Council of the European Union

Brussels, 16 May 2023
(OR. en)

9512/23

Interinstitutional File: 2022/0155(COD)

LIMITE

JAI 638
ENFOPOL 249
CRIMORG 78
IXIM 129
DATAPROTECT 141
CYBER 127
COPEN 160
FREMP 148
TELECOM 149
COMPET 450
MI 419
CONSOM 180
DIGIT 93
CODEC 895

NOTE

From:	Commission services
To:	Law Enforcement Working Party (Police)
Subject:	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 users' rights

Delegations will find hereafter a non-paper from the Commission services on the above-mentioned subject.

ANNEX

Non-paper prepared by the Commission services:

Balancing the rights of children with users' rights

Introduction

1. The Council and the Parliament are currently discussing the Commission's proposal for a Regulation to prevent and combat child sexual abuse[1] ('the proposed Regulation'). This non-paper prepared by the Commission services[2] expands on the compatibility with the Charter of Fundamental Rights of the EU ('Charter') of the proposed system of detection orders in respect of interpersonal communication services.[3]

2. In the following, the proposed Regulation and the relevant legal context are first introduced. Next, some general comments are made. Finally, specific comments are made regarding the four main issues raised in the legal debate, that is, concerning the 'quality' of the law; whether the proposed rules are either general and indiscriminate or targeted in nature; the essence of the fundamental rights at stake; and matters relating to proportionality.

Proposed Regulation and legal context

3. The objective of the proposed Regulation is to tackle child sexual abuse and protect children's rights in relation to the misuse of certain online services provided in the internal market, including interpersonal communications services.[4] One of the measures proposed to that aim entails empowering – but not obliging – national courts or 'court-like' independent administrative authorities to issue detection orders requiring a given service provider to employ certain technologies to detect three specific types of child sexual abuse on its service.[5] The measures aim to be '*targeted, carefully balanced and proportionate*'.[6]

---

[1] COM(2022) 209 final.

[2] This document should not be used for other purposes than the abovementioned one. As a non-paper prepared by the Commission services, it does not contain an official position of the Commission.

[3] On 26 April 2023, the Legal Service of the Council issued an opinion on the matter (reference no. 8787/23). The present non-paper takes account of the arguments raised in that opinion.

[4] Recital 1 and Art. 1(1) proposed Regulation.

[5] See in particular Art. 7-10 proposed Regulation. The three types of child sexual abuse covered are the dissemination of 'known' (i.e. previously detected) and of 'new' (i.e. not previously detected) child sexual abuse material, as well as the solicitation of children (known as 'grooming'). See Art. 2(l)-(p) proposed Regulation.

[6] Recital 2 proposed Regulation.

4. Under the proposed system, detection orders can only be issued where the competent national court, after a diligent and objective assessment involving also several other independent public authorities, considers that: (a) there is evidence of a significant risk that the service is misused for child sexual abuse; *and* (b) the reasons for issuing the order outweigh its negative consequences, having balanced all fundamental rights and other rights and interests at stake.[7] The availability of suitable technologies and the impact on the rights of the users of the service concerned are part of the required assessment and balancing exercise.[8] Whenever possible, the orders must target only identifiable parts or components of the service in question.[9]

5. Detection orders can only be issued after a mandatory prior process of risk assessment and mitigation.[10] They are therefore a measure of last resort, to be issued only if the risks remain significant despite the risk mitigation measures. Public oversight is ensured also at the stage of execution of the detection orders. In particular, detection can only be done using indicators prepared and reviewed by the EU Centre, a newly created independent EU agency.[11] Also, the service provider subject to a detection order must regularly report on the execution and the competent national authority must regularly assess whether any changes to the detection obligation may be required.[12] Other safeguards include rules ensuring effective redress and complaint-handling;[13] specific requirements regarding the technology to be used;[14] rules on purpose limitation and internal oversight and controls;[15] and information provision to users.[16]

6. It is true that the issuance and execution of a detection order limits the exercise of certain fundamental rights, notably those to privacy (protection of private life) and protection of personal data of the users of the services in question.[17] That finding is however in itself not conclusive. It is settled case law that these are not absolute rights but must be considered in relation to their function in society.[18] Therefore, the finding is the starting point of the analysis, not its end point. The central question is whether the limitation on the exercise of those two fundamental rights is compliant with the requirements of Article 52(1) Charter, which regulates such cases. The balancing exercise to be conducted in this regard must take account of all the circumstances of the case at hand.[19]

