Translation of original document
commissioned by

THE GREENS/EFA in the European Parliament

Draft

“Chat control” - Analysis of the EU Commission’s draft regulation 2022/0155 (COD)

“Chat control” - Analysis of the EU Commission’s draft regulation 2022/0155 (COD)

Reference:	WD 10 – 3000 – 026/22
Completion of the draft:	07/10/2022 (last retrieval of the internet links)
Field:	WD 10: Culture, media, and sports

regard.

Table of contents

1.	**Preliminary remark**	**4**
2.	**Draft Regulation 2022/0155 (COD) of the EU Commission**	**4**
2.1.	Summary of the content of the draft regulation 2022/0155 (COD)	4
2.2.	Brief explanation of the problem of the draft regulation 2022/0155 (COD)	5
3.	**Legal framework**	**5**
3.1.	Article 7 of the CFR (Charter of Fundamental Rights of the European Union) - Respect for private and family life	6
3.1.1.	Scope of protection	6
3.1.2.	Interference	8
3.2.	Article 8 of the CFR - Protection of personal data	9
3.2.1.	Scope of protection	9
3.2.2.	Interference	9
3.3.	Article 11 of the CFR - Freedom of expression and Freedom of information	10
3.3.1.	Scope of protection	10
3.3.2.	Interference	10
3.4.	Article 5 of the Directive 2002/58/EC (Privacy Policy for Electronic Communications)	11
3.4.1.	Protection of the confidentiality of communication	11
3.4.2.	Options for restrictions	11
4.	**Previous case law on Articles 7, 8, 11 CFR and Article 15 of the Directive 2002/58/EC**	**12**
4.1.	Article 7, 8 and 11 of the CFR	12
4.2.	Article 15 paragraph 1 of the Directive 2002/58/EC	14
5.	**Evaluative analysis of the draft regulation 2022/0155 (COD)**	**15**
5.1.	Proportionality of the draft regulation 2022/0155 (COD)	15
5.1.1.	Legitimate objective	16
5.1.2.	Suitability	16
5.1.3.	Necessity	16
5.1.4.	Adequacy	17
6.	**Conclusion**	**19**

1. Preliminary remark

In accordance with the given task, this paper examines whether and to what extent the draft Regulation of the European Parliament and of the Council laying down provisions on preventing and combating sexual abuse of children (2022/0155 (COD))[1] conflicts with applicable law, in particular whether the interference with fundamental rights is proportionate.

2. Draft Regulation 2022/0155 (COD) of the EU Commission

2.1. Summary of the content of draft regulation 2022/0155 (COD)

The EU Commission's draft regulation 2022/0155 (COD) of 11 May 2022 deals with combating and preventing child sexual abuse on the internet.

Etteldorf summarises this in her article "EU Commission: Proposed Regulation to Better Protect Children from Sexual Abuse" as follows: "The proposal for a regulation on preventing and combating sexual abuse and sexual exploitation of children aims to protect minors more effectively from sexual abuse online and offline, in particular by making providers of online services more accountable. This is to be done, among other things, through risk assessment and risk mitigation obligations as well as reporting obligations. A new EU Centre for Preventing and Combating Child Sexual Abuse, based in The Hague, is to act as a decentralised EU agency to analyse and support this. The proposed regulation follows preventive and repressive approaches, according to which children should be protected from continued abuse, the re-emergence of child sexual abuse material online should be prevented and perpetrators should be prosecuted more effectively. The first step is for the providers of hosting or messenger services to carry out a risk assessment of the extent to which their services could be misused for the distribution of child sexual abuse material or for the initiation of contact (so-called grooming) by perpetrators towards children. In addition, risk mitigation obligations - including adjustments through appropriate technical and operational measures as well as staffing in content moderation and within the framework of recommendation systems - are also provided for. Clearly defined reporting obligations of providers who have detected online child sexual abuse content to the EU Centre for Preventing and Combating Child Sexual Abuse are to be introduced. The EU centre is supposed to check the reports before forwarding them to the member state law enforcement authorities and Europol. If the child sexual abuse material is not removed promptly, the national authorities may issue a removal order."[2]

Accordingly, the previously voluntary investigations to detect child abuse content will now become compulsory.

---

1 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse of 11 May 2022 – COM/2022/209 final. Available on: https://eur- lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472.

2 Etteldorf, Christina: Proposed Regulation. In: MMR-Aktuell 2022 (Multimedia and Law Newsletter), 449230.

2.2. Brief explanation of the problem of the draft regulation 2022/0155 (COD)

The draft regulation 2022/0155 (COD) raises concerns in several respects. It provides for permanent and blanket analysis and monitoring of private communications.

