Universiteit van Amsterdam

Instituut voor Informatierecht
Institute for Information Law

# Fundamental rights assessment of the framework for detection orders under the CSAM proposal

April 2023

# Fundamental rights assessment of the framework for detection orders under the CSAM proposal

Ot van Daalen

22 April 2023
Amsterdam

Institute for Information Law (IViR, University of Amsterdam), 2023

This project has been carried out in full compliance with the Declaration of Scientific Independence of the Royal Netherlands Academy of Arts and Sciences. Funding included a grant from European Digital Rights (EDRi). Ot van Daalen has been a board member of EDRi during 2013 to 2018.

# Table of contents

# 1 Introduction and summary

The European Commission in 2022 proposed a regulation to combat sexual child abuse (the "proposal").[1] Under the proposal, providers of interpersonal communications services are obliged to assess and mitigate the risk that their service will be used for online child sexual abuse. In addition, they can be ordered to take measures to detect the dissemination of child sexual abuse material ("CSAM") and the solicitation of children for sexual purposes ("grooming"). They are obliged to report suspected online child sexual abuse to relevant authorities.

The objective of the proposal, to combat sexual child abuse, is of the utmost importance. Sexual abuse of children is a horrendous crime, and policymakers should explore every avenue available to them to prevent, detect and otherwise address it. Furthermore, the fundamental rights of children, including their right to human dignity, physical and mental integrity, privacy as well as their right to not be subject to inhuman or degrading treatment, are deeply impacted by sexual child abuse.[2] Given what's at stake, it is crucial that this proposal complies with the Charter of Fundamental Rights of the European Union (the "Charter").

This report aims to contribute to that debate, focusing on one particular issue: whether the proposed legal framework for detection orders is compatible with the rights to privacy, data protection and freedom of expression as laid down in Articles 7, 8 and 11 of the Charter. In summary:

- The proposal allows for the issuing of orders for indiscriminate, automated analysis of confidential communications. These orders can be directed to the providers of popular messaging services such as WhatsApp, Signal and iMessage. An order can oblige such a provider to analyse communications on the devices of users, or analyse the communications on servers through which the communications are routed. In the latter case, if end-to-end encryption is applied, this would require the altering of the encryption in order to allow the analysis of contents of communications. These orders can be issued, in short, where there is evidence of a "significant risk" of the service being used for online child sexual abuse, and the reasons for issuing the order outweigh the negative effects of the order.

- The proposal contains a number of safeguards to ensure that, when issuing an order, relevant interests are taken into account. It is uncertain, however, whether these safeguards would prevent the issuing of these kinds of broad orders in practice. The text of the legal framework is not clear on this, while the logic of the proposal appears intended to create the possibility of issuing these kinds of broad orders.

- These detection orders and the framework for issuing them affect the rights to privacy, data protection and communications freedom under the Charter. As a result, they must respect the essence of these rights, and be proportionate to the aim of the proposal. It can be concluded from case law from the Court of Justice of the European Union ("CJEU") that indiscriminate analysis of confidential communications affects the essence of these rights. When it comes to the assessment of proportionality, a measure must first be clearly circumscribed, and contain minimum safeguards against abuse and unlawful access. Where the interference is potentially more serious, or the risk of abuse is more present, an even higher standard of clarity is required. Second, the

1 Proposal for a Regulation of the European Parliament and of the Council Laying down Rules to Prevent and Combat Child Sexual Abuse, COM(2022) 209 final.
2 See Artt. 1, 3, 4, 7 and 24 of the Charter.

measure must strike the right balance between the objective, the seriousness of the interference, and the connection between the objective and the measure. Generally speaking, an indiscriminate measure which should be considered a serious interference, can only be justified for national security purposes, a term which is interpreted narrowly by the CJEU.

- The legal framework for issuing detection orders is not sufficiently clearly circumscribed to prevent abuse, because the framework allows for the issuing of indiscriminate orders, possibly on device, to analyse confidential communications. These kinds of orders are not proportionate to the aim of combating child sexual abuse online. Firstly, they are aimed at the *service*. The connection between the objective, the combating of child sexual abuse online, and the measure, the analysis of all communications on this service, is remote. Meanwhile, the interference is very serious: it potentially affects all users of a service and affects all their communications via that service. These communications may contain highly sensitive data, and are central to the exercise of privacy, data protection and freedom of expression in the modern age. The detection would be performed on an automated basis, something the the CJEU has considered to further contribute to the seriousness of an interference. And as noted, it may even be done on the device, which should be accorded even more protection in view of the private nature of devices. Finally, orders which change the encryption which is applied, so that communications can be analysed in transit, would increase the risk of unlawful access to confidential communications of all users. Meanwhile, the objective, the combating of child sexual abuse, is highly important, but does not rise to the level of national security. As a result, the proposed legal framework for issuing detection orders and the potential detection orders which may be issued should be considered incompatible with the rights to privacy, data protection and communications freedom under the Charter.

