Hamburg, March 2021

Legal opinion

commissioned by MEP Patrick Breyer,

The Greens/EFA Group in the European Parliament

1. Having regard to the relevant case-law, would EU legislation obliging providers of number-independent electronic communication services (i.e., e-mail, messaging, chat) to generally and indiscriminately screen the content of all private correspondence for 'child pornography' and report hits to the police comply with fundamental rights?

2. What if end-to-end encrypted communications were included in the scope of obligation?

3. Would the answer given to question 1 change if the providers were allowed instead of obliged to take the measures set out in question 1?

Prof. Dr. Ninon Colneric

Table of Contents

1. Context of analysis 2

2. Scope of commission for legal opinion and course of investigation 4

3. Empirical material relating to 'child pornography' 4

3.1. Consequences of child sexual abuse 4

3.2. Online 'child pornography' 5

3.3. Measures to fight online 'child pornography' 6

4. Relevant provisions of EU law 7

4.1. General provisions of EU law 7

4.2. Relevant rights guaranteed by the Charter 9

5. Legal assessment (end-to-end encrypted communications not included) 12

5.1. Preliminary remark 12

5.2. Violation of Articles 7 (Respect for private and family life), 8 (Protection of personal data) and 11 (Freedom of expression and information) of the Charter? 14

5.2.1. Existence of an interference? 14

5.2.2. Justification? 15

5.2.2.1. Provided for by law? 15

5.2.2.2. Respecting the essence? 17

5.2.2.3. Legitimate aim? 20

5.2.2.4. Proportionate to the legitimate aim pursued? 22

5.3. Violation of Article 16 (Freedom to conduct a business) of the Charter? 29

6. End-to-end encryption 29

7. Legal assessment (end-to-end encrypted communications included) 31

8. Legal assessment for permission instead of obligation 33

9. Conclusions 34

Chronological List of Cited Cases 35

About the Author 37

1. Context of analysis

On 24 July 2020, the EU Commission ('Commission') presented a Communication setting out an EU strategy for a more effective fight against child sexual abuse[1] ('Communication'). The Communication highlights that the introduction of end-to-end encryption, while beneficial in ensuring privacy and security of communications, also facilitates the access to secure channels for perpetrators where they can hide their actions from law enforcement, such as trading images and videos. It concludes:

> 'The use of encryption technology for criminal purposes therefore needs to be immediately addressed through possible solutions which could allow companies to detect and report child sexual abuse in end-to-end encrypted electronic communications. Any solution would need to ensure both the privacy of electronic communications and the protection of children from sexual abuse and sexual exploitation, as well as the protection of the privacy of the children depicted in the child sexual abuse material.'[2]

Under the heading 'Ensure that EU legislation enables an effective response', the Commission announces two key actions:

> 'In a first stage, **as a matter of priority**, the Commission will propose the necessary legislation to ensure that providers of electronic communications services can continue their current voluntary practices to detect in their systems child sexual abuse after December 2020.
>
> In a second stage, by Q2 2021, the Commission will propose the necessary legislation to tackle child sexual abuse online effectively including by requiring relevant online services providers to detect known child sexual abuse material and require them to report that material to public authorities.'[3]

The Commission declares that it will work towards the creation of a European centre to prevent and counter child sexual abuse.[4] One of the suggested functions of such a centre is to 'support companies by, for example, maintaining a single database in the EU of known child sexual abuse material to facilitate its detection in companies' systems, in compliance with EU data protection rules'.[5]

Another key action set out in the Communication is described as follows:

---

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: EU strategy for a more effective fight against child sexual abuse, COM(2020) 607 final, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf . Retrieved 9 February 2020.

[2] *Ibid.*, p. 2.

[3] *Ibid.*, p. 6.

[4] *Ibid.*, p. 14.

[5] *Ibid.*, p. 13.

> 'Under the EU Internet Forum, the Commission has launched an expert process with industry to map and preliminarily assess, by the end of 2020, possible technical solutions to detect and report child sexual abuse in end-to-end encrypted electronic communications, and to address regulatory and operational challenges and opportunities in the fight against these crimes.'[6]

In a press statement on the Communication of 24 July 2020, Commissioner Johannsson declared:

> 'We are announcing today that next year, the Commission will propose new legislation to make it mandatory for relevant internet and social media messaging companies to detect, report and remove materials, and refer them to appropriate authorities.'[7]

Meanwhile, the Commission has submitted a Proposal for a Regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online.[8] This measure was triggered by the fact that, with effect from 21 December 2020, the European Electronic Communications Code [9] introduced a new definition of electronic telecommunication services which includes number-independent interpersonal communication services such as voice over IP, messaging and web-based e-mail services. As a result, from that date, such services fall within the scope of the Directive 2002/58/EC[10], the so-called e-Privacy Directive.

According to Article 1 of the proposed regulation, its objective is to enable providers of number-independent interpersonal communications services to continue the use of technologies for the processing of personal and other data to the extent necessary to detect and report child sexual abuse online and remove child sexual abuse material on their services. Recital 16 of the proposal announces the adoption of a new long-term legal framework with more elaborate safeguards, the second stage of the plans for legislation set out in the Communication.

It is in this context that the present legal opinion was commissioned.

---

[6] *Ibid.*, p. 16.

[7] https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1413. Retrieved 9 February 2021.

[8] COM(2020) 568 final of 10 September 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0568&from=EN . Retrieved 9 February 2021.

[9] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36).

[10] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

2. Scope of commission for legal opinion and course of investigation

Question 1 focusses on 'child pornography'. Since a hypothetic action of the EU legislator is to be analysed, it seems appropriate to apply the definition of this term contained in Article 2 point (c) of Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combatting the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.[11] It reads as follows:

> '"child pornography" means:
>
> (i) any material that visually depicts a child engaged in real or simulated sexually explicit conduct;
> (ii) any depiction of the sexual organs of a child for primarily sexual purposes;
> (iii) any material that visually depicts any person appearing to be a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of any person appearing to be a child, for primarily sexual purposes; or
> (iv) realistic images of a child engaged in sexually explicit conduct or realistic images of the sexual organs of a child, for primarily sexual purposes.'

The opinion will not deal with 'pornographic performances' within the meaning of Article 2 point (e) of Directive 2011/93/EU. Nor will text-based child grooming be covered. Consequently, only images and videos not showing a live exhibition will be included.

This legal opinion is structured as follows: The first main section presents empirical material relating to 'child pornography' (*infra* 3). The next section literally reproduces relevant provisions of EU law and, insofar as the Charter of Fundamental Rights of the European Union is concerned, the explanations drawn up as a way of providing guidance in its interpretation (*infra* 4). Subsequently, the first question to be answered will be examined, end-to-end encrypted communications not included (*infra* 5). After some brief empirical remarks on end-to-end encryption (*infra* 6), the second question will be analysed (*infra* 7). The opinion closes with a short summary (*infra* 8).

3. Empirical material relating to 'child pornography'

3.1. Consequences of child sexual abuse

In essence, 'child pornography' is child sexual abuse imagery. Child sexual abuse can have wide-ranging and serious life-long consequences. It has been correlated with higher levels of depression, guilt, shame, self-blame, eating disorders, somatic concerns, anxiety, dissociative patterns, sexual problems, and relationship problems.[12] Victims face a heightened risk of

[11] OJ L 335, 17.12.2011, p. 1.

[12] See *Hall, Melissa, and Hall, Joshua (2011)*, The Long-Term Effects of Childhood Sexual Abuse: Counseling Implications, and literature cited, https://www.counseling.org/docs/disaster-and-trauma_sexual-abuse/long-term-effects-of-childhood-sexual-abuse.pdf?sfvrsn=2 . Retrieved 9 February 2021.

substance abuse and suicide.[13] Depending on the age of the child and the force used, child sexual abuse may cause internal lacerations, bleedings and, in severe cases, damage to internal organs, which may lead to death.[14] Other potential consequences of abuse are infections with sexually transmitted diseases and unwanted pregnancies.

3.2. Online 'child pornography'

The internet has opened a rapidly growing global market for the production, distribution and consumption of child sexual abuse materials, such as photographs and videos.[15] As the German Bundeskriminalamt (Federal Criminal Police Office) put it:

> 'Child pornography on the Internet is an offence of international dimension. More and more state borders are losing significance – the exchange of data over long distances is unproblematic and possible within a matter of seconds. A circumstance which is causing the law enforcement agencies in Germany, but also throughout the world, to be confronted with enormous challenges.'[16]

In the United States, the National Center for Missing and Exploited Children (NCMEC), a private, non-profit organisation, plays a key role in combatting child sexual abuse. Under US law, United States-based electronic communications providers and remote computing service providers are obliged to report child abuse material that has come to their attention to NCMEC.[17] After reviewing it, that organisation will forward the reports to domestic and foreign law enforcement agencies. From 2008 to 2017, NCMEC has transformed from a regional reporting body to a world-wide clearing house with 68 % of its reports relating to Asia[18], 19 % to Americas, 6 % to Europe and 7 % to Africa.[19]

According to a New York Times report of September 2019[20], tech companies reported more than 45 million photographs and videos of children being sexually abused to NCMEC in 2018. Report growth has been exponential.[21]

---

[13] *Bursztein, Elie, and others* (2019), Rethinking the Detection of Child Sexual Abuse Imagery on the Internet, section 1, https://web.archive.org/web/20190928174029/https://storage.googleapis.com/pub-tools-public-publication-data/pdf/b6555a1018a750f39028005bfdb9f35eaee4b947.pdf . Retrieved 9 February 2021.

[14] *Anderson, James; Mangels, Nancie; Langsam, Adam (2004)*, Child Sexual Abuse: A Public Health Issue. Criminal Justice Studies. 17: 107-126. https://www.tandfonline.com/doi/abs/10.1080/0888431042000167938 6?journalCode=gjup20. Retrieved 9 February 2020.