Etteldorf sees in this the danger that such a "general 'chat control' could lead to serious invasions of privacy even of those persons who do not participate in the distribution of abusive material or in initiating contact with children, especially if technical protection mechanisms (or protection options) are lacking or if they fail. The proposed regulation also does not address how these obligations can be (technically) implemented for currently end-to-end encrypted communication services such as WhatsApp." [3] When it comes to end-to-end encrypted services, i.e. services that are invisible to providers and third parties, Zurawski is also of the opinion that "the obligation to monitor entails yet another irreversibly severe interference: the de facto abolition of these secure communication channels. Service providers can only monitor this in two ways. On the one hand, through the encryption, which would mean abolishing or at least weakening the encryption, which would then also allow third parties to know the communication content. Or bypassing encryption, through so-called client-side scanning, which the EU Commission implicitly proposes in its comments on the proposal, but which would entail codified, provider-side backdoors into the devices used, which third parties could in turn exploit". [4]

This planned approach could therefore significantly interfere with the right to privacy, data protection and, among other things, the fundamental rights of the EU Charter of Fundamental Rights (Articles 7, 8, 11 of the CFR). Moreover, the whole process is non-transparent for users of communication services. Ultimately, it remains questionable whether the regulations satisfy the principle of proportionality.

3. Legal framework

Before examining whether and to what extent the draft regulation 2022/0 155 (COD) violates Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union (CFR) [5] as well as Article 15 of 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 - ePrivacy Directive), the respective areas of protection are outlined below. [6]

---

3 Etteldorf, Christina: Proposed Regulation. In: MMR-Aktuell 2022, 449230.

4 Zurawski: EU Commission: Proposal "Chat control" - conditions of surveillance. In: ZD-Aktuell 2022 (Journal for Data Protection), 01240.

5 Charter of Fundamental Rights of the European Union. Official Journal C 202/389 of 7 June 2016. Available on: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:12016P/TXT&from=LT.

3.1. Article 7 of the CFR - Respect for private and family life

3.1.1. Scope of protection

In its judgment of 6 November 2019, the Federal Constitutional Court (BVerfG) defines the scope of protection of Articles 7 and 8 of the CFR as follows: “Article 7 of the CFR establishes the right to respect for private and family life, home and communications, Article 8 of the CFR establishes the right to protection of personal data. These guarantees have a counterpart in Article 8 of the European Convention on Human Rights (ECHR)[7], which in turn protects the right to respect for private and family life, home and correspondence - and in particular also from the processing of personal data. The guarantees of Articles 7 and 8 of the CFR are closely related to each other. At least as far as the processing of personal data is concerned, these two fundamental rights constitute a uniform guarantee of protection. Articles 7 and 8 of the CFR protect against the processing of personal data and require ‘respect for private life’. In this context, personal data - as understood by German constitutional law on Article 2(1) in conjunction with Article 1(1) of the Basic Law (Grundgesetz, GG) - means all information relating to an identified or identifiable natural person. Accordingly, the right to respect for private life is not to be understood narrowly and is in particular not limited to highly personal or particularly sensitive matters. In particular, business and professional activities are not excluded from this. Article 7 and Article 8 of the CFR thus protect the self-determined development of personality against data processing by third parties”. [8]

Private life includes the right to personal self-determination and lifestyle, personal self-expression and self-preservation, i.e. the autonomous decision on the personal way of life and its public disclosure. All natural persons, especially children, are bearers of the right to respect for private life. Nationality does not play a role here.

---

6 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 (Privacy Policy for Electronic Communications). Official Journal L 201, 31 July 2002 p. 37-47. Available on: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32002L0058.

7 European Convention for the Protection of Human Rights and Fundamental Freedoms. Available on: https://www.bmj.de/SharedDocs/Downloads/DE/Themen/EuropaUndInternationaleZusammenarbeit/Euro- paeischeKonventionMenschenrech-te.pdf;jsessio-nid=8D72A8B24CA4DBCAAC648CDF7E37414E.1_cid334?__blob=publicationFile&v=1.

8 Federal Constitutional Court (BVerfG), Judgment of 6 November 2019 - 1 BvR 276/17 - Right to be forgotten II -, para. 99 f.

