Article 11: Freedom of expression and information, which provides:

"1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

2. The freedom and pluralism of the media shall be respected."

d. Article 24: The rights of the child, which provides:

"1. Children shall have the right to such protection and care as is necessary for their well-being. ...

2. In all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration."

41. Article 52 sets out the scope and interpretation of rights and principles. It provides:

"1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. 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."

42. In *Digital Rights Ireland*[21] the CJEU considered a claim brought by Digital Rights challenging the lawfulness of an EU Directive which required telephone communications service providers to retain traffic and location data (but not the content of the communication) for a specified period in order to prevent, detect, investigate and prosecute crime and safeguard national security. This data was considered by the CJEU to be wide-

[21] Joined Cases C-293/12 and C-594/12 EU:C2014:238

ranging, as it observed at: "*those data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period."*[22] The Court concluded that this type of data, taken as a whole, may allow very precise conclusions to be drawn about the private lives of the individuals concerned.[23] The Court therefore had little difficulty in finding an interference with the right to privacy and data protection in Articles 7 and 8 respectively of the Charter which it termed to be "*wide-ranging, and … particularly serious*".[24]

43. In reviewing the proportionality of this interference the CJEU stressed that the extent of the EU legislature's discretion was limited and the review of that discretion by the Court was strict:

> *"With regard to judicial review of compliance with those conditions, where interferences with fundamental rights are at issue, the extent of the EU legislature's discretion may prove to be limited, depending on a number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference (see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, § 102, ECHR 2008-V).*
>
> *In the present case, in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by Directive 2006/24, the EU legislature's discretion is reduced, with the result that review of that discretion should be strict."*[25]

22 §26.
23 §27.
24 §37.
25 §§47-48.

44. Applying this test, the Directive failed the proportionality element of the assessment. The reason was that the Directive applied to a wide-range of electronic communication mechanisms, was wholesale in its application to them, and to "*all subscribers and registered users… it therefore entails an interference with the fundamental rights of practically the entire European population"*.[26] The application of the Directive "*in a generalized manner… without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime"*[27] indicated that the Directive went beyond that which was necessary to pursue its legitimate objective.

45. Subsequently the CJEU had the opportunity in *Quadrature 1* to consider once again the lawfulness of monitoring and retention of various elements of electronic communications for different purposes. This case concerned the processing of traffic and location data (but again not the content of the communication), which the Court noted:

> *"may reveal information on a significant number of aspects of the private life of the persons concerned, including sensitive information such as sexual orientation, political opinions, religious, philosophical, societal or other beliefs and state of health, given that such data moreover enjoys special protection under EU law. Taken as a whole, that data may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. In particular, that data provides the means of establishing the profile of the individuals concerned…"*[28]

46. The judgment specifically considered the sensitivity of retaining IP addresses of the source (as opposed to recipient) of the communication, at §§152-154, which the CJEU considered to be less sensitive than other traffic data:

> *"152. It should be noted that although 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*

---

26 §56.
27 §57.
28 §117.

the terminal equipment from which an Internet communication is made. Thus, in relation to email and Internet telephony, provided that only the IP addresses of the source of the communication are retained and not the IP addresses of the recipient of the communication, those addresses 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.

153. However, since IP addresses may be used, among other things, to track an Internet user's complete clickstream and, therefore, his or her entire online activity, that data enables a detailed profile of the user to be produced. Thus, the retention and analysis of those IP addresses which is required for such tracking constitute a serious interference with the fundamental rights of the Internet user enshrined in Articles 7 and 8 of the Charter, which may have a deterrent effect as mentioned in paragraph 118 of the present judgment.

154. In order to strike a balance between the rights and interests at issue as required by the case-law cited in paragraph 130 of the present judgment, account must be taken of the fact that, where an offence is committed online, the IP address might be the only means of investigation enabling the person to whom that address was assigned at the time of the commission of the offence to be identified."(emphasis added).

47. For present purposes, the relevant conclusions of the CJEU were as follows:

a. the retention of all traffic and location data constitutes a serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. Such an interference, if for the purpose of safeguarding national security, in a situation where there is a serious threat to national security, is lawful provided that certain conditions were met (§§139-140);

b. the retention of traffic and location data, for the purpose of combatting serious crime and preventing serious threats to public security, is permitted provided that the retention of such data is "targeted" with respect to the categories of data to be retained (§§146-147);

c. In other words, unlike in the case of a genuine and present or foreseeable threat to national security, there can be no general, non-targeted, retention of traffic and location data where combating serious crime is concerned. The retention must be limited to data that is likely to reveal a link, whether direct or indirect,

with serious criminal offences, to contribute in one way or another to combating serious crime or to preventing a risk to public security or a risk to national security (§141, 143);

d. the retention of source IP addresses and data relating to civil identity of all users of electronic communication systems for the purposes of preventing, investigating, detecting and prosecuting criminal offences and safeguarding public security was permitted (§155);

e. the automated analysis of traffic and location data (which is independent of the subsequent collection and retention of data and was described by the Court as corresponding in essence to screening) is a particularly serious interference with the rights in Articles 7 and 8 of the Charter and is permitted 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 again subject to certain conditions being met (§§172-177); and

f. The real-time collection of traffic and location data is also a particular serious infringement with the rights in Articles 7 and 8 of the Charter and is permitted only in respect a persons whom there is a valid reason to suspect that they are involved in one way or another in terrorist activities (§§184-188).