[15] https://www.unicef.org/protection/sexual-violence-against-children. Retrieved 9 February 2020.

[16] https://www.bka.de/EN/OurTasks/AreasOfCrime/ChildPornography/childpornography_node.html. Retrieved 9 February 2020.

[17] See in particular 18 USC 2258A. Reporting requirements of providers, https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section2258A&num=0&edition=prelim. Retrieved 9 February 2020.

[18] China is absent from that dataset, *Bursztein, Elie, and others* (no 13), section 3.2.

[19] *Ibid.*, section 4.2.

[20] https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html . Retrieved 9 February 2020.

[21] *Bursztein, Elie, and others* (no 13), section 4.1.

3.3. Measures to fight online 'child pornography'

The Communication gives a good overview of techniques used to fight child sexual abuse both off- and online.

According to that document, the use of online undercover investigation techniques is an important asset in infiltrating the networks that are concealed behind digital technology. The Commission considers that these methods have proven very effective in understanding offender behaviour and interaction on online service providers and have ultimately facilitated the shutting down of communication channels used by the offenders, as well as their prosecution.[22]

As technology has been playing a paramount role in extending the crime of child sexual abuse, technology-led approaches are increasingly being developed to fight it. Several number-independent interpersonal communication services have voluntarily set up specific technology to detect and remove child abuse material online within their services.[23]

One type of technology works by creating cryptographic hashes (unique alphanumeric strings) of previously identified child sexual abuse material. Such hashes, which cannot be converted back into the original images and do not include any personal data, are stored in a database. Images and videos uploaded to a service provider's server are also hashed in this way. Then they are compared with the hashes stored in the database. Due to the unique nature of these hashes, if there is a match, it is an almost 100 % guarantee that the image or video contains child sexual abuse material. This kind of technology is only apt for identifying already known child sexual abuse material.[24]

Another type of technology is equally based on known child sexual abuse material. However, here the provider does not use cryptographic hashes but perceptual hashing algorithms, so-called pHash. Again, the hashes are compared with the hashes stored in a database. When images or videos are similar to each other, the perceptual hashes generated for those images or videos are mathematically close to each other. Thus, this method does not only allow for the detection of known child sexual abuse material (identity with the material in the database) but also of unknown material of this kind based on the features found in known child sexual abuse material (similarity to the material in the database).[25]

[22] Communication, p. 8.
[23] European Parliamentary Research Service, Commission proposal on the temporary derogation from the e-Privacy Directive for the purpose of fighting online child sexual abuse – Targeted substitute impact assessment (February 2021) ('EPRS impact assessment'), p. 2. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662598/EPRS_STU(2021)662598_EN.pdf . Retrieved 13 February 2021.
[24] *Ibid.*, p. 15.
[25] *Ibid.*, pp. 16 f.

A study of 23.4 million incidents of child sexual abuse imagery on the internet, elaborated in cooperation with NCMEC, shows that the public and the electronic service providers based in the US report 84 % of images and 91 % of videos only a single time.[26]

The same paper states that the exponential growth of child sexual abuse imagery on the internet threatens our society's ability to combat online child abuse as the rate at which abusive content emerges vastly outpaces the processing capabilities of clearing houses and law enforcement agencies. The authors consider that the development of detection and processing technologies substantially lags behind the development of content creation and sharing capabilities. They argue that researchers need to develop algorithms that automatically detect child sexual abuse imagery, cluster images and videos of victims, and ultimately surface identifying features to help law enforcement. Absent new protections, society would be unable to adequately protect victims of child sexual abuse.[27]

4. Relevant provisions of EU law

4.1. General provisions of EU law

According to Article 6(1) of the Treaty on European Union ('TEU'), the Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007 ('Charter'), which shall have the same legal value as the TEU and the Treaty on the Functioning of the European Union ('TFEU'). The rights, freedoms and principles in the Charter shall be interpreted in accordance with the general provisions in Title VII of the Charter governing its interpretation and application and with due regard to the explanations referred to in the Charter, that set out the sources of those provisions.[28]

Article 6(3) TEU states that fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms ('ECHR') and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law.

Article 51(1) of the Charter, headed 'Field of application', reads as follows:

> 'The provisions of this Charter are addressed to the institutions, bodies, offices and agencies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law. They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers and respecting the limits of the powers of the Union as conferred on it in the Treaties.'

Article 52 of the Charter, headed 'Scope and interpretation of rights and principles', provides:

[26] *Bursztein, Elie, and others* (no 13), section 6.5.
[27] *Ibid*., section 5.
[28] Article 6(1), third paragraph, TEU.

‘1. Any limitation on the exercise of the rights and freedoms recognised by this charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

2. Rights recognised by this Charter for which provision is made in the Treaties shall be exercised under the conditions and within the limits defined by those Treaties.

3. In so far as this Charter contains rights which correspond to rights guaranteed by the [ECHR], the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.

…

7. The explanations drawn up as a way of providing guidance in the interpretations of this Charter shall be given due regard by the courts of the Union and of the Member States.’

The explanation on Article 52 of the Charter reads as follows:

‘The purpose of Article 52 is to set the scope of the rights and principles of the Charter, and to lay down rules for their interpretation. Paragraph 1 deals with the arrangements for the limitation of rights. The wording is based on the case-law of the Court of Justice: ‘... it is well established in the case-law of the Court that restrictions may be imposed on the exercise of fundamental rights, in particular in the context of a common organisation of the market, provided that those restrictions in fact correspond to objectives of general interest pursued by the Community and do not constitute, with regard to the aim pursued, disproportionate and unreasonable interference undermining the very substance of those rights’ (judgment of 13 April 2000, Case C-292/97, paragraph 45 of the grounds). The reference to general interests recognised by the Union covers both the objectives mentioned in Article 3 of the Treaty on European Union and other interests protected by specific provisions of the Treaties such as Article 4(1) of the [TEU] and Articles 35(3), 36 and 346 of the [TFEU].

Paragraph 2 refers to rights which were already expressly guaranteed in the Treaty establishing the European Community and have been recognised in the Charter, and which are now found in the Treaties (notably the rights derived from Union citizenship). It clarifies that such rights remain subject to the conditions and limits applicable to the Union law on which they are based, and for which provision is made in the Treaties. The Charter does not alter the system of rights conferred by the EC Treaty and taken over by the Treaties.

Paragraph 3 is intended to ensure the necessary consistency between the Charter and the ECHR by establishing the rule that, in so far as the rights in the present Charter also

correspond to rights guaranteed by the ECHR, the meaning and scope of those rights, including authorised limitations, are the same as those laid down by the ECHR. This means in particular that the legislator, in laying down limitations to those rights, must comply with the same standards as are fixed by the detailed limitation arrangements laid down in the ECHR, which are thus made applicable for the rights covered by this paragraph, without thereby adversely affecting the autonomy of Union law and of that of the Court of Justice of the European Union ['CJEU'].

The reference to the ECHR covers both the Convention and the Protocols to it. The meaning and the scope of the guaranteed rights are determined not only by the text of those instruments, but also by the case-law of the European Court of Human Rights ['ECtHR'] and by the [CJEU]. The last sentence of the paragraph is designed to allow the Union to guarantee more extensive protection. In any event, the level of protection afforded by the Charter may never be lower than that guaranteed by the ECHR.

…'

4.2. Relevant rights guaranteed by the Charter

Article 3(1) of the Charter, headed 'Right to integrity of the person', provides:

'Everyone has the right to respect for his or her physical and mental integrity.'

The explanation on Article 3 of the Charter states:

'1. In its judgment of 9 October 2001 in Case C-377/98 *Netherlands v European Parliament and Council* [2001] ECR-I 7079, at grounds 70, 78 to 80, the Court of Justice confirmed that a fundamental right to human integrity is part of Union law …

…'

Article 4 of the Charter reads as follows:

'No one shall be subjected to torture or to inhuman or degrading treatment or punishment.'

The explanation on Article 4 of the Charter states:

'The right in Article 4 is the right guaranteed by Article 3 of the ECHR, which has the same wording: ... By virtue of Article 52(3) of the Charter, it therefore has the same meaning and the same scope as the ECHR Article.'

Article 6 of the Charter, headed 'Right to liberty and security', reads as follows:

'Everyone has the right to liberty and security of person.'

The explanation on Article 6 of the Charter states:

'The rights in Article 6 are the rights guaranteed by Article 5 of the ECHR, and in accordance with Article 52(3) of the Charter, they have the same meaning and scope. …'

Article 7 of the Charter, headed 'Respect for private and family life', provides:

> 'Everyone has the right to respect for his or her private and family life, home and communications.'

The explanation on Article 7 of the Charter is worded as follows:

> 'The rights guaranteed in Article 7 correspond to those guaranteed by Article 8 of the ECHR. To take account of developments in technology the word "correspondence" has been replaced by "communications".
>
> In accordance with Article 52(3), the meaning and scope of this right are the same as those of the corresponding article of the ECHR. Consequently, the limitations which may legitimately be imposed on this right are the same as those allowed by Article 8 of the ECHR:
>
> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."'

Article 8 of the Charter, headed 'Protection of personal data', reads as follows:

> '1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specific purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.'

Article 8(1) of the Charter corresponds to Article 16(1) TFEU, which provides that everyone has the right to the protection of personal data concerning them.

The explanation on Article 8 of the Charter states:

> 'This Article has been based on Article 286 of the Treaty establishing the European Community and Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal date and on the free movement of such data (OJ L 281, 23.11.1995, p. 31) as well as on Article 8 of the ECHR and on the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which has been ratified by all the Member States. Article 286 of the EC Treaty is now replaced by Article 16 of the [TFEU] and Article 39 of the [TEU]. Reference is also made to Regulation (EC)

N. 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1). The above-mentioned Directive and Regulation contain conditions and limitations for the exercise of the right to the protection of personal data.'