This is explained further below.

The scope of this analysis is limited to whether the framework and related detection orders under the Charter respect the essence of certain fundamental rights at stake, and whether they are proportionate. It is based on case law of the CJEU. It builds on other fundamental rights analyses of this proposal.[3]

As a result, this report also has significant limitations. It does not touch on other aspects of the proposal, such as the orders which can be issued against hosting providers. It further does not discuss whether the envisaged technologies would be effective in detecting CSAM and grooming, to what extent these technologies may lead to false accusations, and whether these would create new security risks.[4] It also does not focus on the subsidiarity, e.g. the extent to which there are equally or more effective ways to combat sexual child abuse, which are less intrusive. Finally, this analysis does not discuss the validity of the legal basis of the proposal.

3 See in particular EDPB and EDPS, "Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Rules to Prevent and Combat Child Sexual Abuse", (EDPB and EDPS 2022) Joint Opinion 4/2022; and the complementary impact assessment of the European Parliament of the proposal, which is at the time of writing not yet published, but of which a draft of april 2023 has been leaked.

4 See on this for example Matthew Green, "Remarks on 'Chat Control'", contribution to meeting of EuroISPA on 23 March 2023.

# 2 The detection framework allows for indiscriminate, automated, on-device analysis of confidential communications

## 2.1 The proposal creates the possibility for issuing detection orders to communication providers

The proposal, published by the Commission on 11 May 2022, is part of an approach to combat online sexual child abuse announced by the Commission in 2020.[5] The Commission at that time said that it would first adopt temporary legislation under which providers could voluntarily scan communications for CSAM. This was done in July 2021, when the European Parliament and the Council adopted a temporary exception to the protection of communications confidentiality under the ePrivacy rules.[6] This has made it possible for providers to at their own initiative scan communications for CSAM. Less then a year later, the Commission then launched the proposal supposed to replace this temporary legislation. This proposal is the subject of this report.

The proposal is intended to address one particular kind of sexual child abuse: online abuse. This is why the proposal revolves around creating obligations for certain online service providers. The analysis in this report focuses on one of these kinds of providers in particular: providers of interpersonal communications services ("communications providers"). An interpersonal communications service is a service which enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s).[7] For purposes of this report, it can be assumed that this includes broadly used confidential messaging services, such as WhatsApp, Signal, Telegram and iMessage.

When it comes to communications services, the proposal sets out a two-pronged system to address the use of these services for online child sexual abuse. All these communications providers would be obliged to determine the risk that their service may be used for online child sexual abuse, take "reasonable" measures to mitigate this risk, and report on this to a national designated authority (the "coordinating authority").[8] In addition, the coordinating authority may under certain circumstances request the competent judicial authority or another independent administrative authority to issue a "detection order" against a specific communications provider, which would oblige this provider to install and operate technologies to detect the dissemination of known or new CSAM, or grooming.[9] These detection orders are the topic of this report.

5 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on an EU Strategy for a More Effective Fight Against Child Sexual Abuse, COM(2020)607 final.
6 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, OJ 2021 L 274/41.
7 See the Proposal for a Regulation of the European Parliament and of the Council Laying down Rules to Prevent and Combat Child Sexual Abuse, COM(2022) 209 final, Art. 2(b); and Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 Establishing the European Electronic Communications Code (Recast), 2018 OJ L 321/36, Art. 2(5)
8 Proposal for a Regulation of the European Parliament and of the Council Laying down Rules to Prevent and Combat Child Sexual Abuse, COM(2022) 209 final, Artt. 3-5.
9 Ibid, Artt. 7(1) and 10(1).

## 2.2 The framework for issuing detection orders

The framework for issuing detection orders in broad lines would work as follows:

- *Standard for issuing order*. The detection order shall be requested and issued where (a) there is evidence of a "significant risk" of the service being used for the purpose of online child sexual abuse, and (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.[10] Such a risk shall be deemed to exist where it is likely, despite mitigation measures, that the service is and has been used in past 12 months, to an appreciable extent for the dissemination of known CSAM or grooming.[11] For *new* CSAM, e.g. CSAM which has not been previously detected and identified as such, these conditions are supplemented by the requirement that a detection order for *known* CSAM has already been issued, and the provider has already submitted a significant number of reports with regard to these.[12] Isolated and relatively rare instances of CSAM or grooming should not be considered to rise to the level of appreciability.[13]

- *Process for issuing order*. The process for issuing an order consists of a number of steps. The coordinating authority would first submit a draft request to the provider and offer the provider, and a to-be-formed EU-wide institution called the EU Centre, the opportunity to comment.[14] The coordinating authority will then resubmit the draft request to the provider, amended if appropriate, which will in turn submit to the coordinating authority an implementation plan and – for the detection of grooming – a data protection impact assessment and prior consultation with the data protection authority.[15] The coordinating authority may then submit the request, adjusted if appropriate, to the competent judicial authority or independent administrative authority. This authority shall then issue the order, applying the standard set out above.