48. On three subsequent occasions the CJEU, in Grand Chamber, has refused to depart from *Quadrature 1*.

49. The first two cases raised the question of whether an individual can seek to quash a criminal conviction on the basis that the national law permitting the use of traffic and location data by the prosecution did not meet the CJEU's test for the lawful retention of data. In *Prokuratuur/HK*[29] the CJEU considered that retention of this data enabled one to draw precise conclusions on the private life of a user of electronic communications and it was therefore precluded by EU law[30]. The next case, *GD*[31] concerned the use of electronic location data in criminal proceedings leading to a conviction for murder. The Irish Supreme Court considered that, "*only the general and indiscriminate retention of traffic and location data allows serious crime to be combated effectively, which the targeted and*

[29] Case C-746/18, EU:C:2021:152.
[30] §§35-36.
[31] Case C-140/20, EU:C:2022:258.

expedited retention (quick freeze) of data does not make possible."[32] Nevertheless, the CJEU again refused to modify the approach it had laid down in *Quadrature 1*. The CJEU considered that the combination of permissible measures in *Quadrature 1*, namely targeted and expedited retention together with data relating to the civil identity of users and IP addresses should be sufficient for an effective criminal investigation.

50. On the third occasion, in September 2022 in *Spacenet*,[33] the CJEU gave judgment on a reference from the Federal Administrative Court in Germany on a dispute between telecommunication providers who objected to German legislation requiring them to retain traffic and location data relating to their customers. The German court pointed out that the ambit of data retained was less than in previous cases decided by the CJEU, the period of retention was short (four and ten weeks for location and traffic data respectively). It also referred to the case law of the European Court of Human Rights ("ECtHR") which had held that Article 8 of the ECHR did not preclude national provisions providing for the bulk interception of cross-border flows of data in view of the large number of threats that states faced from terrorists and organised crime. Nevertheless, the CJEU once again reaffirmed its approach in *Quadrature* 1 and subsequent cases.

51. However, a few months before deciding *Spacenet*, in April 2022, in *Poland v. Commission*[34] the CJEU held that the liability imposed by Directive 2019/790 on online content-sharing service providers for any acts of unauthorized communications of copyrighted works to the public was not contrary to the freedom of expression laid down in Article 11 of the Charter. This was, in essence, on the basis that the imposition of such a liability struck a fair balance between, on the one hand, the right to freedom of expression and information of users of content-sharing services and, on the other hand, the right to intellectual property which itself is protected under the Charter. In reaching its conclusion in that case the Court did not, however refer to the *Quadrature 1* line of cases.

52. In June 2022 in *Ligue des droits humains*[35] the CJEU had to consider the legality of Directive 2016/681, on the transfer by air carriers of passenger name record ("PNR") data, with Articles 7 and 8 of the Charter. Such PNR data had to be transferred to public

---

32 §26.
33 Joined Cases C-793/19 and 794/19, EU:C:2022:702.
34 Case C-411/19, EU:C:2022:297.
35 Case C-817/19, EU:C:2022:491.

authorities for screening against automated processing based on pre-determined models and criteria. The system of transfer of data was mandatory for extra-EU flights and permissive for intra-EU flights. The CJEU held that the Directive introduced "*a surveillance regime that is continuous, untargeted and systematic, including the automated assessment of the personal data of everyone using air transport services*".[36] This was an interference with rights guaranteed under Articles 7 and 8 of the Charter. The Court considered such an interference was justified as it observed the principle of legality and respect for the essence of the fundamental rights in question, it pursued an objective of general interest (the lives and safety of passengers), and the interference was necessary for extra-EU flights (the data was to be processed for the purpose of combating terrorist offences and serious crime). Among the offences listed in the Directive are "*the sexual exploitation of children and child pornography*", which were considered by the Court to be "*inherently and indisputably extremely serious*."[37] However, the CJEU relied on the distinction it had drawn in *Quadrature 1* between terrorist threats and serious criminal offences to conclude, in respect of intra-EU flights, that the indiscriminate application by a Member State of the transfer of data in respect of the intra EU flight "*would not be considered to be limited to what is strictly necessary*."[38]