Article 11(1) of the Charter, headed 'Freedom of expression and information', provides:

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

The explanation on Article 11(1) of the Charter reads as follows:

'Article 11 corresponds to Article 10 of the European Convention on Human Rights, which reads as follows:

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

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

Pursuant to Article 52(3) of the Charter, the meaning and scope of this right are the same as those guaranteed by the ECHR. The limitations which may be imposed on it may therefore not exceed those provided for in Article 10(2) of the Convention, ... '

Article 16 of the Charter, headed 'Freedom to conduct a business', provides:

'The freedom to conduct a business in accordance with Union law and national laws and practices is recognised.'

The explanation on Article 16 of the Charter states:

'This Article is based on Court of Justice case-law which has recognised freedom to exercise an economic or commercial activity (see judgments …) and Article 119(1) and (3) of the [TFEU], which recognises free competition. Of course, this right is to be exercised with respect for Union law and national legislation. It may be subject to the limitations provided for in Article 52(1) of the Charter.'

Article 24 of the Charter, headed 'The rights of the child', provides:

> ‘1. Children shall have the right to such protection and care as is necessary for their well-being. …
>
> 2. In all actions relating to children, whether taken by public authorities or private institutions, the child’s best interest must be a primary consideration.
>
> …’

The explanation on Article 24 of the Charter is worded as follows:

> ‘This Article is based on the New York Convention on the Rights of the Child signed on 20 November 1989 and ratified by all Member States, particularly Articles 3, 9, 12 and 13 thereof.
>
> …’

5. Legal assessment (end-to-end encrypted communications not included)

5.1. Preliminary remark

The commission for this legal opinion refers to ‘fundamental rights’ without any further specification. Thus, the question as to which source of fundamental rights should be considered arises.

Whilst, as Article 6(3) TEU confirms, fundamental rights recognised by the ECHR constitute general principles of the European Union’s law and whilst Art. 52(3) of the Charter requires rights guaranteed by the ECHR to be given the same meaning and scope as those laid down by the ECHR, the latter does not constitute, as long as the European Union has not acceded to it, a legal instrument which has been formally incorporated into European Union law.[29] In those circumstances, the CJEU has held that the interpretation of EU law and examination of the legality of EU legislation must be undertaken in the light of the fundamental rights guaranteed by the Charter.[30]

Consequently, this expert opinion will include the ECHR only where EU law refers to it.

This raises the question of how to interpret the reference to the ECHR contained in Article 52(3) of the Charter when limitations on the exercise of the rights and freedoms recognised by the Charter are concerned.

According to the explanation on Article 7 of the Charter, the limitations which may legitimately be imposed on the right guaranteed by this Article are the same as those allowed by Article 8 of the ECHR. The ECtHR held that the notion of ‘necessity’ within the meaning of Article 8(2) of the ECHR implies that a ‘pressing social need’ is involved and that the measure employed is ‘proportionate to the legitimate aim pursued’.[31] The national authorities enjoy a margin of

[29] Judgment of 26 February 2013, *Åkerberg Fransson*, C-617/10, EU:C:2013:105, paragraph 55.
[30] Judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, EU:C:2020:559, paragraph 98.
[31] See, *inter alia*, judgment of 24 November 1986, *Gillow v. the United Kingdom*, no. 9063/80, CE:ECHR:1986:1124JUD000906380, § 55.

appreciation, 'the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved'.[32]

In its judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, C-138/01 and C-139/01,[33] delivered before the entry into force of the Charter, the CJEU referred to Article 6(2) EU, which corresponds to Article 6(3) TEU, and went on to assess whether the right to respect for private life had been violated, on the basis of Art. 8(2) of the ECHR as interpreted by the ECtHR.[34] It concluded that it had to balance the legitimate aim pursued against the seriousness of the interference with the right of the persons concerned to respect for their private life.[35]

Following this approach, two different provisions would have to be applied for assessing whether Articles 7 and 8 of the Charter were violated: As regards Article 7 of the Charter, the starting point would be Article 8(2) of the ECHR because Article 7 of the Charter corresponds to Article 8 of the ECHR. For Article 8 of the Charter, the starting point would be Article 52(1) of the Charter, as there is no corresponding right in the ECHR.[36] However, the CJEU avoids such a split approach. It uses Article 52(1) of the Charter as a starting point, irrespective of whether Article 7 or Article 8 of the Charter is at stake.[37]

The CJEU explained the role of Article 52(3) of the Charter as follows:

> 'Article 52(3) of the Charter is intended to ensure the necessary consistency between the rights contained in the Charter and the corresponding rights guaranteed in the ECHR, without adversely affecting the autonomy of EU law and that of the [CJEU]. Account must, therefore, be taken of the corresponding rights of the ECHR for the purpose of interpreting the Charter, as the minimum threshold of protection (…).'[38]

Consequently, the legal analysis of limitations imposed on rights recognised by the Charter must proceed from Article 52(1) of the Charter even if rights which correspond to rights guaranteed in the ECHR are concerned.

Another cross-reference is contained in Article 52(2) of the Charter: Rights recognised by the Charter for which provision is made in the TEU and the TFEU shall be exercised under the

[32] See judgment of 26 March 1987, *Leander v. Sweden*, no. 9248/91, CE:ECHR:1987:0326JUD000924881, § 59.
[33] EU:C:2003:294.
[34] Paragraph 83.
[35] Paragraph 84.
[36] However, the ECtHR held that the protection of personal data is of fundamental importance for a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the ECHR. See judgments of 18 April 2013, *M.K. v. France*, no 19522/09, CE:ECHR:2013:0418JUD001952209, § 35, and of 27 June 2017, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finnland*, no. 931/13, CE:ECHR:2017:0627JUD000093113, § 137.
[37] See, e.g., judgment of 9 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, '*Digital Rights*', paragraph 38.
[38] Judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/28 and C-520/18, EU:C:2020:791, '*La Quadrature*', paragraph 124. See also judgments of 22 December 2010, *DEB*, C-2079/09, EU:C:2010:811, paragraph 35, and of 17 December 2020, *Central Israëlitisch Consistorie van België and Others*, C- 336/19, EU:C:2020:1031, paragraph 56.

conditions and within the limits defined by those Treaties. This provision which is intended to ensure the consistency between the Charter and the Treaties is lex specialis in relation to Article 52(1) of the Charter.

The right to protection of personal data is not only enshrined in the Charter but also in Article 16(1) TFEU. However, no additional conditions and limits for the exercise of this right can be derived from that provision of the TFEU.

5.2. Violation of Articles 7 (Respect for private and family life), 8 (Protection of personal data) and 11 (Freedom of expression and information) of the Charter?

EU legislation obliging providers of number-independent electronic communication service to generally and indiscriminately screen the content of all private correspondence for 'child pornography' and report hits to the police ('the measure under consideration') raises questions relating to respect for private life and communications under Article 7 of the Charter, the protection of personal data under Article 8 of the Charter and respect for the freedom of expression under Article 11 of the Charter.

In its case-law concerning data protection, the CJEU does not examine in separate sections whether Articles 7, 8 and 11 of the Charter have been violated.[39] This legal opinion adopts the same approach.

5.2.1. Existence of an interference?

Unlike the specific limitation clause contained in Article 8(2) ECHR, the horizontal limitation clause of the Charter does not use the term 'interference'. Nevertheless, the CJEU repeatedly examined whether there was an interference with the rights laid down in Articles 7 and 8 of the Charter.[40] As rights directed against Union or Member State intervention are concerned, this approach is convincing. The existence of an interference constitutes a limitation of the right concerned.[41]

Any adverse effect of Union or Member State conduct on the scope of protection of a right guaranteed by the Charter is sufficient to constitute an interference. To establish the existence of an interference with the fundamental right to privacy, it does not matter whether the persons concerned have been inconvenienced in any way.[42]

Private electronic correspondence is covered by the notions of 'private life' and 'communications' within the meaning of Article 7 of the Charter. The obligation on providers to screen the content of all private correspondence for 'child pornography' and report hits to the police necessarily strikes at the right to respect for private life and communications. The

[39] See, e.g., judgment *La Quadrature*, paragraphs 113 ff.
[40] See, e.g., judgments of 9 November 2010, *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, EU:C:2010:662, paragraphs 56 to 64, and *'Digital rights*', paragraphs 32 to 37).
[41] See, to this effect, judgment of 17 December 2015, *WebMindLicenses*, C-419/14, EU:C:2015:832, paragraph 71).
[42] Judgment *Digital Rights*, paragraph 33.

same goes for the right of everyone to the protection of personal data concerning him and her, guaranteed by Article 8 of the Charter. Consequently, the measure under consideration constitutes an interference with the rights laid down in Articles 7 and 8 of the Charter.

As for the right to freedom of expression recognised in Article 11 of the Charter, the CJEU held that the retention of traffic and location data is liable to deter users of electronic communications systems from exercising their freedom of expression and that such deterrence may affect, in particular, persons whose communications are subject, according to national rules, to the obligation of professional secrecy and whistleblowers whose actions are protected by Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.[43] Screening the content of all private correspondence is no less of a deterrent to exercising the right to freedom of expression than retention of traffic and location data. Therefore, the measure under consideration also constitutes an interference with the right to freedom of expression.