---

[7] Art. 7(4) proposed Regulation. As regards the significant risk, see also its Art. 7(5), (6) and (7).
[8] Art. 7(8) proposed Regulation.
[9] Art. 7(8) proposed Regulation.
[10] Art. 3, 4 and 5 proposed Regulation.
[11] Art. 10(1) and Art. 44, 46 and 47 proposed Regulation.
[12] Art. 9(3) and (4) proposed Regulation.
[13] Art. 9(1) and Art. 10(4)(d) proposed Regulation.
[14] Art. 10(3) and Art. 50(1) proposed Regulation.
[15] Art. 10(4)(a), (c), (d) and (f) proposed Regulation.
[16] Art. 10(5) and (6) proposed Regulation.
[17] Art. 7 and 8 Charter.
[18] E.g. CJEU Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, ECLI:EU:C:2020:791, para. 120; CJEU Case C-817/19, *Ligue des droits humains*, ECLI:EU:C:2022:491, para. 112.
[19] E.g. CJEU Case C-112/00, *Schmidberger*, ECLI:EU:C:2003:333, para. 81-82.

7. In the present case, the limitation is necessary to achieve the objectives of preventing and combating the aforementioned child sexual abuse offences, which the Court of Justice of the EU (CJEU) has described as '*inherently and indisputably extremely serious crime*'.[20] Moreover, the CJEU has also recognised that those crimes entail serious violations of the fundamental rights of the children, notably to protection of private and family life and to protection of an individual's physical and mental integrity, as well as the prohibition of torture and inhuman and degrading treatment.[21]

8. Particularly where, as in this case, children's physical and moral well-being is at risk, public authorities – and therefore logically also the EU legislator – are under a positive obligation to enable effective action against such crimes.[22] In this connection, account should also be taken of Article 24 Charter, which safeguards the rights of the child,[23] as well as the UN Convention on the rights of the child, to which all Member States are a party and which forms part of the general principles of EU law. Article 19 of that Convention is explicit on the need to take appropriate measures, including legislative ones, for the protection of the child from all forms of physical or mental violence, injury, abuse, neglect, maltreatment or exploitation, including sexual abuse.

9. The case at hand is further characterised by the fact that the extremely serious criminal offences at issue and the resulting equally serious violations of the fundamental rights of children inherently centre on the activities that the perpetrators undertake online. They can therefore only be effectively tackled by involving the providers of the relevant online services, including interpersonal communications services.[24] The in principle 'private' nature of these services implies precisely that they tend to be used for said activities, which by their very nature occur covertly, in that they involve typically communications between a limited number of specific persons.

10. That distinguishes the criminal offences at issue from criminal offences that occur offline. In respect of the latter, having access to certain personal data of users held by online service providers can certainly be *helpful* to tackle the crimes, but this is not necessary the *only* means to do so. Furthermore, the criminal offences at issue are also different from other criminal or otherwise unlawful activities that are conducted online, but that by nature tend to be 'public' at least to some extent, in the sense that they tend to involve communications to larger groups of persons in general, for instance terrorist propaganda, hate speech or copyright-infringing file-sharing.

11. Put simply, in the case at hand, the content is the crime.

---

[20] C-817/19, *Ligue des droits humains*, para. 149 (emphasis added). See also C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 154 (speaking of '*particularly serious*' offences).
[21] Art. 7, 3 and 4 Charter, respectively. See C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 126.
[22] C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 126-128.
[23] See also Art. 3(3) TEU (stating that the EU is to promote protection of the rights of the child).
[24] Recital 2 proposed Regulation.

12. Finally, the operational and legal challenges currently encountered arise against the background of the changes made as part of the introduction of the European Electronic Telecommunications Code,[25] which took effect from 21 December 2020. The adjusted definitions contained therein in effect extended the scope of the rules on the confidentiality of communications, set out in the e-Privacy Directive.[26] As a consequence, providers of interpersonal communications services were precluded from voluntarily detecting child sexual abuse on their services, as some had done.