53. In Case C-470/21 *La Quadrature du Net* (" *Quadrature 2*"), which is currently before the CJEU, the Court has to consider the lawfulness under the Charter of the right of an administrative authority, which is responsible for protecting copyright online, to have access to civil identity data, corresponding to source IP addresses, so that the authority can identify the holders of those addresses suspected of an infringement and if necessary take the necessary action. The Advocate General ("AG") delivered his first Opinion on 27 October 2022 ("AG1") in which he concluded:

    a. Articles 7, 8 and 11 of the Charter are not absolute rights, rather the CJEU must strike a balance between the various legitimate interests and rights at issue (§§59-60);
    b. The CJEU has drawn a distinction between - on the one hand - interferences resulting from access to data which by itself provides precise information on communications and therefore on the private life of the individuals concerned,

[36] §111.
[37] §149.
[38] §173.

and – on the other hand – interferences resulting from access to data which may provide such information only if it is viewed in combination with other data such as IP addresses. The rules on retention are stricter in the former case than in the latter (§62).

c. It is relevant that where offences are committed online, IP addresses may be the only means of identifying the perpetrator (§65). Accordingly, in cases concerning serious crime, serious threats to public security and national security, the general and indiscriminate retention of IP addresses assigned to the source of a connection is not unlawful provided strict conditions are met (§66).

d. By restricting the indiscriminate, untargeted retention of IP addresses to combat serious crime, the CJEU ruled out the ability to retain IP addresses to combat crime in general – irrespective of whether the retention of IP addresses is the only way to combat such general crime perpetrated online. The consequence of this is that "*a whole range of criminal offences may evade prosecution entirely*", risking *"systemic impunity for offences committed exclusively online"* (§§79-81).

e. A "*readjustment*" of the relevant case law was proposed but without prejudice to the well-established requirements that the retention of the data must be proportionate, limited to that which is strictly necessary, and be accompanied by appropriate safeguards (§§83-89).

f. This *"readjustment"* of the relevant case law would permit the general and indiscriminate retention of IP addresses assigned to the source of the connection for a strictly limited period of time for the purposes of preventing, investigating, detecting, and prosecuting online criminal offences for which the IP address is the only means by which individuals who commit crime online can be identified (§§83, 94, 105).

54. Following AG1 the CJEU decided to transfer the case from the Grand Chamber to the Full Court. There has been another oral hearing and the AG delivered his second Opinion ("AG2") on 28 September 2023. He maintained the conclusion reached in AG1. He focused on two issues, proportionality and adequate material and procedural guarantees.

55. As regards proportionality, his key points were:

a. Access to a person's IP address does not enable one to draw very precise conclusions about that person's private life[39],

b. The monitoring taking place is not of the activity of all users of peer-to-peer networks but only that of persons uploading infringing files[40],

c. Hence it is not a serious interference with fundamental rights as it does not result in the exhaustive tracking of the user's click stream and in very precise conclusions being drawn about that person's private life[41], and

d. Where the offence is committed exclusively online, the IP address may be the only means of investigation enabling the person to whom that address was assigned at the time of the commission of the infringement to be identified[42].

56. As regards adequate material and procedural guarantees, a prior review by a court or independent administrative body is not a systematic requirement but depends on a comprehensive analysis of the measure in issue in which both the seriousness of the interference which it entails and the guarantees which it provides are taken into account.[43]

57. AG2 summarised his approach as a "*necessary and limited development of the case law*" where obtaining the civil identity data corresponding to an IP address is the only means of identifying a copyright infringement and added that "*the risk of systematic impunity is not limited to infringements of copyright committed on peer-to-peer networks, but ... extends to all offences exclusively committed online*."[44] The AG also considered that such a solution enabled one to reconcile two lines of case law, namely, on the one hand, the case law relating to the retention of and access to the data and, on the other hand, the case law relating to the disclosure IP addresses assigned to the source of a connection in actions to enforce the protection of IP rights brought by private individuals.[45] Nevertheless he emphasized that this approach did not amount to "*reconsidering the Court's case-law*".[46]

---

39 §50.
40 §53
41 §§55-57.
42 §§58-62.
43 §§65-77.
44 §81. Albeit at §§83-84 the AG appeared to accept that there were other ways to identify the perpetrators of online offences but that they would entail a greater interference with a person's fundamental rights as they would allow very precise conclusions to be drawn about that person's private life.
45 §85.
46 §88.

On this basis AG1 and AG2 should be seen as distinguishing *Quadrature 1* from the facts in *Quadrature 2*.