5.2.2. Justification?

5.2.2.1. Provided for by law?

According to Article 52(1), first phrase, of the Charter, any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law. It follows from Article 52(3) of the Charter that, in so far as Articles 7 and 11 are concerned, this requirement must be interpreted in the light of the corresponding requirements 'in accordance with law' and 'prescribed by law' contained in Articles 8(2) and 10(2) ECHR. [44] According to the case-law of the ECtHR, these expressions not only necessitate compliance with domestic law, but also relate to the quality of that law, requiring it to be compatible with the rule of law.[45] The law should be accessible to the persons concerned and formulated with sufficient precision to enable them – if need be, with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.[46]

The question to be examined in this opinion does not contain any information about the legal form of the measure under consideration. A regulation as well as a directive may be considered. In its judgment *Digital rights*, which concerned a directive[47], the CJEU, after listing the conditions Article 52(1) of the Charter imposes on limitations of rights and freedoms laid down by the Charter, did not spend a single sentence on the problem of whether the limitation was provided for by law.[48] As directives are listed under the legal acts of the EU in Article

[43] Judgment *La Quadrature*, paragraph 118.
[44] See, to this effect, judgment of 5 October 2010, *J.McB*, C-400/10 PPU, EU:C: 2010:582, paragraph 53.
[45] Judgment of 25 June 1997, *Halford v. the United Kingdom*, no. 20605/92, CE:ECHR:1997:0625JUD002060592, § 49.
[46] See judgment of 17 February 2004, *Maestri v. Italy*, no. 39748/98, CE:ECHR:2004:0217JUD003974898, § 30.
[47] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).
[48] See paragraphs 38 ff.

288 TFEU, a coherent interpretation of the Charter and the TEU requires to consider them as 'law' within the meaning of Article 51(1) of the Charter.

To be compatible with the rule of law, the act imposing the limitation must have a legal basis. Article 16(2) TFEU provides a legal basis for rules relating to the protection of individuals with regard to the processing of personal data. However, the measure under consideration does not aim at data protection. Therefore, it could not be based on Article 16(2) TFEU. According to Article 114 TFEU, the EU can adopt measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and the functioning of the internal market. The e-Privacy Directive is based on the predecessor of this provision, Article 95 of the Treaty establishing the European Community. Like this provision, Article 114 TFEU can be used to eliminate obstacles to the exercise of the fundamental economic freedoms, resulting from the lack of a common standard. It is sufficient that such obstacles are likely to arise in future.[49] This can be assumed in the present case as the issue is controversial.

The requirement of accessibility does not raise a problem because regulations and directives which are addressed to all Member States shall be published in the *Official Journal of the European Union* according to Article 297(2) TFEU.

Foreseeability can only be guaranteed to a limited extend when the EU legislator opts for a directive since a directive is binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave the national authorities the choice of form and methods.[50] In that case, the test of foreseeability must be applied to the law of the Member States implementing the directive.

In Case *WebMindLicenses*, C-419/14, where the interception of telecommunications and seizure of emails were challenged, the CJEU set out that the legal basis in national law must be sufficiently clear and precise to comply with the requirement that any limitation of the right guaranteed by Article 7 of the Charter must be provided for by law.[51]

The CJEU adopted a different approach in a case where an EU directive was concerned. With regard to an interference with the rights guaranteed by Articles 7 and 8 of the Charter, the CJEU held that the EU legislation in question 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 have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against unlawful access and use of that data.[52] However, this statement did not concern the problem of foreseeability but the necessity of the measure concerned. The CJEU invoked three judgments of the ECtHR in

[49] See judgment of 5 October 2000, *Germany v. European Parliament and Council*, C-376/98, EU:C:2000:544, paragraph 97.
[50] Article 288 paragraph 3 TFEU.
[51] Paragraph 81.
[52] Judgment *Digital Rights*, paragraph 54.

support of its view by analogy, two of them concerned foreseeability.[53] The third judgment is that of 4 December 2008 in Case *S. and Marper v. the United Kingdom*.[54] In § 99 of this judgment, which is part of the section headed "In accordance with law", the ECtHR stated that it is essential, in the context concerned, as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed ruled rules governing the scope and application of measures, as well as minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness. The ECtHR noted, however, that these questions were in the case concerned closely related to the broader issue of whether the interference was necessary in a democratic society. It dealt with these requirements under that heading.

There can be no doubt that the CJEU would adopt the same approach in the event of a regulation.

In view of the case-law of the CJEU exposed above, the requirement of a sufficient legal basis can be considered fulfilled.

5.2.2.2. Respecting the essence?

According to the first sentence of Art. 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must respect the essence of those rights and freedoms.

It results from the explanation on Article 52 that the source of this requirement is a judgment by the Court of Justice of the European Communities ('ECJ') which stated:

> '… it is well established in the case-law of the Court that restrictions may be imposed on the exercise of fundamental rights … provided that those restrictions in fact correspond to objectives of general interest pursued by the Community and do not constitute, with regard to the aim pursued, disproportionate and unreasonable interference undermining the very substance of those rights.'[55]

The case-law of the CJEU gives some hints on how to interpret the requirement that any limitation must respect the essence of the rights and freedoms concerned.

In its judgment of 14 January 2021, *OM*, C-393/19,[56] the CJEU paraphrased the content of Article 52(1) of the Charter as follows:

> 'In accordance with Article 52(1) of the Charter, limitations may be placed on the exercise of the rights and freedoms enshrined therein, on condition that those

[53] Judgments of 1 July 2008, *Liberty and Others v. the United Kingdom*, no. 58243/00, CE:ECHR:2008:0701JUD005824306, § 62 and 63, and of 4 May 2000, *Rotaru v. Romania*, no. 2341/95, CE:ECHR:2000:0504JUD002834195, § 57 to 59.
[54] Nos 30562/04 and 30566/04, CE:ECHR:2008:1204JUD003056204.
[55] Judgment of 13 April 2000, Karlsson and Others, C-292/97, EU:C:2000:202, paragraph 45.
[56] EU:C:2021:8.

> limitations genuinely correspond to objectives of public interest pursued by the European Union and do not constitute, in relation to the aim pursued, a disproportionate and intolerable interference, impairing the very substance of the right so guaranteed.'[57]

Repeatedly, the CJEU held that the essence of the right concerned was not respected. One example is the case just referred to, which concerned national legislation providing for the confiscation, for the benefit of the State, of property used to commit the offence of smuggling. It was about property belonging to a third party acting in good faith, in the main proceedings a vehicle used to transport the smuggled goods. The CJEU held:

> 'Given that the confiscation of property, that is to say, the definite deprivation of the right of ownership in respect of that property, substantially affects the rights of persons, it must be noted that as regards a third party acting in good faith, who did not know and could not have known that his or her property was used to commit an offence, such confiscation constitutes, in the light of the objective pursued, a disproportionate and intolerable interference impairing the very substance of his or her right to property.'[58]

Two judgments relating to Article 47 of the Charter are along the same lines: The CJEU held that legislation not providing any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter.[59]

In these rulings, the CJEU did not go through the stages of a proportionality test. It immediately concluded that the essence of the right concerned was not respected. The violation of the rights concerned was blatant.

There are other cases where the CJEU affirmed that the essence of the rights and freedoms had been respected. One example is the judgment of 16 July 2020, *Adusbef and Federconsumatori*, C-686/18.[60] It concerned acts adopted by the Bank of Italy as part of its task of prudential supervision of Italian people's banks. These acts raised questions about the compatibility of national provisions in this field with Articles 16 and 17 of the Charter. The CJEU held that the essence of the freedom to conduct a business, guaranteed by Article 16 of the Charter, and of the right to property under Article 17 thereof, is respected by national legislation providing for the ability to limit the redemption of shares in the event of withdrawal

[57] Paragraph 53.
[58] Paragraph 55.
[59] See judgments of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650, paragraph 95, and *Facebook Ireland and Schrems*, C-311/18, paragraph 187.
[60] EU:C:2020:567.

of a shareholder, which is intended to satisfy the condition set out in Article 29(2)(b) of Regulation No 575/2013.[61] It gave the following reasoning:

> 'First, that ability does not lead to a deprivation of property and therefore does not constitute interference that undermines the very substance of the right to property. Second, even if it were concluded that that ability limited the freedom to conduct a business, it respects the essence of the freedom since it does not prevent the exercise of banking activities.'[62]

Another case of this category is *Digital Rights*. The CJEU held:

> 'So far as concerns the essence of the fundamental rights to privacy and the other rights laid down in Article 7 of the Charter, it must be held that, even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference with those rights, it is not such as to adversely affect the essence of those rights given that, as follows from Article 1(2) of the directive, the directive does not permit the acquisition of knowledge of the content of the electronic communications as such.
>
> Nor is that retention of data such as to adversely affect the essence of the fundamental right to protection of personal data enshrined in Article 8 of the Charter, because Article 7 of Directive 200/24 provides, in relation to data protection and data security, that without prejudice to the provisions adopted pursuant to Directives 95/46 and 2002/58, certain principles of data protection and data security must be respected by providers of publicly available electronic communications services or of public communications networks. …'[63]

The CJEU's reasoning regarding Article 7 of the Charter raises the question whether there is an absolute core of fundamental rights inference with which would violate their essence in any individual case. This question must be answered in the negative. There can be no doubt that the CJEU would not consider any confiscation of property used for committing an offence as an intolerable interference impairing the very substance of the right to property although it means the definite deprivation of the right of ownership in respect of that property. Likewise, the *Digital Rights* judgment cannot be understood to mean that any provision permitting the acquisition of knowledge of the content of electronic communications would constitute non-respect of the essence of the rights laid down in Article 7 of the Charter. It results from judgment *WebMindLicenses*, C-419/14, that the justification of such a measure is not excluded.[64]

---

[61] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ 2013 L 176, p. 63.

[62] Paragraph 89.

[63] Judgment *Digital Rights*, paragraphs 39 and 40. See also judgment of 21 December 2016, *Tele2 Sverige and Watson and Others*, C-203/15, EU:C:2016:970, *'Tele2'*, paragraph 101.

[64] See paragraphs 73 f.

The following conclusions can be drawn from this overview:

To state that the essence of the rights and freedoms concerned was not respected is kind of a short-cut for blatant cases. A closer look reveals that violation of the essence is just a sub-category of violation of the principle of proportionality. It is unconceivable that the essence of a right is not respected while the principle of proportionality is observed. The essence of a right guaranteed by the Charter is not respected where the violation of the principle of proportionality is so serious that it is intolerable. The statement that there was non-respect of the essence adds particular weight to the statement of unlawfulness. However, it does not contribute an additional source of unlawfulness. Once a measure violates the principle of proportionality, it is contrary to the Charter without any need to analyse whether it also impairs the essence of the right or freedom concerned.