13. As a temporary solution to enable continued voluntary detection, the Interim Regulation was adopted.[27] This was done to allow for the necessary time to adopt a new, long-term legal framework.[28] The proposed Regulation is intended to constitute that new legal framework.[29] The proposed system of detection orders resembles the Interim Regulation in various respects, including that it limits the exercise of the rights and obligations under Articles 5 and 6 e-Privacy Directive.[30] However, the proposed system is based on mandatory rather than voluntary detection and it establishes a far more elaborate and stringent framework, including the limits and safeguards mentioned.

14. The Interim Regulation applies only until 3 August 2024.[31] Therefore, in the absence of a solution found by the EU legislator before that date, the detection activities at issue would again be precluded from that date. Apart from the internal market implications, that implies that the aforementioned criminal offences and fundamental rights violations would remain unaddressed.

General comments

15. In the first place, it has to be acknowledged that the Court of Justice of the EU (CJEU) has to date never expressed itself on measures of the kind at issue. There is therefore necessarily a degree of uncertainty. Particularly in respect of complex and sensitive matters such as the present ones, no definitive and absolute conclusions can be drawn in either direction when it comes to compliance with the Charter.

[25] Directive (EU) 2018/1972, OJ 2018 L 321/36.
[26] Art. 5 and 6 Directive 2002/58, OJ 2002 L 201/37. In particular, because of the changes enacted, providers of (number-independent) interpersonal communications also qualified as 'electronic communications services' within the meaning of the e-Privacy Directive.
[27] Regulation (EU) 2021/1232, OJ 2021 L 274/41. See in particular its Recitals 7-10.
[28] Recital 23 Interim Regulation.
[29] Recital 78 Interim Regulation.
[30] Art. 1(4) proposed Regulation.
[31] Art. 10 Interim Regulation.

16. In the second place, precisely because the CJEU has not yet ruled on the complex and sensitive matter at issue, it is necessary to take a broad perspective. That involves especially taking account of all potentially relevant case law, including on the combating of illegal online content, and therefore not to focus only on the CJEU's data retention case law, that is, the line of case law centred on the judgment in *La Quadrature du Net*.[32]

17. Whilst relevant, the *La Quadrature du Net* line of case law is in itself not decisive. That is so already for the simple reason that the proposed rules at issue concern detection orders, not retention obligations. Insofar as that case law relates to particularly intrusive forms of processing other than retention, the situation at issue is not comparable, as explained below. It should also be noted that this line of case law cannot be said to be consolidated yet, the CJEU being asked until this day to reconsider and refine it on important aspects.[33] Moreover, the restrictive elements contained in that case law should not be over-emphasised; as shown below, account should also be taken of the elements that could justify a less restrictive reading.

18. In the third place, and relatedly, the potential broader implications of an expansive reading of the data retention case law should be considered. One concern is the impact that it may have on the possibilities for effective law enforcement, including on the pending EncroChat case.[34] Another concern is the potential impact on other EU legislation, most notably the Interim Regulation which, as mentioned, despite relying on voluntary action and not providing for a similarly elaborate legal framework, resembles the presently proposed measures in certain respects.

19. Finally, the proposed Regulation is obviously still under discussion. Where deemed necessary, adjustments could be made, including to address possible legal concerns relating to detection orders for interpersonal services. At the same time, apart from possible legal questions relating to any such adjustments, regard should be had to considerations of effectiveness. Entirely excluding detection on interpersonal communications may, for example, help address certain possible legal risks on which the current debate focuses. However, this would likely also make much of the proposed Regulation devoid of purpose. As explained, having regard to the nature of the criminal activities at issue, precisely these kinds of services tend to be misused for child sexual abuse. Moreover, without effective detection, many of the other proposed measures – such as reporting and removal obligations – also risk losing much of their practical significance.

---

[32] C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*. Other judgments in this line of case law include CJEU Joined Cases C-293/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238; CJEU Joined Cases C-203/15 and C-698/15, *Tele2*, ECLI:EU:C:2016:970; CJEU Case C-140/20, *Commissioner of An Garda*, ECLI:EU:C:2022:258; CJEU Joined Cases C-793/19 and C-794/19, *SpaceNet*, ECLI:EU:C:2022:702.