(ii) Analysis

58. The stated aim of the Regulation is to fight effectively against child sexual abuse. Legitimate aims, as recognized by Article 52(1) of the Charter, can either be (i) objectives of general interest recognized by the Union or (ii) the need to protect the rights and freedoms of others. Professor Colneric's Opinion (pages 20-21) cogently sets out why the effective fight against child sexual abuse satisfies both (i) and (ii). I fully agree with that analysis and do not repeat it here. The key questions are therefore:
    (1) Does the DO regime constitute an interference with the right to privacy and data protection in Articles 7 and 8 of the Charter and how serious is any such interference?
    (2) Is the DO regime provided by law?
    (3) Does the DO regime constitute a proportionate means of meeting the legitimate aims of the Regulation?
    (4) Does the DO regime respect the essence of the rights under Articles 7 and 8 of the Charter?
    (5) Is the Regulation, in the context of the application of DOs to encryption, properly reasoned and compliant with the principle of legal certainty?

    (1) <u>Does the DO regime constitute an interference with the right to privacy and data protection in Articles 7 and 8 of the Charter and how serious is any such interference?</u>

59. In order to comply with the screening and monitoring obligations imposed by a DO[47], a Provider will be obliged to install, as yet unspecified, technology to detect CSAM on its network. Such an order would cover not only metadata, such as traffic and location data, but the actual content of electronic communications and indeed may require the Provider to break encrypted communications.[48]

[47] See §§7-18 and 25-36 above.
[48] See §§11-13 above.

60. No one disputes that these obligations on a Provider would constitute an interference within the meaning of Articles 7 and 8 Charter of the private lives and personal data of all individuals using that Provider's services.

61. Nor can there be any doubt that the level of interference would go far beyond the data that has been considered by the CJEU so far, such as traffic and location data in the telecommunication cases from *Digital Rights* to *Spacenet*, IP addresses in *Quadrature 1 and 2*, and PNR data in *Ligue*. By contrast a DO may well require monitoring the actual content of all electronic communications made by every user of that Provider's electronic communications network, including encrypted communications.

62. Thus, on any view, this would be an extremely serious interference with the rights to privacy and data protection of all such users.

(2) Is the DO regime provided by law?

63. The first question that arises here is whether the requirement that any limitation on the exercise of the right recognized by the Charter "*must be provided for by the law*" encompasses the primary act which provides for the limitation, rather than just the individual decision which is adopted pursuant to the primary act. Thus, in terms of the present case, does one look at both the Regulation or just the DO? The answer is that it is necessary to look at both.[49]

64. The second question is what does the term "*provided for by the law*" require in terms of the precision of the law. The test is as follows:

[49] See C-311/18 *Facebook Ireland and Schrems*, EU:C:2020:559 "*the requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned (Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 139 and the case-law cited).*" (emphasis added), §175 and *Quadrature 1,* §175. See also *Poland v Council* at §67. This approach is also consistent with the approach taken by the European Court of Human Rights, see *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria***,** no. 62540/00, 28 June 2007. The primary legislation there was the Special Surveillance Means Act 1997. It permitted surveillance to be used where necessary to prevent or uncover serious offences if the required intelligence could not be obtained through other means. The primary legislation was held to infringe the "*in accordance with the law"* provision in Article 8 of the ECHR.

"*the legislation which entails an interference with fundamental rights must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose exercise of those rights is limited have sufficient guarantees to protect them effectively against the risk of abuse. That legislation must, in particular, indicate in what circumstances and under which conditions such a measure may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where the interference stems from an automated process*." [50]

65. While the test is clear, its application is less so. Thus in *Poland v Council* the relevant legislation did not define the actual measures that the service providers should adopt in order to avoid liability for unauthorized uploading of copyright material but the CJEU held that the need for clear and precise rules did not preclude a limitation on a fundamental right "*from being formulated in terms which are sufficiently open to be able to keep pace with changing circumstances*."[51] This application of the test is therefore capable of leading to a considerable qualification of the terms "*clear and precise*".

66. On one view, the Regulation could be said to comply the application of this principle as set out in *Poland v Council* on the basis that detection of CSAM is constantly evolving in the light of technological developments. On the other hand, the interference with the rights to privacy and data protection in the present case is much more serious than that of the interference with the right to freedom of expression in *Poland v Council.* In this context, the approach the Regulation adopts towards encryption is, in my view, highly material.

67. There is no doubt that the Commission intends the Regulation to provide a legal basis for breaking encrypted communications. In this respect the Regulation would amount to a complete *volte face* by the EU legislator from the position under the 2021 Regulation.

68. In my view the EU legislator should itself provide guidance as to the circumstances when encrypted communications can be broken. This is a privacy and data protection issue of the highest constitutional importance. It would be inappropriate for this issue to be left by the legislator to the competent authority designated by the Coordinating Authorities to make a DO. A competent authority can either be an administrative body or a judicial

50 *Poland v Council*, §67.
51 §73.

authority.[52] While a DO can apply the principles laid down in the Regulation, on an issue of this importance, it is the legislator that should provide the necessary guidance.