For these reasons, it is not necessary to answer the question whether the measure under consideration respects the essence of the rights concerned. The decisive test is whether it complies with the principle of proportionality.

5.2.2.3. Legitimate aim?

Article 52(1) of the Charter accepts two kinds of legitimate aims: on the one hand, objectives of general interest recognised by the Union and, on the other hand, the need to protect the rights and freedoms of others.

The question to be examined in this legal opinion does not specify the aim pursued. It will be assumed that the aim is the same as that of the Communication, that is to say, a more effective fight against child sexual abuse.

This is an objective of general interest recognised by the Union. According to Article 3(2) TEU, the Union shall offer its citizens an area of freedom, security and justice, in which the free movement of persons is ensured in conjunction with appropriate measures with respect to, among other things, the prevention and combatting of crime. It results from Article 3(3), second subparagraph, TEU that the Union shall promote the protection of the rights of the child. These rights are also emphasized in Article 3(5) TEU, which addresses the relations of the Union with the wider world. More specifically, the general interest of the Union in fighting child sexual abuse is demonstrated by the Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography[65] and the above-mentioned Directive 2011/93/EU[66] that replaced it. At the same time, the aim of combatting child sexual abuse responds to the need to protect the rights of children recognised in Article 24 of the Charter. According to the first sentence of Article 24(1) of the Charter, children have the right to such protection and care as is necessary for their well-being. Consequently, a more effective fight against child sexual abuse is a legitimate aim under both parts of the second sentence of Article 52(1) of the Charter.

[65] OJ L 13, 20.1.2004, p. 44.
[66] *Supra* 2.

In its case-law, the CJEU considered further rights when analysing whether limitations, in the electronic communication sector, on the exercise of the rights enshrined in Articles 7, 8 and 11 of the Charter could be justified.

The CJEU held that positive obligations of the public authorities may arise from Articles 3 and 4 of the Charter as regards the protection of an individual's physical and mental integrity and the prohibition of torture and inhuman and degrading treatment.[67] However, when a child is concerned, these requirements are already covered by the right of children to such protection and care as is necessary for their well-being. The source of Article 24 of the Charter is the United Nations Convention on the Rights of the Child ('Convention').[68] The Convention contains several provisions aiming at securing the physical and mental integrity of the child. Thus, the State Parties recognize the right of the child to the enjoyment of the highest attainable standard of health (Article 24(1) of the Convention). More specifically, they undertake to protect the child from all forms of sexual exploitation and sexual abuse (Article 34 of the Convention). According to Article 37(a) of the Convention, no child shall be subjected to torture or other cruel, inhumane or degrading treatment or punishment. The right to protection according to the first sentence of Article 24(1) of the Charter comprises protection equivalent to that resulting from these provisions of the Convention. Consequently, there is no need to deal with Articles 3 and 4 of the Charter separately.

As for Article 6 of the Charter, the CJEU underlined, in its judgment *Digital Rights*, that this article lays down the right of any person not only to liberty, but also to security.[69] This was one of the elements on which the CJEU based its conclusion that the measure concerned genuinely satisfied an objective of general interest. In its judgment *La Quadrature*, the CJEU seems to have taken a different view. The Court recalled that account must be taken of the corresponding rights of the ECHR when interpreting the Charter. It stated that Article 5 of the ECHR, which enshrines the 'right to liberty' and the 'right to security', is intended to ensure that individuals are protected from arbitrary or unjustified deprivations of liberty[70] and went on to conclude: 'However, since that provision applies to deprivations of liberty by a public authority, it cannot be interpreted as imposing an obligation on public authorities to take specific measures to prevent and punish certain criminal offences.'[71] In other words, the CJEU interpreted the 'right to liberty and security' as just referring to protections against arbitrary or unjustified deprivations of liberty by a public authority. This restrictive interpretation of the right to security is in line with the case-law of the ECtHR.[72]

[67] Judgment *La Quadrature*, paragraph 126.
[68] New York, 20 November 1989, United Nations, *Treaty Series*, vol. 1577, p. 3.
[69] Paragraph 42.
[70] See also ECtHR, judgment of 14 October 1999, *Riera Blume and Others v. Spain*, no. 37680/97, CE:ECHR:1999:003768097, § 28.
[71] Judgment *La Quadrature*, paragraphes 124 f.
[72] See, e.g., judgment of 20 February 2020, *Nasirov and Others v. Azerbaijan*, no. 58717/10, CE:ECHR:2020:0220JUD005871710, § 47 f. See also *Rengeling, Hans-Werner, and Szczekalla, Peter* (2004), Grundrechte in der Europäischen Union – Charta der Grundrechte und Allgemeine Rechtsgrundsätze, p. 449 f.

On the other hand, the CJEU emphasised that, as regards, in particular, effective action to combat criminal offences committed against, inter alia, minors and other vulnerable person, positive obligations of the public authorities may result from Article 7 of the Charter, requiring them to adopt legal measures to protect private and family life.[73] Again, in so far as children are concerned, this obligation already results from Article 24(1) of the Charter.

5.2.2.4. Proportionate to the legitimate aim pursued?

How the other elements of the second sentence of Article 52(1) of the Charter are related to each other is not evident at first sight. It results from the case-law of the CJEU that they must be seen as facets of the principle of proportionality.

It is settled case-law that the principle of proportionality, which is one of the general principles of European Union law, requires that measures implemented by acts of the European Union are appropriate for attaining the objective pursued and do not go beyond what is necessary to achieve it.[74] The requirement that the limitation must 'genuinely meet' a legitimate aim is just another way of saying that the restrictive measure must be appropriate for attaining it.

The current practice of voluntary screening can serve as a starting point when assessing whether the measure under consideration is appropriate for attaining the objective pursued. In a letter to the Members of the European Parliament, the President and CEO of NCMEC John F. Clark presented recent empirical material related to the EU:[75] In 2019, more than 3 million child sexual abuse images and videos which NCMEC received originated from an offender in the EU. In the first nine months of 2020, more than 2.3 million child abuse files involving an offender or a child victim in the EU have been reported to NCMEC. Over 95 % of the child abuse imagery shared by offenders in the EU was reported from an email, chat or messaging service. In his letter, Clark also gave some concrete examples: Authorities have informed NCMEC of more than 200 German children depicted in child sexual abuse material circulating online. Tech companies using PhotoDNA, a technology using cryptographic hashes of previously identified child abuse material,[76] have detected and removed these images more than 400,000 times and reported them to NCMEC. Likewise, authorities have identified 70 Dutch children whose sexual abuse was filmed and shared online. Tech companies using PhotoDNA have detected and removed the sexually abusive images of these children more than 80,000 times.

The authors of a targeted substitute impact assessment of the Commission proposal mentioned above[77] asked EUROPOL whether there would be an additional benefit for a

[73] Judgment *La Quadrature*, paragraph 126. In the same sense, judgment of 18 June 2020, *European Commission v. Hungary*, C-78/18, EU:C:2020:476, paragraph 123. See also judgments of the ECtHR of 26 March 1985, *X and Y v. the Netherlands*, no. 8978/80, CE:ECHR:1985:0326JUD000897880, § 23, and of 2 December 2008, *K.U. v. Finland*, no. 2872/02, CE:ECHR:2008:1202JUD000287202, § 46.
[74] Judgment *Volker und Markus Schecke* and *Eifert*, C-92-09 and C-93/09, paragraph 74 and case-law cited.
[75] Letter of 17 November 2020 by John F. Clark,
[76] EPRS impact assessment (no. 23), p. 15.
[77] *Supra* 1.

database of child sexual abuse material reports administered by a European organisation/public authority. The answer they received included the following information:

> 'Europol has one of the largest volumes of CT referral material securely stored globally, second only to NCMEC. This has led to significant advances in different CSE [78] investigations because this data can be cross-matched against existing data from non-related CSE investigations received from Member States and Third Country partners. As a result, children have been identified and suspects identified and arrested.'[79]

This shows that the current voluntary practices are apt to fight child sexual abuse online. It could not be argued that they are inefficient because they could not prevent the sharp increase in child abuse material on the internet. This would be tantamount to saying that the analysis of fingerprints is not efficient when burglaries are on the rise.

The measure under consideration would use the same approach as the current voluntary practices. It would extend screening for child sexual abuse material to providers that have not yet adopted it on a voluntary basis. One might argue that, in reaction to such a measure, abusers are likely to increasingly use technologies that make detection of child sexual abuse imagery more difficult.[80] However, such a trend exists anyway.[81] It cannot be assumed that possible counter-reactions would reduce the positive effects of the measure under consideration to zero. It is thus appropriate for attaining the aim pursued.

A measure is not necessary where a milder, but equally effective measure would be available.[82] As the Communication sets out, the use of online undercover investigation techniques is an important asset in infiltrating the networks that are concealed behind digital technology. However, even if these techniques were used more extensively, relying only on them would not be as effective as combining them with a systematic search for 'child pornography' by the providers. It has also been argued that preventive measures should be prioritised.[83] However, prevention programmes, important as they are, cannot be considered as a milder, equally effective measure when it comes to law enforcement in cases where prevention has failed. Like the fight against crime in general, the fight against online child

[78] Child sexual exploitation.
[79] Note for the attention of the LIBE Committee Secretariat following the shadows meeting of 25 January 2021 on the proposal for a temporary derogation form the e-Privacy Directive for the purpose of fighting online child sexual abuse, RPRS Draft final targeted impact assessment, Written answers to questions to the author of the study, Prof. Jeanne Pia Mifsud Bonnici, by the LIBE Committee Rapporteur and Shadow Rapporteurs, ('Written answers to questions'), footnote 3.
[80] In this sense, *Hanff, Alexander*, Why I don't support privacy invasive measure to tackle child abuse (11 November 2020), https://www.linkedin.com/pulse/why-i-dont-support-privacy-invasive-measures-tackle-child-hanff . Retrieved 14 February 2021.
[81] See the figures for the evolution of technologies involved in the distribution of child sexual abuse imagery in *Bursztein, Elie, and others* (no 13), Figure 6.
[82] See, to this effect, judgment *Österreichischer Rundfunk and Others*, C-465/00, C-138/01 and C-139/01, paragraph 88.
[83] *Hanff, Alexander* (no. 80).

sexual abuse needs a strategy based on the combination of multiple tools. As the crime in question happens online, online screening is a necessary tool in this box.