- *Scope of order*. As noted above, communication providers must execute the detection order by "installing and operating technologies" to detect the dissemination of known or new CSAM, or grooming.[16] While the EU Centre shall make available detection technologies for providers to use, providers shall not be required to use any specific technology, as long as four requirements are met.[17] First, the technologies must be effective in detecting CSAM or grooming. Second, they must not be able to extract any other information from the relevant communications than the information strictly necessary to detect patterns pointing to the dissemination of known or new CSAM or grooming. Third, they must be in accordance with the state of the art in the industry, and must be the least intrusive in terms of privacy and data protection. Finally, they must be sufficiently reliable, in that they limit the rate of errors regarding the detection to the maximum extent possible. The European Commission may issue guidelines on this.[18] Detection would work by applying a database of "indicators", which are provided the EU Centre.[19]

10 Ibid, Art. 7(2).
11 Ibid, Art. 7(5) and 7(7).
12 Ibid, Art. 7(6) jo. 2(n) jo. 44(1)(b).
13 Ibid, rec. 21.
14 Ibid, Art. 7(3).
15 See Regulation (EU) 2016/679 (General Data Protection Regulation), 2016 OJ L 119/1, Art. 7(3); ibid Artt. 35 and 36.
16 Proposal for a Regulation of the European Parliament and of the Council Laying down Rules to Prevent and Combat Child Sexual Abuse, COM(2022) 209 final, Art. 10(1).
17 Ibid, Artt. 50(1), 10(2) and (3).
18 Ibid.
19 Ibid, Art. 44

- *Safeguards regarding the detection order*. There are a number of safeguards to ensure that the detection order takes relevant interests into account. The competent authorities requesting and issuing a detection order shall target and specify the order so that the 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, remain limited to what is strictly necessary to effectively address the significant risk.[20] To that aim, they shall take into account all relevant parameters, including the availability of sufficiently reliable detection technologies and the impact of the measures on the rights of the users affected, and require the taking of the least intrusive measures from among several equally effective measures.[21] In particular, they shall ensure that, where possible, the order is only applied to a part or component to which the risk is limited, that "effective and proportionate safeguards" are provided for; and that the period of application remains limited to what is strictly necessary.[22] In the order, the application period must be specified, but cannot be longer than 24 months (for CSAM) or 12 months (for grooming).[23] The detection orders concerning grooming can apply only where one of the users is a child.[24] The proposal also prescribes the way in which the detection order must be drafted, which must follow a template provided in the proposal.[25] Communications providers and affected users also have a right to challenge the detection order before the courts.[26]

- *Safeguards with the provider*. The provider must take all necessary measures to ensure that the technologies, indicators, and data processed in the context of the detection order are used solely and only to the extent strictly necessary for executing the detection order, including through internal procedures.[27] Moreover, it must ensure regular human oversight to ensure the reliability of the detection technology and intervene in the case of errors.[28] It must also establish a complaint mechanism for users.[29] Finally, the provider must inform users that it uses these kinds of detection technologies, how they work, what this means for communications confidentiality, that findings must be reported to the EU Centre and inform them on their rights to redress and complaints.[30]

- *Effect of order.* The communications provider must promptly report "any information indicating potential online child sexual abuse on its services" to the EU Centre in a certain format.[31] It must also inform the user concerned that it has submitted such a report.[32] This obligation applies, regardless of how the communications provider has become aware of this information, so this obviously includes information it has detected through the execution of a detection order.

20 Ibid, Art. 7(8).
21 Ibid, Art. 7(8).
22 Ibid, Art 7(8).
23 Ibid, Art. 7(9).
24 Ibid, Art. 7(7).
25 Ibid, Art. 8.
26 Ibid, Art. 9(1).
27 Ibid, Art. 10(4)(a) and (b). When executing the detection order, 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 the proposal, nor by third parties, and thus to avoid undermining the security and confidentiality of the communications of users; ibid, rec. 26.
28 Ibid, Art. 10(4)(c).
29 Ibid, Art. 10(4)(d).
30 Ibid, Art. 10(5).
31 Ibid, Artt. 12(1) and 13.
32 Ibid, Art. 12(2).