[33] See in particular the re-opening of the proceedings and referral to the Full Court in CJEU Case C-470/21, *HADOPI* (pending).

[34] CJEU Case C-670/22, *EncroChat* (pending).

'Quality' of the law

20. The first key issue is whether the proposed rules on detection orders meet the requirements as to the 'quality' of the law, that is, whether the rules are sufficient clear, specific and complete to justify the conclusion that the limitation on the exercise of the fundamental rights at issue are 'provided for by law' within the meaning of Article 52(1) Charter. The Commission services are of the view that they are and, consequently, that any doubts raised in this respect are unfounded.

21. There is no debate that the proposed Regulation, in itself, provides a 'law' as required under Article 52(1) Charter. It is true that the proposed rules contain certain open norms, which leave a degree of flexibility and some scope for interpretation. However, that does not mean that the 'quality of the law' requirements are not met.

22. First, the CJEU has held – with reference to case law of the Court of Human Rights (ECtHR)[35] – that said requirements do not preclude the legislation containing the limitation on the exercise of the relevant fundamental rights '*from being formulated in terms which are sufficiently open to be able to keep pace with changing circumstances*'.[36] In fact, the CJEU has noted that precisely the need to respect fundamental rights – and in particular to strike a fair balance between *all* fundamental rights at stake, including the freedom to conduct a business of the service providers involved[37] – may make it necessary to leave it to those service providers '*to determine the specific measures to be taken in order to achieve the result sought*'.[38]

23. Second, other examples such as the Copyright in the DSM Directive[39] and the Digital Services Act[40] (DSA) show that such an approach is not unusual when regulating online services, including in respect of tackling illegal content and activities online.[41] The area is characterised by relatively fast technological and commercial developments, whilst almost by definition involving activities that are sensitive from a fundamental rights perspective. Tellingly, the abovementioned relatively permissive case law of the CJEU and ECtHR relates precisely to measures taken in this area.

---

[35] ECtHR Application no. 64569/09, *Delfi v. Estonia¸CE:ECHR:2015:01616JUD006456909*, para. 121 (with further references).
[36] CJEU Case C-401/19, *Poland v. EP and Council*, ECLI:EU:C:2022:503, para. 74 (with further references).
[37] Art. 16 Charter.
[38] C-401/19, *Poland v. EP and Council*, 75 (with further references).
[39] Directive (EU) 2019/790, OJ 2019 L 130/92. See e.g. the references to '*best efforts*', '*a sufficiently substantiated notice*' and '*high industry standards of professional diligence*' in Art. 17(4) of this Directive.
[40] Regulation (EU) 2022/2065, OJ 2022 L 277/1. See e.g. the references to '*a criminal involving a threat to the life or safety of a person or persons*', '*promptly inform*' and '*all relevant information*' in Art. 18(1) and to '*a reasonable period of time*', '*frequently*' and '*manifestly illegal content*' in Art. 23(1) of this Regulation.
[41] For another example, see the Interim Regulation.

24. Third, it is important not to overlook that, in the case at hand, any such discretion and flexibility would be exercised within a detailed framework set out in the proposed Regulation, which includes, as mentioned, many important limits and safeguards. One of the safeguards is that the detection orders are issued by courts or independent administrative authorities and are prepared by, and are executed under the supervision of, other independent public authorities, notably the Coordinating Authority, the EU Centre and national data protection authorities.[42] These public authorities are all legally bound to ensure compliance with the Charter.[43] Their decisions are open to redress,[44] which may lead to preliminary references being made to the CJEU. In addition, the Commission will provide guidance.[45]

25. Thus, on the one hand, in situations like the one at issue, it is permissible and even necessary to leave a degree of discretion and flexibility. On the other hand, there is no question of the service providers being given a free hand. The discretion and flexibility are primarily to be exercised by relevant public authorities, subject to the Charter. Any 'residual' exercise thereof by the service providers concerned occurs under the control of those public authorities and ultimately the CJEU. Only in this manner can the matters at issue be regulated in a manner that is technologically neutral and future-proof and that allows for proportionate, case-specific solutions.