However, this does not, in itself, justify considering the measure under consideration, which would require general and indiscriminate screening, as necessary within the meaning of Article 52(1) of the Charter. For assessing its necessity, the objective of fighting child sexual abuse more effectively must be reconciled with the fundamental rights set forth in Articles 7, 8 and 11 of the Charter.[84] The question to be answered is whether the EU legislator would strike a proper balance between the objective pursued and the rights affected if they adopted the measure under consideration.[85]

On the one hand, Article 24(2) of the Charter provides that, in all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration. That provision affirms the fundamental nature of the rights of the child.[86] Given the pandemic dimension of child sexual abuse, making the fight against it more effective is of paramount importance. It is about protecting a particularly vulnerable part of society against wide-spread serious crime. Modern investigation techniques are imperative in this respect.

On the other hand, rights of considerable weight are affected. The ECtHR emphasised that 'the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life'.[87] As for freedom of expression, the CJEU has consistently stated that this fundamental right constitutes one of the essential foundations of a pluralist, democratic society and is one of the values on which, under Article 2 TEU, the Union is founded.[88]

The interference with the rights guaranteed by Articles 7 and 8 of the Charter is grave. The screening concerns the content of private correspondence; it will be done by private individuals and that generally and indiscriminately. Necessarily, particularly sensitive visual material would be included such as nude photos.[89] Even if hashing techniques are used, the starting point remains the original image material. A large part of the population of the EU would be affected. In the minds of the people concerned, the measure under consideration is likely to generate the feeling that their private lives are the subject of constant surveillance.[90] Given the quantity and the breadth of the data to be screened, the deterrent effect on the

[84] See, to this effect, judgment *Volker und Markus Schecke* and *Eifert*, C-92-09 and C-93/09, paragraph 76 and case-law cited.
[85] See, to this effect, judgment *Digital Rights*, paragraph 47.
[86] See judgment of 14 January 2021, *TQ*, C-441/19, EU:C:2021:9, paragraph 45.
[87] *Supra* no 36.
[88] Judgment *La Quadrature*, paragraph 114, and case-law cited.
[89] In its judgment of 24 September 2019, *GC and Others*, C-136/17, EU:C:2019:773, paragraph 67, the CJEU underlined that interference with the data subject's fundamental rights to privacy and protection of personal data is liable to be particular serious where the data are sensitive.
[90] In its judgment *Digital Rights*, paragraph 37, the CJEU used a similar reasoning in relation to retention and subsequent use of data.

exercise of the freedom of expression enshrined in Article 11 of the Charter is also serious.[91] As the interference aims at detecting crimes, there is the risk of false suspicion. Considering that the crime of child sexual abuse is at stake, this may have severe consequences for the person concerned.

According to settled case-law, the protection of the fundamental right to privacy requires that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary.[92]

In its judgment *Schrems*, C-362/14, the CJEU held that legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.[93] Even more, legislation permitting private individuals to screen the content of private electronic correspondence generally and indiscriminately would not be in line with Article 52(1) of the Charter.

Other rulings of the CJEU confirm this conclusion. The Court integrated that case-law into its judgment *La Quadrature*. As this judgment is particularly comprehensive and illustrates the nuanced approach of the CJEU very well, it will be used as a starting point in the following analysis.

Case *La Quadrature* is about retention of data. Several groups of data were at stake: data relating to civil identity, IP addresses, other traffic data and location data.

Before dealing with these groups in detail, the CJEU set out that legislation requiring the retention of personal data must always meet objective criteria that establish a connection between the data retained and the objective pursued.[94]

The CJEU held that the retention of data relating to the civil identity of users of electronic communication systems cannot, in principle, be classified as serious because that data does not provide, apart from the contact details of those users, such as their addresses, any information on the communications sent and consequently, on the users' lives. Therefore, the CJEU did not object to legislative measures that provide, for the purposes of safeguarding national security, combatting crime and safeguarding public security, for the general and indiscriminate retention of data relating to the civil identity of users of electronic communication systems provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse.[95] In this context, there is no need for the criminal

[91] In its judgment *La Quadrature*, paragraph 118, the CJEU used a similar reasoning in relation to the retention of traffic and location data for policing purposes.
[92] Judgment of 7 November 2013, *IPI*, C-473/12, EU:EC:2013:715, paragraph 39 and case-law cited.
[93] Paragraph 94.
[94] Judgment *La Quadrature*, paragraph 133. See also Opinion of 26 July 2017, 1/15 (*EU-Canada PNR Agreement*), EU:C:2017:592, paragraph 191.
[95] *Ibid.*, paragraphes 157 and 168.

offences or the threats to or acts having adverse effects on public security to be serious.[96] Also, a connection between all the users of electronic communications systems and the objectives pursued is not necessary.[97]

As regards IP addresses, the CJEU noted that although they are part of traffic data, they are generated independently of any particular communication and mainly serve to identify, through providers of electronic communications services, the natural person who owns the terminal equipment from which an Internet communication is made. Provided that only the IP addresses of the source of the communication are retained and not the IP addresses of the recipient of the communication, the CJEU considered that category of data as less sensitive than other traffic data.[98] However, since IP addresses may be used, among other things to track an Internet users' complete click stream and, therefore, his or her entire online activity, that data enables a detailed profile of the user to be produced. The CJEU concluded that the retention and analysis of those IP addresses which is required for such tracking constitute a serious interference with the fundamental rights of the Internet user enshrined in Articles 7 and 8 of the Charter.[99]

In order to strike a balance between the rights and interest at issue, the CJEU stressed that, where an offence is committed online, the IP address might be the only means of investigation enabling the person to whom that address was assigned at the time of the commission of the offence to be identified. In this respect, the CJEU highlighted cases involving particularly serious child pornography offences, such as the acquisition, dissemination, transmission or making available online of child pornography.[100] It therefore accepted legislative measures that provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the general and indiscriminate retention of IP addresses assigned to the source of an Internet connection for a period that is limited in time to what is strictly necessary, provided that those measures establish strict conditions and safeguards concerning the use of that data, particularly via tracking, with regard to communications made and activities carried out online by the person concerned.[101]

As for traffic data in general and location data, the CJEU stated that such data may reveal information on a significant number of aspects of the private life of the person concerned, including sensitive information such as sexual orientation, political opinions, religious, philosophical, societal or other beliefs and state of health. Taken as a whole, that data may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. In particular, that data

[96] *Ibid.*, paragraph 159.
[97] *Ibid.*, paragraph 159.
[98] *Ibid.*, paragraph 152.
[99] *Ibid.*, paragraph 153.
[100] *Ibid.*, paragraph 154.
[101] *Ibid*, paragraph 156.

provides the means of establishing a profile of the individuals concerned, information that is not less sensitive, having regard to the right to privacy, than the actual content of communications.[102]

In the following, the CJEU distinguished according to the purpose pursued by the preventive retention of traffic and location data.

It held that the objective of safeguarding national security is capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by other objectives.[103] The CJEU did not oppose legislative measure that allow, for the purposes of safeguarding national security, recourse to an instruction requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data in situations where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable if a number of conditions are fulfilled (in particular, effective review the aim of which being to verify that one of those situations exist and that the conditions and safeguards which must be laid down are observed, as well as limitation in time to what is strictly necessary).[104] The CJEU explained that even if such a measure is applied indiscriminately to all users of electronic communications systems, without there being at first sight any connection between the data to be retained and the objective pursued, the existence of a serious threat to national security is, in itself, capable of establishing that connection.[105] In its judgment *Privacy International*, C-623/17,[106] pronounced on the same day as the judgment *La Quadrature*, the CJEU held that national legislation enabling a State authority to require providers of electronic communications services to carry out the general and indiscriminate transmission of traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security exceeds the limits of what is strictly necessary and cannot be considered as justified.[107] In that case, the link with a serious threat was absent.