## 2.3 The framework allows for ordering indiscriminate, automated, on-device analysis of confidential communications

For the fundamental rights analysis which follows, one important factor is what the potential scope of an order is. As discussed above, an order will be aimed at the detection of the dissemination of CSAM or grooming through the use of the communications service. This means that execution of a detection order in all cases will require a certain form of analysis of the communications in question. There are, however, different ways in which this could be done.

One potential distinction is between the analysis of *content* of the communication, e.g. particular messages, and the *metadata* of the communications, such as the sender, recipient, subject and time of the messages, or, more generally, the communications patterns. For the detection of CSAM, it is unavoidable to do some sort of analysis of the contents of communications. For the detection of grooming, it could in first instance be sufficient to merely analyse the metadata of communications, e.g. an older man is chatting with a younger girl he has not been in contact with before. Even in that case, however, this would have to be followed up with analysis of the messages in question – it might be that the older man is chatting with his long lost niece. The European Commission also notes that metadata is not considered an effective tool in detecting CSAM by providers, and that the use of metadata is "usually insufficient to initiate investigations" – thus suggesting that the analysis of content will have to form part of the detection order for it to be effective.[33]

Another distinction is between analysis at the *endpoints*, usually the phone or computer of a user, and analysis *in transit*, which may be at internet cables or the servers of the app service through which the communication flows. The most popular messaging apps currenty apply encryption, which means that when the messages leave the endpoint, their contents cannot be accessed without the decryption key. For end-to-end encryption technologies currently applied in popular messaging services, such as WhatsApp, iMessage and Signal, only the sender and recipient have the necessary keys, which means that it would not be possible for the communications provider to analyse the content of the messages at the server level.

Given the ubiquitous use of end-to-end encryption in messaging apps, combined with the purported need to analyse the content of messages, a detection order will have to be directed at either (i) analysis of the messages at the endpoints, before encryption is applied (a "device detection order"), or (ii) changing of the applied encryption protocol while, if necessary, forcing communications to be routed through servers operated by the communications provider, so that it is possible for the provider to analyse the contents of the communications *in transit* (an "encryption altering order").

The *text* of the proposal appears to allow the issuing of these two kinds of detection orders. As noted above, the provider is not required to use any specific technology, as long as it meets the conditions set out in the proposal, one condition being that it is effective. And because most popular messaging services apply end-to-end encryption, this condition of effectiveness logically implies that the detection order must be aimed at analysis at the endpoints, or that encryption and routing must be changed. For completeness, it is noted in the recitals that orders "should not be understood as incentivising or disincentivising the use of any given technology, [which] 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". This consideration, however, cannot be read to prevent encryption altering orders.

33 European Commission, "Impact Assessment Report Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council Laying down Rules to Prevent and Combat Child Sexual Abuse", Commission Staff Working Document, SWD(2022) 209 final.

Firstly, the recital is neutral on whether encryption technologies could be altered, but even if the intent were to prevent this, recitals do not take precedence over the text of provisions in European legislation.

It is furthermore likely that these detection orders would be applied indiscriminately, to *all* users of a service. The reason for this is that under the proposal, a detection order shall be applied where there is a "significant risk" that the *service* is used for the dissemination of CSAM or grooming. The risk identified in the proposal, in other words, extends to the entire service, not to particular users – so the detection order would then likely also extend to the entire service, not to particular users. Furthermore, the text, explanatory memorandum and impact assessment of the proposal are not clear on the need to limit the scope of the detection order to certain users as a way to make it more proportionate. The text notes that where a "risk is limited to an identifiable part or component of a service, the required measures are only applied in respect of that part or component."[34] In the recitals, it is further explained that this "should concern, in particular, 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."[35] Because of the emphasis on service-wide risks, the requirement that this limitation would only be applied "where possible", means that its potential to restrict orders to certain users, will in practice probably be limited (because user restrictions *on* the service will not be "possible" where the risk is associated with the service itself). The Commission's press release accompanying the proposal is illustrative in this regard, where it is suggested that detection orders may be limited "in time, targeting a specific type of content on a specific service", but not mentioning users as a potential selection criterion.[36] The underlying logic of the proposal also suggests that the intention of the proposal is to allow for these broad kinds of orders. As noted above, the proposal is intended to replace the temporary exception which allowed for voluntary scanning – voluntary scanning which is presumably already applied on an indiscriminate basis under the temporary exception and, which, according to the European Commission, "has proven to be insufficient to adequately protect children."[37]

Finally, given the scale of the messages which have to be analysed, this detection will have to be done automatically, using artificial intelligence (AI) technologies. For known CSAM, the most likely solution would involve comparing a set of hashes against material transmitted in communications. This set of hashes will have to be generated on the basis of known CSAM and then shared with the communications provider, who then can use this set to perform matching on the server or the endpoint. For new CSAM, matching will have to be based on image recognition of certain patterns which are indicative of CSAM. And for grooming, this will involve the automated analysis of text, something which is already realistic, given the adoption of services based on large language models, such as ChatGPT. To be clear – there are serious questions on the rate of false positives and false negatives in these technologies, which could even stand in the way of their application, but these are not the topic of this report.[38]

34 Proposal for a Regulation of the European Parliament and of the Council Laying down Rules to Prevent and Combat Child Sexual Abuse, COM(2022) 209 final, Art. 7(8)(a).