69. I therefore consider that the Regulation does not, in this respect, comply with the "*provided for by the law*" condition. In my view there is an overlap between this requirement and the principle of legal certainty and need to provide sufficient reasoning in the Regulation. For reasons that I set out in section 5 below, I do not consider that the Regulation, on this point, complies with the obligation to give reasons pursuant to Article 296 TFEU or complies with the principle of legal certainty.

(3) Does the DO regime constitute a proportionate means of meeting the legitimate aims of the Regulation?

70. In order to consider whether an interference with rights to privacy and data protection is proportionate, a number of issues are relevant.

71. The first is the degree of interference. Put simply, the greater the interference the greater the need for a justification. As already indicated[53], the imposition of a DO on a Provider, which could include breaking encrypted communications, creates a degree of interference in users' Article 7 and 8 rights, that is very substantial and goes far beyond any interference that has so far been considered by the CJEU. Thus, in this respect the position is different from that in *Poland v Council* and *Quadrature 2* where the interference did not enable one to draw precise conclusions about a person's private life and so a lesser justification for the interference was required.

72. The next issue is whether these very substantial interferences can be justified as being necessary. This involves a consideration both of the effectiveness of such interferences in tackling CSAM online and whether such an objective can be tackled by a measure by which involves a lesser interference. It is to be recalled that where there is a serious interference with the right to privacy and data protection, as in the present case, the legislator's discretion is limited and review by the CJEU is strict.[54]

---

52 See §20 above.
53 See §§11-13 above.
54 See *Digital Rights* §§47-48.

73. The Commission states: *"Despite the fact that the sexual abuse and sexual exploitation of children and child sexual abuse materials are criminalised across the EU… it is clear that the EU is still currently failing to protect children from falling victim to child sexual abuse, and that the online dimension represents a particular challenge."*[55] It goes on, relying on the IAR, to say "*that voluntary actions alone against online child sexual abuse have proven insufficient, by virtue of their adoption by a small number providers only, of the considerable challenges encountered in the context of private-public cooperation in this field, as well as of the difficulties faced by Member States in preventing the phenomenon and guaranteeing an adequate level of assistance to victims*".[56] It considered five options, ranging from non-legislative practical measures (Option A) to imposing a legal obligation on Providers to detect known and new CSAM as well as grooming (Option E).[57] Option E was chosen as "*the option which best achieves the policy objective in an effective and proportionate way, all the while ensuring proportionality through the introduction of rigorous limits and safeguards so as to ensure, in particular, the required fair balance of fundamental rights.*"[58]

74. As regards grooming, the Explanatory Memorandum states:

> " *… detecting 'grooming' would have a positive impact on the fundamental rights of potential victims especially by contributing to the prevention of abuse; if swift action is taken, it may even prevent a child from suffering harm. At the same time, the detection process is generally speaking the most intrusive one for users (compared to the detection of the dissemination of known and new child sexual abuse material), since it requires automatically scanning through texts in interpersonal communications. It is important to bear in mind in this regard that such scanning is often the only possible way to detect it and that the technology used does not 'understand' the content of the communications but rather looks for known, pre-identified patterns that indicate potential grooming. Detection technologies have also already acquired a high degree of accuracy* [Reference is made in footnote 32 to the reported accuracy of the Microsoft grooming detection tool], *although human oversight and review remain necessary, and*

55 The Explanatory Memorandum to the Regulation ("the Explanatory Memorandum"), page 1.
56 See page 9 of the Explanatory Memorandum.
57 See page 10 of the Explanatory Memorandum.
58 See page 11 of the Explanatory Memorandum.

indicators of 'grooming' are becoming ever more reliable with time, as the algorithms learn."[59]

75. The Commission addresses the issue of proportionality in the Explanatory Memorandum. It states:

"The proposed rules only apply to providers of certain types of online services which have proven to be vulnerable to misuse for the purpose of dissemination of child sexual abuse material or solicitation of children (known as 'grooming'), principally by reason of their technical features or the age composition of their typical user base. The scope of the obligations is limited to what is strictly necessary to attain the objectives set out above."[60]

76. The same point is made at recital 23 to the Regulation:

"In addition, to avoid undue interference with fundamental rights and ensure proportionality, when it is established that those requirements have been met and a detection order is to be issued, it should still be ensured that the detection order is targeted and specified so as to ensure that any such negative consequences for affected parties do not go beyond what is strictly necessary to effectively address the significant risk identified."

77. Crucial to the overall effectiveness of the Regulation is not only the types of communication to which it can apply but also whether it is capable of applying to end-to-end encrypted services. However, so far as I can see, the only discussion of this key topic is to be found in the IAR.[61] Given that the IAR is only a Working Document produced by the Commission Services one cannot use this as a basis for determining whether the authors of the Regulation, namely the Council and Parliament, have considered the effectiveness of requiring Providers to break end-to-end encrypted services.