The next category dealt with in *La Quadrature* is the preventive retention of traffic and location data for the purposes of combating crime and safeguarding public security. This category is of particular importance for assessing the measure under consideration. The CJEU held that, in accordance with the principle of proportionality, only action to combat serious crime and measures to prevent serious threats to public security are capable of justifying serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, such as the interference entailed by the retention of traffic and location data.[108] Building on

[102] *Ibid*., paragraph 117, and case-law cited.
[103] *Ibid.*, paragraph 136.
[104] *Ibid.*, paragraph 168.
[105] *Ibid.*, paragraph 137.
[106] EU:C:2020:790.
[107] Paragraphes 81 f.
[108] Judgment *La Quadrature*, paragraph 140.

its judgment *Tele2*[109], which in turn builds on the judgment *Digital rights*[110], the CJEU continued:

> "National legislation providing for the general and indiscriminate retention of traffic and location data for the purpose of combating serious crime exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter (…)"[111]

The CJEU emphasized that legislation providing for the general and indiscriminate retention of traffic and location data covers the electronic communications of practically the entire population without any differentiation, limitation or exception being made in the light of the objective pursued. It therefore applies even to persons with respect to whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with that objective of combating serious crime.[112] Even the positive obligations of the Member States which may arise, depending on the circumstances from Articles 3, 4 and 7 of the Charter and relating to the establishment of rules to facilitate effective action to combat criminal offences cannot have the effect of justifying such a serious interference.[113]

By contrast, the objectives of combating serious crime, preventing serious attacks on public security, and, a fortiori, safeguarding national security are capable of justifying the particularly serious interference entailed by the *targeted* retention of traffic and location data.[114] The CJEU also held that, in situation where serious criminal offences or acts adversely affecting national security have already been established or where such offences or acts may reasonably be suspected, Member States can provide for the possibility of instructing, by means of a decision of the competent authority that is subject to effective judicial review, providers of electronic communications services to undertake the expedited retention of traffic and location data at their disposal for a specified period of time.[115] The retention obligation must relate only to traffic and location data that may shed light on the serious offences or the acts adversely affecting national security concerned.[116]

The judgment *La Quadrature* devotes a separate section to automated analysis of traffic and location data by way of a screening of all the traffic and location data retained by providers of electronic communications services, which is carried out by those providers at the request of competent national authorities applying the parameters set by the latter. The CJEU accepted

[109] Judgment *Tele2*, paragraphs 105-107.
[110] Judgment *Digital Rights*, paragraph 59.
[111] Judgment *La Quadrature*, paragraph 141.
[112] *Ibid.*, paragraph 143.
[113] *Ibid.*, paragraph 145.
[114] *Ibid.*, paragraph 146.
[115] *Ibid.*, paragraph 163.
[116] *Ibid.*, paragraph 164.

recourse to such a measure only for situations in which a Member State is facing a serious threat to national security which is shown to be genuine and present or foreseeable.[117]

The measure under consideration concerns the general and indiscriminate screening of all private correspondence for 'child pornography'. The very content of the communication is affected. Therefore, the interference is at least as serious as the retention and automated analysis of traffic and location data. On the basis of the CJEU's case-law, it must be concluded that, although the purpose is fighting the serious crime of 'child pornography', general and indiscriminate screening exceeds the limits of what is strictly necessary. It does not comply with Articles 7, 8, 11 and 52(1) of the Charter.

This conclusion is independent of the technology used. However, it has been argued that the scanning is limited and not indiscriminate when hashing technology is used to detect known images and videos. This argument is based on two assertions: First, hashing algorithms do not scan the content of communications data. Second, it is only when the identifier of an image or video uploaded to the service providers' servers matches with those in the database that any further processing is done.[118] The first assertion rests on fact that there is a technological difference between scanning and creating a hash. Nevertheless, to create a hash of an image or video, this image material and thus the content of communications data must be accessed. As for the second assertion, the fact that further processing only takes place in the event of a hit does not change the preceding general and indiscriminate interference if all communications are included in the screening.[119]

5.3. Violation of Article 16 (Freedom to conduct a business) of the Charter?

Obliging providers of number-independent electronic communications services to generally and indiscriminately screen the content of all private correspondence for 'child pornography' constitutes an interference with their freedom to conduct a business. As such general and indiscriminate screening would violate the fundamental rights guaranteed by Articles 7, 8 and 11 of the Charter, it is obvious that this interference would not be proportionate to the legitimate aim pursued. Consequently, the measure under consideration would also violate Article 16 of the Charter.

6. End-to-end encryption

The second question to be dealt with in this expert opinion concerns end-to-end encrypted communications.

Encryption is the key-dependent conversion of data called 'plain text' into a 'ciphertext' so that the plain text can only be recovered from the ciphertext by using a secret key. The terms 'plain text' and 'ciphertext' are explained by history. Nowadays, in addition to text messages

[117] *Ibid.*, paragraph 177.
[118] Written answers to questions (no 78), p. 2.
[119] See also Bundesverfassungsgericht, order of 18 December 2018, 1 BvR 142/15, DE:BVerfG:2018:rs20181218.1bvr014215, Rn. 51.

other types of information, such as photos and videos, can also be encrypted. The underlying cryptographic principles remain the same. The reverse step to encryption is decryption. This term must be linguistically separated from decipherment, i.e., extracting the secret message from the ciphertext without being in possession of the key. That is the work of cryptanalysts, also called 'code breakers'.

There are two basic kinds of encryption methods: symmetrical encryption and asymmetrical encryption. With both methods, keys must be exchanged between the communication partners. Symmetrical encryption methods use the same key for encryption and decryption. Asymmetric encryption is characterized by the fact that a completely different key is used for encryption than for decryption. Here a distinction is made between the 'public key', which is used for encryption, and the 'private key' for decrypting the ciphertext. A pair of private and public keys is generated. The private key is only used by its owner and is kept secret. The associated public key of the same owner is made available to all potential communication partners. The public key can be compared to a conventional open padlock, which can be locked by anyone, but can only be opened again by the owner of the associated private and secret key. In order to transmit a message securely, the sender locks the message with the recipient's public key. The recipient can then open and read/see the message with the private key.[120]

In order to understand end-to-end encryption, it is helpful to have a look at transport encryption first. Transport encryption (also called point-to-point encryption) means that the message is encrypted 'in transit'. E.g., in the case of e-mails, with transport encryption, a connection that is encrypted is established between the e-mail program and the server. All data that is exchanged between the two communication partners is then encrypted during transmission. However, the plain text is accessible by the service provider. Where server-side disk encryption is used, it prevents unauthorized users from viewing this information. It does not prevent the company itself from viewing the information, as they have the key and can simply decrypt the data.

In contrast to transport encryption, with end-to-end encryption, each individual message itself is encrypted. The messages are encrypted by the sender. The recipient retrieves the encrypted data and decrypts it with the help of the private key. The provider of the communication service does not have the private key and therefore cannot decrypt the communication.[121]

Here are some practical examples for the use of end-to-end encryption. The e-mail program Outlook by Microsoft supports two options for sending encrypted messages: S/MIME and Microsoft 365 message encryption. Users must be active themselves to use this technology.[122]

---

[120] Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security), Verschlüsselt kommunizieren, E-Mail Verschlüsselung, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesselt-kommunizieren/E-Mail-Verschluesselung/e-mail-verschluesselung_node.html . Retrieved 9 February 2020.

[121] *Ibid.*

[122] https://support.microsoft.com/de-de/office/verschl%C3%BCsseln-von-nachrichten-373339cb-bf1a-4509-b296-802a39d801dc . Retrieved 9 February 2020.

The e-mail provider Posteo offers two standards for end-to-end encryption: S/MIME and OpenPGP. To make use of this, it is not necessary to use a local e-mail program like Outlook or Thunderbird. However, here, too, users must become active themselves.[123] The instant messaging service WhatsApp uses automatic end-to-end encryption for WhatsApp client software released after March 31, 2016. It is based on the Signal Protocol. Images and videos are also encrypted. The WhatsApp server has no access to the client's private keys. The key is changed with each message sent. Even if encryption keys from a user's device are ever physically compromised, they cannot be used to go back in time to decrypt transmitted messages.[124] In the ordinary course of providing their service, WhatsApp does not store messages once they are delivered or transaction logs of such delivered messages.[125]

Vulnerable points of end-to end encryption are the two ends, where the messages are encrypted and decrypted, i.e., the computers or other devices of the users. Here, perpetrators can simply read the non-encrypted messages.

End-to-end encryption is an ambivalent tool. On the one hand, it protects confidentiality, authenticity and integrity of data on the Internet. It wards off criminals and other intruders. On the hand, it is a way for criminals to hide their communications. Thus, it presents a major challenge for law enforcement agencies.

States around the world have different views on how to deal with the problem of encryption in general.[126] There are Governments that seek to protect encryption to ensure the privacy of communications. Some States, e.g., Germany[127], even actively promote the use of encryption tools including end-to-end encryption. Other Governments restrict the use of encryption. A variety of methods is used for this purpose, e.g., requiring licences for encryption use, setting weak standards for encryption, in particular by imposing so-called back-door access, requiring users to store their private key with the Government or a 'trusted third party', key disclosure or decryption orders in specific situations, and legal presumptions that the use of encryption technologies is evidence of criminal behaviour.

7. Legal assessment (end-to-end encrypted communications included)

If end-to-end encryption were included within the scope of the obligation of providers of number-independent electronic communications services to generally and indiscriminately

[123] https://posteo.de/site/verschluesselung . Retrieved 9 February 2020.

[124] https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption/?lang=en ; WhatsApp Encryption Overview – Technical white paper, https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption/?lang=de . Retrieved 9 February 2020.

[125] https://faq.whatsapp.com/general/security-and-privacy/information-for-law-enforcement-authorities?lang=en . Retrieved 9 February 2020.

[126] For an overview, see United Nations, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, on the use of encryption and anonymity in digital communications (2015), https://www.undocs.org/A/HRC/29/32 . Retrieved 9 February 2020.

[127] See Bundesamt für Sicherheit in der Informationstechnik https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesselt-kommunizieren/verschluesselt-kommunizieren_node.html . Retrieved 9 February 2020.

screen the content of all private correspondence for 'child pornography' and report hits to the police, a preliminary question is how providers could comply with such an obligation in the event of end-to-end encryption.

One option would be to try to crack the code by means of deciphering software[128] while the message is on the server of the provider. The feasibility of this approach is doubtful because sufficiently powerful software might not be available for private individuals. Another option would be to build in an encryption backdoor when designing the software. Such backdoors serve as a way to access the private keys. A third option would be to install, on the computer or other device of the client, additional software that scans the messages before they are encrypted and sent to the intended recipient. An example of such client-side scanning is anti-virus software. Comparison with a database of known child abuse material could be performed on the user's device, which would require maintaining an up-to-date version of the full reference database on every device, or on a remote central server to which the hashes would be sent.[129]

Although client-side scanning would not break the cryptography, all methods of accessing the content of the communications mentioned above would fundamentally impair the end-to-end encryption model.