General and indiscriminate or targeted

26. The second key issue relates to the nature of the detection orders contained in the proposed Regulation. In essence, the question here is whether these instruments and the processing of personal data required thereunder is to be qualified as general and indiscriminate, or rather targeted, in nature.

27. That question should be answered in the light of all circumstances of the case at hand. In the view of the Commission services, there are in the present case strong grounds to believe that the proposed measures are not general and indiscriminate like the measures at issue in the data retention case law, but are rather targeted in nature. That is so especially considering that:

- a detection order would be targeted at only a specific service, whenever possible even only to an identifiable part or component thereof,[46] rather than at all electronic communications services collectively;

- the detection obligation would result from an order tailored to the case at hand, including an assessment of the potential impact on fundamental rights, the availability of suitable technologies and the need for any additional safeguards that may be necessary,[47] rather than from generally applicable legislation not involving any case-specific assessment and measures;

[42] See in particular Art. 7(1), (2) and (3) and Art. 9(3) and (4) proposed Regulation.
[43] Art. 51(1) Charter. The requirement of fair balancing has been made explicit in Art. 7(4) proposed Regulation.
[44] See in particular Art. 9(1) proposed Regulation.
[45] Art. 11 proposed Regulation.
[46] Art. 7(8) proposed Regulation.
[47] Art. 7(1), (4) and (8) proposed Regulation.

- a detection order would only be issued where justified in the light of the existing risks of child sexual abuse, as a measure of last resort, namely where a significant risk of child sexual abuse remains despite the mandatory prior risk assessment and mitigation process;[48]

- a detection order would be subject to strict limits in time,[49] rather than applying without any such limits under generally applicable legislation;

- a detection order would be targeted at certain specific material and conversations entailing specific criminal offences violating children's fundamental rights,[50] rather than a broad list of crimes or threats to national security in general.

28. It has been suggested that, nonetheless, the proposed detections orders would be general and indiscriminate in nature. Any such view may well affect various aspects of the broader analysis, including regarding the degree of seriousness of the interference with the aforementioned fundamental rights, the possible effects on the essence of those rights and proportionality. In other words, should this view not prove correct, then the concerns that might exist on those points lapse altogether or at least appear to be considerably less serious.

29. In this regard, reference is sometimes made to the position taken by the CJEU on the system of automated analysis provided for in the national legislation at issue in certain parts of *La Quadrature du Net.*[51] However, the national system at issue in that case is different from the detection orders contained in the proposed Regulation. That national system involved the *retention and automated analysis* of certain personal data.[52] That is not at issue under the proposed rules on detection orders, which operate based on a 'hit/not hit' model. That system was also much broader in scope – for instance, focusing on '*links that might constitute a terrorist threat*'[53] – and not subject to the limits and safeguards provided for in the proposed Regulation. Moreover, whilst that system involved general and indiscriminate processing, that is not the case under the proposed Regulation.

30. Furthermore, the abovementioned view could only be based on a very expansive reading of the data retention case law properly speaking, which the Commission services deem neither merited nor convincing.

[48] Art. 3 and 4, as well as Art. 7(4), proposed Regulation.
[49] Art. 7(9) proposed Regulation.
[50] Art. 2(l)-(p) proposed Regulation.
[51] C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 172-180.
[52] C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 172.
[53] C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 43

31. First, any such view fails to acknowledge the differences between retention, at issue in that case law, and detection, at issue in the case at hand. General and indiscriminate retention creates a large pool of personal data, which can subsequently be accessed and analysed. This, in turn, implies that a serious risk may exist of drawing very precise conclusions regarding the private lives of individuals, which is the main driving force behind the strict line taken in the CJEU's data retention case law.[54] Similar risks can arise in respect of other particularly intrusive forms of processing of personal data, such as the automated analysis on a general and indiscriminate basis of the kind referred to above. Although detection can still be intrusive, in the absence of retention or similar processing of the kind mentioned, 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.