35 Ibid, rec. 23.

36 European Commission 11 May 2022, "Press Release: Fighting Child Sexual Abuse: Commission Proposes New Rules to Protect Children"; the European Commission when discussing ways to limit the impact on users' fundamental rights in the impact assessment further mentions that "supplementary safeguards would be required, including targeting the voluntary detection of new material and grooming to services where children may be at high risk, and providing clear information to users" – but not restricting it to certain users; Commission, "Impact Assessment Report Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council Laying down Rules to Prevent and Combat Child Sexual Abuse", Commission Staff Working Document, SWD(2022) 209 final, p. 96.

37 European Commission 11 May 2022, "Press Release: Fighting Child Sexual Abuse: Commission Proposes New Rules to Protect Children".

38 See on this for example Matthew Green, "Remarks on 'Chat Control'", contribution to meeting of EuroISPA on 23 March 2023.

## 2.4 The safeguards may not prevent the issuing of indiscriminate orders

One crucial question for this analysis is whether the safeguards set out in the proposal are sufficient to mitigate the risk of such potentially broad detection orders. The strongest safeguard in this respect is that the authorities must apply certain tests when requesting, respectively issuing the order. To be precise, they must "target" and "specify" the order in such a manner that the 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, remain limited to what is "strictly necessary" to effectively address the significant risk.[39] Part of this language appears to be borrowed from human rights case law, where certain limitations on fundamental rights must be "strictly necessary" and, in the case of conflicting rights or interests, strike a "fair balance" between them.

As to the requirement of "strict necessity" – this implies a particularly stringent test. The CJEU has repeatedly considered that the protection of the fundamental right to respect for private life at EU level requires that "derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary."[40] In *Digital Rights Ireland*, it further explained that this means that: "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 […], the EU legislature's discretion is reduced, with the result that review of that discretion should be strict."[41] The CJEU also recently considered how this requirement must be interpreted when it is used in an EU legal framework.[42] In that particular case, EU law provided that the processing of biometric and genetic data by police is only allowed if "strictly necessary". The CJEU considered that this must be interpreted as establishing "strengthened conditions for lawful processing of sensitive data", which in that particular context entails "particularly strict checking, in that context, as to whether the principle of data minimisation is observed."[43]

As to the requirement of a "fair balance", the CJEU's decision in *La Quadrature* is relevant. Here, the Court considered that a legal framework protecting the rights of children must strike a balance between the various interests and rights to be protected.[44]

There are, however, a number of reasons why the correct application of these principles to detection orders is at the very least uncertain. It is firstly not made explicit in the proposal that, in fact, these terms should be applied in conformity with human rights case law. More importantly, it is not a given that these will be applied like that *in practice* either. This has to do with the institutional setup, where the coordinating authority which is supposed to apply this standard is primarily responsible for combating sexual child abuse online, not for safeguarding fundamental rights. There is, thus, a certain risk that this authority would interpret the "fair balance" and "strict necessity" as allowing for broader detection orders than would in fact be allowed under human rights case law, in order for the regulation to function as is likely intended.[45] And this risk is also present to a certain extent in regard to the authority issuing the order. These risks are compounded by, firstly, the intent of the proposal, which arguably is to allow for these broad orders. Secondly, this is supported by the history of the proposal, building on the temporary exception allowing for voluntary scanning, which presumably also is being applied indiscriminately, and is not considered sufficiently effective by the European Commission (see above). Finally, these coordinating

39 Proposal for a Regulation of the European Parliament and of the Council Laying down Rules to Prevent and Combat Child Sexual Abuse, COM(2022) 209 final, Art. 7(8).
40 See CJEU 6 October 2020, C-511/18, C-512/18 and C-520/18 (La Quadrature Du Net), par. 130 and references quoted there.
41 CJEU 8 April 2014, C-293/12 and C-594/12 (Digital Rights Ireland and Others), par. 48; see also CJEU 6 October 2015, Case C-362/14, par. 78.
42 CJEU 26 January 2023, C-205/21 (V.S. / Ministerstvo Na Vatreshnite Raboti).
43 Ibid, par. 117, 125.
44 CJEU 6 October 2020, C-511/18, C-512/18 and C-520/18 (La Quadrature Du Net), par. 128.
45 Proposal for a Regulation of the European Parliament and of the Council Laying down Rules to Prevent and Combat Child Sexual Abuse, COM(2022) 209 final, Art. 25.