As regards compliance with the fundamental rights guaranteed by the Charter, the answer given to question 1 would not change. However, there would be even stronger reasons to answer this way because the interference with these rights would be even more serious.

Securing one's date by encryption can be compared to securing the doors of one's home by an anti-burglar device. When assessing whether and when it is legitimate to break such protection, the damage done to the protective device and the enhanced risk of burglary must be considered in a proportionality analysis. The same goes for impairing end-to-end encryption. As the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye put it: '…, a proportionality analysis must take into account the strong possibility that encroachments on encryption and anonymity will be exploited by the same criminal networks that the limitations aim to deter.'[130] Also, if client-side scanning were used, the feeling of constant surveillance would be particularly strong because surveillance would happen on a tool that is a constant companion in the everyday life of a large number of people.

From the providers' perspective, the methods described would be a particularly serious interference with their freedom to conduct a business because they would have to generally

[128] A company that offers such software is the Israeli Digital Intelligence company Cellebrite https://www.cellebrite.com/de/erweiterte-dienste/ . Retrieved 9 February 2020.
[129] Internet Society, Client-Side Scanning – What it is and why it threatens trustworthy, private communications, https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/ . Retrieved 9 February 2020.
[130] Report (2015), https://www.undocs.org/A/HRC/29/32 . Retrieved 9 February 2020.

and indiscriminately disappoint the expectation associated with their lawful end-to-end encryption product, namely, that they have no access to the content of the messages.

8. Legal assessment for permission instead of obligation

If the providers were not obliged but allowed to generally and indiscriminately screen the content of all private correspondence for 'child pornography' and report hits to the police, their freedom to conduct a business would not be affected.

As for the fundamental rights guaranteed by Articles 7, 8 and 11 of the Charter, the first question to be answered is whether there would be an interference with these rights. This question must be answered in the affirmative. Where the EU legislator allows behaviour that endangers fundamental rights, the interference lies in granting the permission.[131]

Mutatis mutandis the above analysis of proportionality is also valid for this constellation:

Unlike in the case of an obligation, there would be no mandatory extension of the current practice of screening. However, in reaction to the change brought about by the inclusion of number-independent interpersonal communication services in the scope of application of the e-Privacy Directive, not all providers have continued this practice. The consequence was a considerable decrease in the number of reports.[132] A legal permission for the screening is likely to restore the *status quo ante* and could prompt providers that have not yet practiced screening for 'child pornography' to do so on a voluntary basis. It is thus appropriate for attaining the aim of a more effective fight against child sexual abuse.

As set out above, online screening is a necessary tool in the toolbox needed to achieve this aim.[133]

At the stage of balancing the objective pursued and the rights affected, it must be noted that the weight of the interference with the rights guaranteed by Articles 7, 8 and 11 of the Charter is not the same in the case of an obligation as in the case of a permission. If providers of number-independent electronic communication services are obliged to generally and indiscriminately screen the content of all private correspondence for 'child pornography', users of such services are inevitably exposed to such screening. If the providers are only allowed to do so, there is a chance that not all will adopt this practice. As long as there are providers that do not generally and indiscriminately screen for 'child pornography', clients could use the services of those providers. However, if this implies switching from one provider to another, 'friends' who have used the services of the first provider may not be willing to take

[131] See *Regeling, Hans-Werner, and Szczekalla, Peter* (no 72), p. 231. Alternatively, one could base the reasoning on a duty to protect, as the ECJ did in its judgment of 12 June 2003, *Schmidberger*, C-112/00, EU:C:2003:333, paragraphs 58 f., in the context of obstacles to the free movement of goods, which can be considered as a fundamental economic right.
[132] Oral information by Europol on 2 March 2021.
[133] *Supra* 5.2.2.4.

the same step. Also, for those who are exposed to voluntary screening, the interference is the same as in the case of obligatory screening.

Although the interference would be less grave for the population as a whole if providers were not obliged but only allowed to generally and indiscriminately screen the content of all private correspondence for 'child pornography', the result of the proportionality test would be the same. As already mentioned above, in its judgment *La Quadrature* the CJEU also dealt with automated analysis of traffic and location data by way of a screening of all the traffic and location data retained by providers of electronic communications services, which is carried out by those providers at the request of the competent national authorities applying the parameters set by the latter. The CJEU accepted such a measure only for situations in which a Member State is facing a serious threat to national security which is shown to be genuine and present or foreseeable.[134] It would be inconsistent not to apply the same standard if the EU legislator permitted providers to generally and indiscriminately screen all private correspondence for 'child pornography'.

Consequently, except for Article 16 of the Charter, the answer to question 3 is the same as the answer to question 1.

9. Conclusions

Having regard to the relevant case-law, EU legislation obliging providers of number-independent communications services (i.e. e-mail, messaging, chat) to generally and indiscriminately screen the content of all private correspondence for 'child pornography' and report hits to the police would not comply with the fundamental rights guaranteed by Articles 7, 8, 11 and 16 of the Charter. This would apply all the more if end-to-end encrypted communications were included in the obligation. If the providers were allowed instead of obliged to practice such screening, the result would be the same except that there would be no violation of Article 16 of the Charter.

Undoubtedly fighting online child abuse material is of utmost importance. However, the requirement of Article 24(2) of the Charter to ensure that in actions relating to children, the child's best interests must be a primary consideration does not mean that those interests prevail over all other interests. The rights of the child must be given particular weight, but they cannot completely supersede the rights and freedoms of others.

[134] Judgment *La Quadrature*, paragraphes 172 and 177.

Chronological List of Cited Cases

1. CJEU/ECJ

Judgment of 13 April 2000, Karlsson and Others, C-292/97, EU:C:2000:202

Judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, C-138/01 and C-139/01, EU:C:2003:294

Judgment of 12 June 2003, *Schmidberger*, C-112/00, EU:C:2003:333

Judgment of 5 October 2010, *J.McB*, C-400/10 PPU, EU:C: 2010:582

Judgment of 22 December 2010, *DEB*, C-2079/09, EU:C:2010:811

Judgment of 9 November 2010, *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, EU:C:2010:662

Judgment of 26 February 2013, *Åkerberg Fransson*, C-617/10, EU:C:2013:105

Judgment of 7 November 2013, *IPI*, C-473/12, EU:EC:2013:715

Judgment of 9 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, '*Digital Rights*'

Judgments of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650

Judgment of 17 December 2015, *WebMindLicenses*, C-419/14, EU:C:2015:832

Judgment of 21 December 2016, *Tele2 Sverige and Watson and Others*, C-203/15, EU:C:2016:970, *'Tele2'*

Opinion of 26 July 2017, 1/15 (*EU-Canada PNR Agreement*), EU:C:2017:592

Judgment of 24 September 2019, *GC and Others*, C-136/17, EU:C:2019:773

judgment of 5 October 2000, *Germany v. European Parliament and Council*, C-376/98, EU:C:2000:544

Judgment of 18 June 2020, *European Commission v. Hungary*, C-78/18, EU:C:2020:476

Judgment of 16 July 2020, *Adusbef and Federconsumatori*, C-686/18, EU:C:2020:567

Judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, EU:C:2020:559

Judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/28 and C-520/18, EU:C;2020:791, '*La Quadrature*'

Judgment of 6 October 2020, *Privacy International*, C-623/17, EU:C:2020:790

Judgement of 17 December 2020, *Central Israëlitisch Consistorie van België and Others*, C-336/19, EU:C:2020:1031

Judgment of 14 January 2021, *OM*, C-393/19, EU:C:2021:8

Judgment of 14 January 2021, *TQ*, C-441/19, EU:C:2021:9

2. ECtHR

Judgment of 26 March 1985, *X and Y v. the Netherlands*, no. 8978/80, CE:ECHR:1985:0326JUD000897880

Judgment of 24 November 1986, *Gillow v. the United Kingdom*, no. 9063/80, CE:ECHR:1986:1124JUD000906380

Judgment of 26 March 1987, *Leander v. Sweden*, no. 9248/91, CE:ECHR:1987:0326JUD000924881

Judgment of 25 June 1997, *Halford v. the United Kingdom*, no. 20605/92, CE:ECHR:1997:=625JUD002060592

Judgment of 14 October 1999, *Riera Blume and Others v. Spain*, no. 37680/97, CE:ECHR:1999:003768097

Judgment of 4 May 2000, *Rotaru v. Romania*, no. 2341/95, CE:ECHR:2000:0504JUD002834195

Judgment of 17 February 2004, *Maestri v. Italy*, no. 39748/98, CE:ECHR:2004:0217JUD003974898

Judgment of 1 July 2008, *Liberty and Others v. the United Kingdom*, no. 58243/00, CE:ECHR:2008:0701JUD005824306

Judgment of 2 December 2008, *K.U. v. Finland*, no. 2872/02, CE:ECHR:2008:1202JUD000287202

Judgment of 4 December 2008, *S. and Marper v. the United Kingdom*, Nos 30562/04 and 30566/04, CE:ECHR:2008:1204JUD003056204

Judgment of 18 April 2013, *M.K. v. France*, no 19522/09, CE:ECHR:2013:0418JUD001952209

Judgment of 20 February 2020, *Nasirov and Others v. Azerbaijan*, no. 58717/10, CE:ECHR:2020:0220JUD005871710

Judgment of 27 June 2017, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finnland*, no. 931/13, CE:ECHR:2017:0627JUD000093113

3. Bundesverfassungsgericht (German Federal Constitutional Court)

Order of 18 December 2018, 1 BvR 142/15, DE:BVerfG:2018:rs20181218.1bvr014215

About the Author

Ninon Colneric was honorary professor at the University of Bremen, President of the Labour Appeal Court of Schleswig-Holstein, a Judge of the Court of Justice of the European Communities and the European Co-Dean of the China-EU School of Law at the China University of Political Science and Law in Beijing. Now she is retired.