32. Second, the aforementioned view appears to assume that solely the *personal scope* of the measures in question – that is, the persons subject to the measures in question – is decisive when determining whether the measures are targeted. However, the CJEU's case law shows that other elements can be relevant too, such as any *limit in time*.[55] Moreover, the case law expressly leaves scope for the use of *other* criteria to prevent the measures from being general and indiscriminate. The CJEU has held that this is, in principle, a matter to be decided by the legislator.[56] This underlines the relevance of the factors listed above which, especially when considered together, clearly point to the targeted nature of the proposed rules.

33. Third, even if we were to focus solely on the persons affected, it follows from the CJEU case law that an indirect connection to the possible crimes may suffice.[57] It is essential to take account of also this aspect in the analysis. The requirement of a 'connection' should not be taken to mean that something akin to an actual *suspicion* in respect of each person concerned is required. Besides seeming not feasible in practice, the case law does not support such an assumption. The CJEU's own example relating to the retention of personal data of persons present in certain geographical spaces, including those involving a '*very high volume of visitors*',[58] illustrates that such an indirect connection could be a rather loose one.

34. To be more concrete, when it comes to the geographical space at which targeted measures may *inter alia* focus, the CJEU gives the example of an airport.[59] Major airports tend to handle millions, if not tens of millions of passengers per year each. Cumulatively, the number of persons affected is logically much greater still. This shows that, whilst any measures entailing an interference should always be as targeted as possible, it is not excluded that they affect large parts of the EU population.

[54] C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 117. See also C-293/12 and C-594/12, *Digital Rights Ireland*, para. 27; C-203/15 and C-698/15, *Tele2*, para. 99.
[55] C-793/19 and C-794/19, *SpaceNet*, para. 75.
[56] C-793/19 and C-794/19, *SpaceNet*, para. 112.
[57] C-793/19 and C-794/19, *SpaceNet*, para. 105.
[58] C-793/19 and C-794/19, *SpaceNet*, para. 110.
[59] C-793/19 and C-794/19, *SpaceNet*, para. 108.

35. If that can hold true for a *geographical* space, it can in principle also hold true for a digital space, such as a specific online service or a part or component thereof. That is especially so if – as in this case – the measures are justified by the need to effectively tackle extremely serious crimes and fundamental rights' violations, multiple factors ensure the targeted nature of the measures, and adequate limits and safeguards are provided for. Thus, there are in this case objective criteria that establish a connection between the processing of the personal data concerned and the objective pursued.[60]

36. Finally, there is no reason to consider that the need for a connection should be appreciated in a fundamentally different manner, depending on whether the personal data at issue concerns metadata or content data. The case law available to date simply does not offer any support for an argument to that effect.

Essence of the rights

37. Pursuant to Article 52(1) Charter, if a limitation on the exercise of fundamental rights compromises the essence of those rights, the measures in question would violate the Charter *per se*, that is, irrespective of any proportionality assessment. In the view of the Commission services, there is however no reason to believe that this would be the case here or that serious risks in this respect would exist.

38. First of all, that it is true that the CJEU has in certain cases alluded to the sensitivity of content data, which is indeed affected to some extent by the proposed measures.[61] However, this was done in connection to measures that are general and indiscriminate in nature. As explained above, that is not the case here. The proposed measures are targeted in nature. By extension, there is no question under the proposed Regulation of giving certain private parties or public authorities access, on a generalised basis, to the content of electronic communications.

39. Furthermore, the approach whereby such a fundamental distinction is drawn between interferences involving metadata and content data finds no support in the case law. For instance, in *La Quadrature du Net* the CJEU held that information derived from metadata can be '*no less sensitive having regard to the right of privacy, than the actual content of communications*'.[62] Thus, whilst the nature of the personal data is not irrelevant, the principal question is what is *done* with the data.[63]

[60] E.g. C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 133; C-817/19, *Ligue des droits humains*, para. 118 (both with further references).
[61] E.g. CJEU Case C-362/14, *Schrems,* ECLI:EU:C:2015:650, para. 94.
[62] C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 117 (with further references; emphasis added).
[63] Note also that the system established under the national law at issue in -511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 172-180 was not deemed to violate the essence of the fundamental rights at stake.

40. The case law also suggests that it is not so much the interference with the content of communications as such that may be problematic, but rather whether it '*permit[s] the acquisition of knowledge of the content*' of the communications.[64] Given especially the technology and indicators to be used under the proposed Regulation,[65] no such knowledge of the content could be acquired, certainly not on a generalised basis.