78. In any event even if one has regard to the IAR, this issue has not been fully addressed. For example, if a DO is imposed on a Provider which requires the Provider to break encrypted communications, the likelihood is that distributors of CSAM will migrate to other platforms. Is it therefore intended that all platforms would also be subject to a similar DO?

---

59 See page 14.
60 See page 7.
61 There is nothing in the Regulation (other than recital 26) or the Exploratory Memorandum.

If so, this would mean it would be impossible for any user anywhere in the EU to continue using an encrypted service.

79. In the absence of such an analysis in the Regulation, it is difficult, not to say impossible, for a court to review the effectiveness of policy choice made by the EU legislator and hence its proportionality.[62]

80. In reaching this conclusion, I am mindful of the argument that the problem of the distribution of CSAM is inherently an online problem which can be effectively tackled by not only an obligation of general monitoring arising out of the DO but also opening up encrypted communications. Such an argument finds support from the observations in AG1 and AG2 in *Quadrature 2* that an interference with fundamental rights may be justified if it is strictly necessary to ensure that criminal law cannot be breached with impunity.

81. Nevertheless I do not consider that it can serve as a lawful justification for the monitoring obligations that would be imposed on a Provider following a DO.

82. First, it is to be recalled that the observations of the AG in those Opinions concern a case where the degree of interference in someone's private life was considerably less serious than under the Regulation and, in particular, there was no suggestion of breaking any encrypted communications. In *Quadrature 2* information as to the copyright work did not allow precise conclusions to be drawn about the private life of the person at the origin of such a work being made available.

83. Secondly, the basis of the justification put forward by the AG in *Quadrature 2* was that it was the only way to ensure illegal activity could not be carried out with impunity. However the breadth of a DO would cover activity that goes beyond the detection of criminal activity, particularly as regards grooming material. The definition of CSAM is not dependent on that material being criminal.[63]

84. The third issue under proportionality involves a balancing exercise, namely whether the advantages of the measure outweigh the disadvantages as regards fundamental rights and

---

62 See §§43-44 above.

63 The definition of CSAM in Article 2(l) of the Regulation is by reference to the definition of child pornography or pornographic performance in Article 2(c) and (e) of Directive 2011/93/ EU and not by reference to sexual abuse offences in Article 3.

reconciling different rights and freedoms.[64] In the present case that involves balancing the rights of children against the rights to privacy and data protection.

85. However, in the absence of a proper consideration by the legislator of the feasibility of breaking encryption, its effectiveness, its consequence for electronic networks as a whole, it is impossible for the legislator to carry out the required balancing test and for the CJEU to engage in its strict review of the balance struck by the legislator. As I have indicated[65], it is not, in my view, sufficient that such a balancing exercise is left entirely to an independent administrator or court.

86. For the sake of completeness I now turn to examine other points that have been put forward on proportionality.

87. In the IAR the Commission seeks to distinguish the general monitoring obligation that would be imposed pursuant to a DO from previous cases before the CJEU as it says that the CJEU "*has not yet had to assess a similar obligation with regard to manifestly illegal content such as most CSAM*"[66]. It is true to say that the traffic and location data in issue in *Quadrature 1* was generally not itself manifestly illegal content. Rather the data was wanted in order to be, and was capable of being, used to identify actual or potential illegal activities. By contrast, despite the fact that laws may vary between EU Member States, generally speaking the dissemination of known and new CSAM is likely to be illegal. Nevertheless, as I pointed out above[67], the definition of CSAM is not made by reference to criminal offences.

88. In any event, although the majority of data retained at stage 2 may be manifestly illegal, it is difficult to see how it can justify the general monitoring of all data at stage 1 which includes both manifestly illegal and legal content.

89. In my view it is therefore unlikely that this is a relevant distinction between this case and *Quadrature 1*.

64 See Case C-283/11 *Sky Österreich* EU:C:2013:28, §§58-60.
65 See §68 above.
66 See Box 9 of the IAR at page 51.
67 See §82 above.