authorities would all have a national remit, while the European Commission in its most recent Rule of Law report concluded that "systemic concerns" remain in some member states when it comes to the rule of law.[46]

If, however, the "fair balance" and "strict necessity"-requirement in the proposal should be interpreted in line with human rights case law, then authorities requesting and issuing a device detection order or an encryption altering order which could extend indiscriminately to all users of the service would likely act in breach of the regulation. This is because such orders cannot be considered to be compatible with the human rights to privacy, data protection and freedom of expression as set out in the Charter, as will be further explained further below.

46 See European Commision, "Press Release: Rule of Law Report 2022: Commission Issues Specific Recommendations to Member States.".

# 3 The detection framework must comply with Article 52 of the Charter

## 3.1 The detection framework limits the rights to privacy, data protection and freedom of expression

The proposal – like any EU law – must comply with Article 52 of the Charter, which requires that any limitation on the rights in the Charter must be provided for by law, respect their essence and be necessary and proportionate to meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.

As noted in the introduction, for this analysis, three of these rights in the Charter are of particular interest. The proposal would create a framework for issuing detection orders. Detection orders have a significant impact on confidential communications, because of the analysis involved.

This analysis of confidential communications limits the exercise of the right to privacy (Article 7 Charter), the right to data protection (Article 8 Charter) and the right to freedom of expression (Article 11 Charter).[47] Because the CJEU often applies these rights in combination, often without clearly distinguishing their application, in the report these will also be discussed together. For completeness, the detection orders may also affect other fundamental rights, such as the freedom of assembly and association (Article 12), the freedom to conduct a business (Article 16), the right to property (Article 17) and the right to non-discrimination (Article 21). These are, however, outside of the scope of this analysis.

## 3.2 The detection framework must respect the essence of the fundamental rights

As noted, any limitation on the exercise of the rights to privacy, data protection and freedom of expression must respect the essence of those rights. If it can be concluded that a limitation does not respect the essence, then it does not need to be considered whether the limitation is proportionate: it should already be considered incompatible with Article 52 of the Charter.

Two cases from the CJEU are relevant for determining how this concept of the "essence" relates to confidential communications. The CJEU in *Schrems I* considered that legislation permitting the public authorities access on a generalised basis to the content of communications compromises the essence of the right to privacy under the Charter and so never can be lawful.[48] By contrast, it can be inferred from the CJEU-decision in *La Quadrature* that the automated analysis of traffic and location data of all users of electronic communications systems for a strictly limited period, is a particularly serious interference, but should not be considered to affect this essence.[49] That meant that the limitation could be examined, to see if it was proportionate.

47 See e.g. CJEU 8 April 2014, C-293/12 and C-594/12 (Digital Rights Ireland and Others); CJEU 6 October 2015, C-362/14 (Schrems I); and CJEU 6 October 2020, C-511/18, C-512/18 and C-520/18 (La Quadrature Du Net).
48 CJEU 6 October 2015, C-362/14 (Schrems I), par. 94.
49 CJEU 6 October 2020, C-511/18, C-512/18 and C-520/18 (La Quadrature Du Net), par. 178.

It would be wrong to conclude from these considerations that the surveillance of metadata of communications, or "behavioral data", would be less problematic than the surveillance of content of communications. Behavioral data can paint a very detailed picture of a person – even more detailed than what could be constructed on the basis of "content". In fact, the European Court of Human Rights in *Big Brother Watch* (2021) also suggested that the interference with regard to both content and metadata is equally severe.[50]

This is also relevant in the context of analysis through *hashes* of communications. Using hashes has significant advantages for protecting the privacy of victims of sexual abuse, because it is difficult to reconstruct the original image from a hash. From a fundamental rights perspective, however, the analysis of hashed interpersonal communications is materially the same as the analysis of unhashed interpersonal communications: it still requires a form of analysis of *all* communications, albeit in a translated, hashed form. This is why, for the rest of this analysis, no distinction is made between the analysis of metadata, content or hashes – instead, the report refers to the analysis of communications where possible.

### 3.3 The detection framework must be proportionate to the aim

Not only must the proposal respect the essence of the fundamental rights that it limits; it must also be proportionate to its aim. For purposes of this analysis, the assessment framework developed by the CJEU in *Digital Rights Ireland* and *La Quadrature du Net* is relevant.