41. It should also be noted that in other case law the CJEU has applied different standards. In *Ligue des droits humains*, it has for instance held that measures that might reveal very specific information on the private lives of individuals did not affect the essence of the fundamental rights at issue. That was because the information in question, having regard to the limits and safeguards enacted, did not allow for '*a full overview*' of those private lives.[66] Nothing even resembling a full overview could be obtained through the proposed detection orders.

42. Finally, once more, regard should be had to the specifics of the case at hand. As mentioned, the proposed Regulation aims to tackle certain specific forms of extremely serious criminal offences and violations of children's fundamental rights carried out *online*. This is yet another important difference with the data retention case law, which mostly seeks to contribute to tackling criminal activities and activities entailing threats to national security that are carried out *offline* and that could, generally speaking, therefore also be tackled through other means.[67] As explained above, the particular criminal offences at issue are different even from must other crimes or otherwise unlawful activities committed online.

43. As noted, simply put, in the case at hand, the content is the crime.

44. Where that is so, the measures taken must necessarily affect the content, at least to some extent, for them to be effective. It is likely for this reason that the CJEU has deemed measures of this kind acceptable and even necessary in its case law on illegal online content, for instance to tackle online copyright infringement[68] and online defamation.[69] There is no reason to think that this would be fundamentally different for the measures contained in the proposed Regulation.[70] Arguably rather the contrary, having regard to the extremely serious nature and consequences of the crimes at issue, the likelihood of the crimes being carried out in a covert manner, as well as the expansive set of limits and safeguards provided for. Thus, in addition to the nature of the personal data at issue and the question what is done with the data, the questions *why* and *how* it is done are relevant too.

---

[64] C-293/12 and C-594/12, *Digital Rights Ireland*, para. 39 (emphasis added).
[65] See in particular Art. 10(3)(b) proposed Regulation.
[66] C-817/19, *Ligue des droits humains*, para. 120 (emphasis added).
[67] Cf. e.g. C-793/19 and C-794/19, *SpaceNet*, para. 96.
[68] C-401/19, *Poland v. EP and Council*.
[69] CJEU Case C-18/18, *Facebook Ireland*, ECLI:EU:C:2019:821.
[70] Note that whereas the case law cited deals essentially with hosting services (that is, services turning around the online storage of third-party information), such services do not necessarily involve information that is publicly available; they can also involve communications of an in principle 'private' nature. Hosting services and interpersonal communications services are not mutually exclusive legal concepts.

45. In the light of the above, the Commission services acknowledge that interferences involving the content of communications tend to be sensitive and intrusive. A strong justification and adequate limits and safeguards are therefore required. However, the available case law, properly assessed, provides no ground to conclude that, in a situation such as the one at issue, the fact that content data is processed affects the essence of the fundamental rights at stake and is therefore precluded *per se*.

Proportionality

46. The fourth and last key issue to be addressed relates to the proportionality assessment required under Article 52(1) Charter. In practice, this is often the central element in the review conducted by the CJEU.

47. The Commission services are of the view that there are numerous elements that, especially when considered in their totality, likely justify the conclusion that the proposed system of detection orders is proportionate.

48. As a first point, it is important to recall, once more, that the proposed detection orders do not entail processing that is general and indiscriminate in nature, within the meaning of the CJEU's case law available to date. Any proportionality assessment based on the premise that they are, therefore does not seem correct.

49. In addition, it is important to distinguish between the retention generally at issue in the data retention case law, the analysis required under the aforementioned particular national legal system at issue in some parts of the *La Quadrature du Net* judgment, and the detection actually at issue in the case at hand. It goes without saying that precisely identifying the nature of the activities causing the interference is of great importance when assessing their proportionality. That means that any conclusions articulated by the CJEU in cases involving the former two types of processing cannot simply be applied one-to-one to the activities at issue here.

50. Furthermore, proportionality is essentially about the relationship between the means employed to achieve the objective pursued. It is generally recognised that combating child sexual abuse is an objective of general interest within the meaning of Article 52(1) Charter. Moreover, the fact that, as has been seen, the crimes and violations of the fundamental rights of children at issue are extremely serious, and that relevant public authorities are under a positive obligation to act in this respect, is of crucial importance precisely on this point. These circumstances, which are specific to the present case, should be placed at the very heart of the proportionality assessment.