90. I have been shown a Note from the Commission services ("the Commission Note") which considers that the data falling within the scope of a DO can be distinguished from the data in *Quadrature 1* because in that case "*the national system involved the retention and automated analysis of certain personal data. That is not an issue under the proposed rules on detection orders, which operate based on a 'hit/not hit' model."*[68] The Commission Note further states that there are "*differences between retention, at issue in that case law and detection, at issue in the case at hand… Although detection can still be intrusive, in the absence of retention… no similar risk exists. That is especially so given that the detection would function on a 'hit/no hit' basis rather than involving any actual analysis."*[69]

91. I am unable to accept this distinction.

92. Whilst a number of the provisions in issue in *Quadrature 1* did concern data retention, the CJEU specifically addressed the lawfulness of a provision which operated on a 'hit/no hit' basis, namely Article L.851-3 of the French Internal Security Code ("CSI"), which provided that operators may be required to implement automated data processing practices designed to "*detect links that might constitute a terrorist threat"*.[70] This provision was expressly considered in the judgment, summarised above.[71] The fact that such processing was independent of any retention did not preclude the CJEU from stating that such interference was "*particularly serious since it covers, generally and indiscriminately, the data of persons using electronic communication systems*".[72] This does not suggest that the interference arising from automatic analysis of all traffic data is less serious where it is not accompanied by retention.

93. Finally, I turn to consider whether the fact that a DO is required before a monitoring obligation is imposed on a Provider means that such a monitoring obligation, which is imposed after an individual consideration of the position of a specific Provider, can be distinguished from the general monitoring obligation considered in *Quadrature 1*. The argument here is that the grant of the DO requires an individual examination by an

---

68 See §29 of the Note dated 16 May 2023 and entitled "*Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse - balancing the rights of children with the users rights*."

69 *Ibid, §*31.

70 Set out at §43 of the Judgment.

71 §§172-177 of the judgment summarised at §47 (e) above.

72 §174.

independent person of whether the two conditions in Article 7(4) are satisfied and thus any monitoring obligation imposed pursuant to a DO cannot be equated to the indiscriminate and general monitoring obligations, as condemned by the CJEU in *Quadrature 1*.[73]

94. However, once a DO is in place, a Provider will be subject to an obligation to indiscriminately monitor the data of potentially all users on his network, whether or not those users constitute any form of risk of dissemination of CSAM.

95. The Commission further argues that the "*significant risk*" requirement as a pre-condition for the making of a DO relates to a "digital space" that is in effect analogous to a geographical space where targeted measures may be permitted. It is to be recalled that for such targeted measures to be permitted, the Court referred not only to a geographical area characterised by "*a high risk of preparation for or commission of serious criminal offences*" in that area but also reiterated that "*there can be no question of reinstating, by [the means of targeted data retention], the general and indiscriminate retention of traffic and location data*." While the CJEU was there addressing the issue of retention, rather than the monitoring, of data, there is nothing in in *Quadrature 1* to suggest that the same analysis does not apply to the monitoring of data. Thus, when analysing the automated screening of all traffic and location data in *Quadrature 1* (which did not involve retention) the CJEU did not suggest that it could be justified by reference to any broader form of targeting than permitted for retention of data. Accordingly, any form of targeting, whether for monitoring or retention, must take place exceptionally, not as a rule.

96. Furthermore, the proposed Regulation would only require "*evidence of a significant risk*" (Article 7 (4)) or an "*appreciable*" amount of child sexual abuse offences committed using a service (Article 7 (5-7)) beyond "*isolated and relatively rare instances*" (Recital 21). This is a lower threshold than the "*high risk*" set out in the Court's case law on permissible targeted data retention. In any event once a DO is in place it covers every user on the Provider's electronic communications system wherever that user is located which is far less "targeted" than a measure directed at a specific geographic location.

97. Thus I cannot see how a DO, and the process leading up to it, can preclude it being considered to require general and indiscriminate monitoring of electronic communications.

[73] §27 of the Commission Note.

(4) Does the DO regime respect the essence of the rights under Articles 7 and 8 of the Charter?

98. In *Digital Rights* the CJEU held that the retention of data provided by the Directive did not adversely affect the essence of those rights since the Directive did not permit the acquisition of knowledge of the content of the electronic communications.[74] In *Schrems* legislation which permitted public authorities to have access on a generalised basis to the content of electronic communications was held to compromise the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.[75] However those findings were made by the Court in respect of access to retained data. In *Quadrature 1,* the Court concluded that the automated analysis of traffic and location data, regardless of any subsequent retention, was an interference with rights under Articles 7 and 8.[76] It went on to consider the issue of justification without considering whether such interference adversely affected the essence of those rights. In other words it must have assumed that there was no adverse effect on the essence of those rights. Nevertheless I do not think one can draw the conclusion that access to data without retention can never impinge on the essence of the right. This is because the data in question was traffic and location data rather than the content of the communication.

99. Thus the case law of the CJEU suggests that is what is relevant to the essence of the right is more the content of the data rather than whether such data is retained or not. It is, however, not necessary for me to reach a concluded view on this point, as I consider that there are other reasons why the treatment of CSAM by the Regulation is unlawful.

(5) Is the Regulation, in the context of the application of DOs to encryption, properly reasoned and compliant with the principle of legal certainty?