The framework firstly requires the powers to be clearly circumscribed. According to the CJEU, EU legislation 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 data are affected have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data.[51] Safeguards are even more important where personal data is subjected to automatic processing, where there is a significant risk of unlawful access to those data or where sensitive data are at stake.[52] Furthermore, in *La Quadrature*, as already noted, the CJEU in the context of the protection of children's rights established that a legal framework should be established enabling a balance to be struck between the various interests and rights to be protected.[53] Based on these considerations, it can be concluded that, where the interference is potentially more serious, or the risk of abuse is more present, an even higher standard of clarity with regard to the scope and application of these measures is required.

Not only must the powers be clearly circumscribed; a measure must also be sufficiently connected to its objective. In *La Quadrature du Net*, the CJEU considered that "legislation requiring the retention of personal data must always meet objective criteria that establish a connection between the data to be retained and the objective pursued."[54] Similarly, The CJEU in *Digital Rights Ireland* in its proportionality assessment attached importance to whether there was a link between the measures and the purported aim.[55] Criteria through which this link can be established are, for example, limitations in terms of people, data, time, geographic region, and access to surveilled data.

50 ECHR 25 May 2021, Applications nos. 58170/13, 62322/14 and 24960/15 (Big Brother Watch and Others v. United Kingdom), par. 342, 363.
51 CJEU 8 April 2014, C-293/12 and C-594/12 (Digital Rights Ireland and Others), par. 54; CJEU 6 October 2020, C-511/18, C-512/18 and C-520/18 (La Quadrature Du Net), par. 132.
52 CJEU 8 April 2014, C-293/12 and C-594/12 (Digital Rights Ireland and Others), par. 55; CJEU 6 October 2020, C-511/18, C-512/18 and C-520/18 (La Quadrature Du Net), par. 132.
53 CJEU 6 October 2020, C-511/18, C-512/18 and C-520/18 (La Quadrature Du Net), par. 128.
54 Ibid, par. 133.
55 CJEU 8 April 2014, C-293/12 and C-594/12 (Digital Rights Ireland and Others), par. 57-64.

The CJEU in *La Quadrature* further explained how this requirement of a connection works in the context of an obligation on providers to retain certain data for surveillance purposes. In short, the more important the objective, the less of a connection to the measure is required.

For instance, when the objective is the safeguarding of the highly important objective of *national security*, the requirement of a connection does not, in principle, preclude the mandatory retention of traffic and location data of all users of electronic communications systems for a limited period of time, as long as there is sufficiently solid evidence of a serious, genuine, present or foreseeable threat to national security.[56] According to the CJEU, even if this measure is applied indiscriminately to all users, without there being at first sight any connection with a threat to the national security of that Member State, the existence of that threat is, in itself, capable of establishing that connection.

By contrast, when the objective is *combating serious crime* and *preventing serious threats to public security*, the retention of traffic and location data must be *targeted* in order for it to be allowed – such retention must be limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.[57] The limits may be set according to the categories of persons concerned, whose traffic and location data are likely to reveal a link, at least an indirect one, with serious criminal offences.[58] The limits may also be set using a geographical criterion, restricted to regions where there is high risk of preparation for or commission of serious criminal offences, such as places with a high incidence of serious crime, places that are particularly vulnerable to the commission of serious criminal offences, or strategic locations.[59]

Finally, where the objective is to combat *criminal offences in general*, e.g. not only "serious" crime, then the interference need not be serious either, and this would for example allow for the retention of civil identification information – e.g. contact details, such as addresses – of all users of electronic communications services, without imposing a specific time limit.[60]

Finally, the case on the collection of biometric and genetic data, also discussed under the header of "strict necessity" above, bears mentioning here as well. In that case, the CJEU considered that the systematic, indiscriminate and generalised collection of biometric and genetic data of any person accused of an offence could not be considered "strictly necessary."[61]

To be clear: it is not useful to read into these considerations sharp distinctions between the different objectives and the kinds of measures which are allowed. Rather, these considerations should be understood as examples of underlying principles, involving, in short, an interplay between the objective of a measure, the seriousness of the interference, and the connection between the objective and the measure itself.[62] The next question is, how these principles would apply to the detection framework in the proposal.

56 CJEU 6 October 2020, C-511/18, C-512/18 and C-520/18 (La Quadrature Du Net), par. 137.
57 Ibid, par. 147.
58 Ibid, par. 148.
59 Ibid, par. 150.
60 Ibid, par. 159.
61 CJEU 26 January 2023, C-205/21 (V.S. / Ministerstvo Na Vatreshnite Raboti), par. 128, 129.
62 See to that end CJEU 6 October 2020, C-511/18, C-512/18 and C-520/18 (La Quadrature Du Net), par. 131.