Furthermore, legal persons and associations of persons are, in principle, holders of fundamental rights. This is supported by the fact that business privacy is also protected.[9]

Family life is characterised in particular by the protection of private living spaces as well as by their individual form - comparable to the scope of private life. The broad concept of family life encompasses all close personal relationships of a private nature that are designed to last and are based on living together, as occurs in a traditional family. What is necessary is an *actual* family life, for which there is criteria such as living together, the type and length of the relationship as well as the interest and commitment of the partners to each other. Only natural persons are entitled to the right to respect for family life. All family members, i.e. parents and children, grandparents and siblings, are entitled to this right. [10]

Respect for the **home** includes the protection of all rooms which are not generally accessible as a result of spatial partitioning and are made a place of private life (in the broad sense). Business premises are also subject to Article 7 of the CFR. The European Court of Justice (ECJ) is guided by the case law of the European Court of Human Rights (ECHR), which extends the relevant fundamental right to establishments and business premises of both natural and legal persons. The holders of the right to respect for the home are all *natural persons* who are the direct owners of the home, in particular tenants, as well as legal persons and associations of persons. [11]

The guarantee of **communication** exclusively protects communication between absent parties, in particular when it is handed over to a third party or a technical device controlled by a third party for transmission to the recipient (*mediated communication*). There are specific risks for communication as a result of transmission. This is particularly about the confidentiality of communication. Furthermore, as the term “Correspondence” in the relevant provision of Article 8 of the ECHR suggests, only communications addressed to specific addressees are protected and not those that are addressed to the public. It is irrelevant whether the transmission is made by state institutions or private individuals. In addition, the technology of transmission is irrelevant. For example, transmission by letter or postcards, by phone or via the internet (email) is covered. The bearers of the right to communicate are all *natural* persons as well as legal persons and associations of persons. [12]

---

9 Jarass CFR, 4th ed. 2021, EU Charter of Fundamental Rights, Art. 7 para. 3, 14 ff.

10 loc. cit., Art. 7 para. 18 ff.

11 loc. cit., Art. 7 para. 22 f.

12 loc. cit., Art. 7 para. 25 f.

3.1.2. Interference

A measure that affects one of the aforementioned areas of protection interferes with the scope of protection of Art. 7 CFR. There is no interference if the holder of the fundamental right has consented to the interference. [13]

Private life protected by Article 7 of the CFR is affected as soon as the private sphere, i.e. the personal lifestyle, is invaded. This happens, for example, by searching a person or accessing information about their private life. The right to respect for **family life** is affected by, among other things, the deprivation of custody or parenting rights or the physical separation of family members. There is interference with regard to the **home** if the privacy of the protected spaces is impaired, for example by entering or searching the home without the consent of the authorised person or by surveillance. There is interference with the respect for **communications** in the case of any action that leads to knowledge of the contents or data of communications. [14] Examples are monitoring letters, telecommunications, and internet use.

Limitations of the scope of protection are possible in accordance with Article 52 (1) of the CFR.
It states:

> *"Any limitation on the exercise of the rights and freedoms recognised in this Charter shall be provided for by law and shall respect the essence of those rights and freedoms. While respecting the principle of proportionality, restrictions may be imposed only if they are necessary and genuinely meet the objectives of common welfare recognised by the Union or for the need to protect the rights and freedoms of others".* [17]

According to Art. 52 para. 3 sentence 1 CFR, the provisions of Art. 8 ECHR must also be taken into account.

> *"Insofar as this Charter contains rights which correspond to the rights guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms, the rights in this Charter shall have the same meaning and scope as conferred upon the rights by the said Convention. This provision shall not prevent Union law from granting more extensive protection."*

---

13 Jarass CFR, 4th ed. 2021, EU Charter of Fundamental Rights, Art. 7 para. 27.

14 Jarass CFR, 4th ed. 2021, EU Charter of Fundamental Rights, Art. 7 para. 28 ff.

15 ECJ, Judgment of 17 December 2015 - C-419/14 - WebMindLicenses -, para. 71 f.

16 ECtHR, Judgment of 3 April 2007 - 62617/00 - Surveillance of private email and internet use.

17 Jarass CFR, 4th ed. 2021, EU Charter of Fundamental Rights, Art. 52.

> *This provision does not preclude Union law from granting more extensive protection."* [18]

In addition, every restriction requires a legal basis, whereby the essence of the fundamental right as well as the proportionality of the interference must be considered. [19]

3.2. Article 8 of the CFR - Protection of personal data

3.2.1. Scope of protection

Article 8 of the CFR protects the processing of personal data. Personal data is any information about a natural person. The scope of protection of Article 8 of the CFR is not to be interpreted narrowly. In addition to information relating to the private sphere in the narrow sense, it includes all personal data, for example, occupation or assets (also see point 3.1.1).[20] All natural persons are holders of fundamental rights. Whether legal persons are also holders of fundamental rights is disputed. The EU Court of Justice recognises legal persons as holders of fundamental rights if *"the name of the legal person contains one or more natural persons".* [21]

3.2.2. Interference

There is an interference with Article 8 of the CFR when personal data is processed. Processing is understood to mean any action in relation to personal data, in particular collection, storage, use, alteration, blocking or erasure. It is irrelevant whether the processing leads to an interference. An interference does not exist if the holder of the fundamental right has previously consented to the processing of his or her data. [22]

Limitations are possible in accordance with Article 52 (1) of the CFR. In this context, Article 8 para. 2 of the CFR must be taken into account. It states:

> *"These data may only be processed in good faith for specified purposes and with the consent of the data subject or on another legitimate basis laid down by law. Every person has the right to be informed about the data collected concerning him or her and to have the data rectified.* [23]

---

18 loc. cit., Art. 52.