100. I will deal first with the question of whether this part of the Regulation is properly reasoned and then the issue of legal certainty.

---

74 §39.
75 Case C-362/14 *Schrems* ECLI:EU:C:2015:650, §94.
76 §§172-174.

101. Article 296 TFEU requires all EU legal acts, including Regulations, to state the reasons on which they are based.[77] The reasoning must be appropriate to the act in issue. In the case of a measure intended to have general application (e.g. a Regulation as opposed to a Decision), provided the statement makes clear the essential objective pursued by the institutions, a specific statement of reasons for each of the technical choices made is not required.[78] The statement of reasons must show clearly and unequivocally the reasoning of the author of the measure in question, so as to enable those to whom the act applies to ascertain the reasons for the measure, but need not go into every relevant point of fact and law since the question of whether the statement of reasons meets the requirements of Article 296 must be assessed by reference to its wording and context.[79]

102. In my view, the relevant context to the Regulation includes (i) a major inroad into the fundamental right to the protection of privacy and data guaranteed by Articles 7 and 8 of the Charter which is, so far as I am aware, far greater than contained in any previous legislation[80], (ii) the express recognition by the 2021 Regulation that end-to-end encryption is an important tool to guarantee the security and confidentiality of the communications of users, including those of children and that therefore nothing in that Regulation should be interpreted as prohibiting or weakening end-to-end encryption, (iii) the position adopted to encryption in the Regulation which represents a complete reversal of the previous legislative provision, (iv) uncertainty as to the scope and type of anti-encryption tools to be used, (v) uncertainty as to the effectiveness of such anti-encryption tools and (vi) uncertainty as to the impact on both Providers and users if a DO required the Provider to "break" encryption.

---

77 See, e.g. C-157/21 *Poland v Parliament and Council* concerning the application of Article 296 to an EU Regulation at §§247-252.

78 See Case C-344/04 *IATA and ELFAA*, EU:C:2006:10, §67; Case C-380/03 *Germany* v *Parliament and Council*, EU:C:2006:772, §108; C-304/16 *American Express*, EU:C:2018:66, §76, and also Case C-493/17 *Weiss and Ors* ,§32.

79 C-63/12 *Commission v Council*, EU:C:2013:752, § 98; C-62/14, *Gauweiler and Others*, EU:C:2015:400, §70; C-367/95 P, *Commission* v *Sytraval and Brink's France*, EU:C:1998:154, §63, C-450/17 P, *Landeskreditbank Baden-Württemberg* v *ECB* EU:C:2019:372, §87.

80 See also the EDRi Paper states that encryption is "a vital human rights tool, with organisations across the world emphasizing that the security of people's private lives frequently relies on E2E encryption."[80] The EDRi Paper goes on to explain that client-side scanning poses a serious risk to the privacy of communications and increases vulnerability to attacks and hacking from third parties.

103. While EU law does not preclude the legislator changing its mind, even on an issue as fundamental as rights to privacy and data protection, any such change needs to be properly explained so that everyone can see understand – from the legislation itself – not only that a change is being made but the reasons for such a change. I say the legislation itself because that is what the TFEU requires. On an issue as fundamental as this it is not sufficient to say that one can look, for example, at the IAR rather than the legislation itself. There is an important constitutional point here. This Regulation, if adopted, is a Regulation of the Council and Parliament, not of the Commission. Furthermore, the IAR does not even represent the official, let alone, the concluded position of the Commission. As its title indicates it is a "*Commission Staff Working Document*".

104. The only place in the Regulation that tackles the issue of encryption is recital 26. Recital 26 in this respect is wholly obscure. Indeed a reader of that recital might be forgiven for considering that there is no change in the legislator's position between the 2021 Regulation and the Regulation. This is because recital 26 refers, in glowing terms, to "*the use of end-to-end encryption technology, which is an important tool to guarantee the security and confidentiality of the communications of users, including children.*" Nowhere does the recital flag up that end-to-end encryption technology is now considered by the legislator to be a problem rather than a benefit. So not only is there an absence of any reason as to why is a problem which needs to be tackled but the existing text, which I have quoted above, is misleading as it gives the impression that end-to-end encryption technology is a benefit rather than a problem. Thus the Regulation is, in this respect, incompatible with Article 296.

105. Finally I come to the issue of legal certainty. It is apparent from recital 26 that there is an absence of any reason as to why end-to-end encryption technology is a problem. Indeed, as I have indicated, the impression is given that end-to-end encryption technology is a benefit rather than a problem. Nothing is said about the scope of anti-encryption technology to be used or its effectiveness. In those circumstances I also conclude that the potential application of the Regulation to encrypted communications, through an individual DO, fails to comply with the principle of legal certainty.

CHRISTOPHER VAJDA KC

Member of the Bar of England and Wales and of Luxembourg

19 October 2023