51. It may be true that the CJEU has held that such positive obligations cannot justify the imposition of *general and indiscriminate* obligations to *retain* personal data of *practically the entire population*, and also that only the purpose of safeguarding *national security* and not tackling *serious crime* are able to justify those kinds of measures.[71] However, that does not mean that these positive obligations, as well as the other specific circumstances mentioned, are to be ignored when assessing the *proportionality* of *targeted* measures for the *detection* of the criminal offences at issue in the present case.

52. Far from it. In fact, ignoring them would go against two considerations that are central to much of the case law. Namely, firstly and most generally, that in situations like these, where several fundamental rights conflict with each other, a fair balance must be struck between them.[72] And secondly and more specifically, that the more serious the objectives pursued by the measures entailing an interference are, the more serious the interferences they can justify, and *vice versa*.[73] The extremely serious nature of the crimes and the violations of children's fundamental rights at issue are therefore highly relevant when assessing the proportionality of the proposed rules.

53. In line with what has been said above, interferences with the content of communications may be sensitive, but it does not follow that they are necessarily disproportionate. Particularly not where, as in the present case, the interferences occur with the objective of tackling certain specific, extremely serious criminal offences and violations of the fundamental rights of children, which – as was noted earlier – by virtue of their nature can only be effectively tackled in that manner.

54. In the data retention case law, the CJEU has accepted that the fact that a particular measure may be the only means of effectively tackling certain crimes can mean that it is compatible with the Charter, including as a matter of proportionality.[74] That is so even when the measure constitutes a serious interference with fundamental rights.[75] That decision by the CJEU may have related to intrinsically less sensitive personal data (namely source IP addresses), but that is counterbalanced by the fact that that data is retained in a general and indiscriminate matter, which is inherently more intrusive than targeted detection. The latter aspect should not be ignored. That argues in favour of taking account of this circumstance also in this case.

55. Precisely on this point – that is, the '*risk of systemic impunity for offences committed exclusively online*' – the data retention case law may be subject to further refinement.[76]

---

[71] C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 145; C-793/19 and C-794/19, *SpaceNet*, para. 92-94.
[72] E.g. C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 127.
[73] C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 131; C-140/20, *Commissioner of An Garda*, para. 53. See also CJEU C-207/16, *Ministerio Fiscal*, ECLI:EU:C:2018:788, para. 55; C-817/19, *Ligue des droits humains*, para. 116.
[74] C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 154.
[75] C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 153.
[76] See Opinion AG Szpunar, Case C-470/21, *HADOPI*, para. 68-88.

56. Finally, it is settled case law that, in situations like the present one, account must be taken of the system in its entirety, in particular the applicable limits and safeguards.[77] Therefore, when conducting the proportionality assessment, it is imperative that account is taken of the extensive system of limits and safeguards that the proposed Regulation would establish for the issuance and execution of detection orders. As observed earlier, these safeguards include the following: issuance by a court or independent administrative authority based on a case-by-case balancing exercise; involvement and oversight by other independent public authorities at all stages; prior risk assessment and mitigation; only issued in case of an objectively evidenced significant risk of child sexual abuse, graduated in function of the degree of intrusiveness; mandatory targeting; strict limits in time; regular reporting and review; effective redress and complaint-handling; information provision to users; purpose limitation and internal oversight and controls; specific requirements regarding the technology to be used; detailed safeguards regarding the indicators to be used; and safeguards stemming from Commission guidance.

Conclusion

57. In conclusion, the system allowing for the issuance, under certain conditions, of detection orders to be employed in respect of interpersonal communication services contained in the proposed Regulation is novel and relates to a complex and sensitive area of law. Questions as to the compatibility with the Charter therefore arise and cannot be answered with absolute certainty. However, the Commission services consider that the proposed rules and the case law available to date, seen in their entirety and properly construed, provide no reasons to conclude that on this point the proposed Regulation is incompatible with the Charter.

---

[77] See e.g. C-401/19, *Poland v. EP and Council*, para. 82-98.