# 4 The detection framework and some potential orders do not comply with Article 52 of the Charter

## 4.1 The detection framework and some potential orders do not respect the essence

As noted above, the legislative framework in the proposal allows for issuing orders to analyse confidential communications of all users of a communications service, on an automated basis, and even on the device. Detection orders can be issued relating to a *service*, on the basis of the risk that this service will be used for online child sexual abuse. As explained above, these "service-based" detection orders can be untargeted in terms of persons whose communications will be analysed. They can further require the analysis of all communications from a user, and given the scale of the use of communications services, this will have to be automated. Finally, this detection may have to take place on the device, because of the end-to-end encryption which is applied by most of these services.

As discussed above, the CJEU has in the past clarified that access to the content of confidential communications on a generalised basis, that is, without targeting specific users, does not respect the essence of these rights. Because of this, a good argument can be made that an order to analyse confidential communications of all users of a communications service, on an automated basis, and even on the device, does not respect the essence of the rights to privacy, data protection and freedom of expression under the Charter. As a consequence, the *legal framework* which allows for such orders should also not be considered to respect the essence of these rights.

Already on that basis, the legal framework, and the broad detection orders it allows for, should be considered incompatible with the Charter, and a further proportionality assessment is not necessary.

## 4.2 The detection framework and some potential orders are not proportionate

However, even if one should conclude that the legal framework and the potential orders which can be issued respect the essence of the relevant rights, these do not meet the criteria of proportionality under the Charter. Firstly, it is required that the detection framework lays down clear and precise rules governing their scope and application and imposing minimum safeguards so that the persons whose data are affected have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data.

It is questionable whether the detection framework meets this threshold. The framework for issuing these orders contains certain safeguards against abuse, but as discussed above, it is uncertain whether these would in practice prevent the issuing of disproportionate orders. This is particularly problematic because a higher standard of clarity with regard to the scope and application of an order is required where the interference is serious, because the risk of abuse is higher. In this case, the risk of abuse is very high: detection orders would allow authorities and providers to (indirectly) monitor confidential communications, a power which could easily be overstepped. And both a device detection order and an encryption altering order would introduce new avenues for other parties – such as foreign governments or malicious individuals – to gain unlawful access. This, by the way, is also in tension with member states' positive obligations

to take measures to reduce the risk of unlawful access to confidential communications under the rights to privacy, data protection and communications freedom, but this avenue will not be further explored in this study.

Further, as noted above, the proposal must strike the right balance between the objective of a measure, the seriousness of the interference, and the connection between the objective and the measure. The aim of the proposal is to combat sexual child abuse, which is a serious crime, also in view of the human rights of the child involved. This would justify a more serious interference.

Even then, however, the kinds of indiscriminate orders which may be issued under the legal framework are not proportionate to this aim. Firstly, they are directed at the *service*. The connection between the objective, the combating of child sexual abuse online, and the measure, the analysis of all communications on this service, is remote. Meanwhile, the interference is very serious: it potentially affects all users of a service and affects all their communications via that service. These communications may contain highly sensitive data and are central to the exercise of the rights to privacy, data protection and free expression in the modern age. The detection would be performed on an automated basis, something the the CJEU has considered to further contribute to the seriousness of an interference. And as noted, it may even be done on the device, a domain which should be accorded even more protection in view of its private nature. Finally, orders which change the encryption which is applied, so that communications can be analysed in transit, would increase the risk of unlawful access to confidential communications of all users.

As noted above, the CJEU in *La Quadrature* has discussed the possibility of surveillance for safeguarding national security, a domain where the Court considers that more indiscriminate surveillance would under certain strictly described circumstances be considered proportionate. Even in the context of national security, however, a "serious threat" is required for indiscriminate measures to be imposed.[63] By contrast, the legal framework under the proposal provides for the possibility issue detection orders where there is a "significant risk", a decidedly lower and not well-defined threshold, while the objective, the combating of child sexual abuse, is highly important but does not rise to the level of national security.

Finally, it is worth discussing whether certain forms of detection via matching of hashes would be more "targeted" as the term is used by the CJEU. This does not appear to be the case. In order for the hashing to work, *all* information which is subject of this matching must be analysed. The fact that the analysis goes through an intermediate step of comparing hashes does not make this analysis less salient. The fact that, in the case of known CSAM, the hashes against which the communications are matched are "specific" does not make the analysis more targeted; it would still apply to all users of a service, and to all their communications on that service.

As a result, the proposed legal framework for issuing detection orders and the potential detection orders which may be issued under that framework should be considered incompatible with the rights to privacy, data protection and communications freedom under the Charter.

63 Ibid, par. 137.

**IViR - Institute for Information Law**
**P.O. Box 15514, 1001 NA Amsterdam, the Netherlands**

**https://www.ivir.nl/**