19 Kingreen, in: Calliess/Ruffert (eds.), EUV/AEUV, 6th ed. 2022, Art. 7 para. 14.

20 ECJ, Judgment of 9 November 2010 - C-92, 93/09 - Volker und Markus Schecke GbR -, para. 59.

21 ECJ, Judgment of 9 November 2010 - C-92, 93/09 - Volker und Markus Schecke GbR -, para. 53.

22 Jarass CFR, 4th ed. 2021, EU Charter of Fundamental Rights, Art. 8 para. 9 ff.

23 loc. cit. Art. 8.

Any restriction requires a legal basis and must respect the essence of the fundamental right and the principle of proportionality. [24]

3.3. Article 11 of the CFR - Freedom of expression and information

3.3.1. Scope of protection

Article 11 of the CFR protects freedom of expression and information and the freedom and plurality of the media. Opinions are to be understood in particular as value judgements. [25] Forming, having or not having, expressing and disseminating an opinion as well as the right to not express one's opinion are protected. [26] Freedom of information protects the entire information process, i.e. the receipt of information and ideas, their dissemination, and use of systems.
Freedom of the media includes the classical media (freedom of press, freedom with regard to radio and film) as well as the "new media". [27] Diversity of opinion is ensured through the concept of plurality. The subjects of fundamental rights are natural persons, employees and officials of the Union and legal persons. [28]

3.3.2. Interference

Freedom of expression and information is interfered with by all impediments to communication. Not only direct acts, but also indirect effects or de facto acts can constitute interference if they make the protection of the protected domain impossible or at least more difficult in a qualified manner. [29]

For the justification of interference, the special provision of Art. 10 para. 2 ECHR applies to freedom of expression and information under Art. 52 para. 3 CFR. The restriction of Art. 52 (1) CFR does not apply as long as the ECHR grants more extensive protection. [30] A legal basis is required for restrictions on the rights of Art. 11 CFR. In addition, the principle of proportionality must be upheld here as well.

---

24 Jarass CFR, 4th ed. 2021, EU Charter of Fundamental Rights, Art. 8 paras. 13-15

25 Jarass GrCh, 4th ed. 2021, EU Charter of Fundamental Rights, Art. 11 para. 10.

26 Thiele, in: Pechstein/Nowak/Häde (eds.), Frankfurter Kommentar, EUV/GRC/AEUV, 1st ed. 2017, Art. 11 para. 9-12.

27 Jarass CFR, 4th ed. 2021, EU Charter of Fundamental Rights, Art. 11 para. 15 f.

28 Jarass CFR, 4th ed. 2021, EU Charter of Fundamental Rights, Art. 11 para. 16.

29 Jarass CFR, 4th ed. 2021, EU Charter of Fundamental Rights, Art. 11 para. 20.

30 Calliess, in: Calliess/Ruffert/Kingreen (eds.), EUV/AEUV, 6th ed. 2022, Part II, Art. 11 para. 29.

3.4. Article 5 of Directive 2002/58/EC (Directive on Privacy and Electronic Communications)[31]

3.4.1. Protection of the confidentiality of communication

Article 5 paragraph 1 of Directive 2002/58/EC (confidentiality of communications) states:

> *"Member States shall ensure the confidentiality of **messages and associated 'traffic data' transmitted using public communications networks and publicly available communications services** using national legislation. In particular, the Member States shall prohibit listening, tapping, storage and other forms of interception or surveillance of messages and associated 'traffic data' by persons other than users, without the consent of the users concerned, unless such persons are authorised by law in accordance with Article 15(1). This provision shall not preclude - without prejudice to the principle of confidentiality - the technical storage necessary for forwarding a message."* [32]

3.4.2. Options to restrict rights

Article 15(1) of Directive 2002/58/EC (application of certain provisions of Directive 95/46/EC) provides for the following options for restricting the rights under Article 5(1) of Directive 2002/58/EC:

> *"Member States may adopt legislative measures restricting the rights and obligations referred to in Articles 5, 6, 8(1), (2), (3) and (4) and 9 of this Directive, provided that such restriction is necessary, appropriate and proportionate for **national security** (i.e. State security), **defence, public security** and the **prevention, investigation, detection and prosecution of criminal offences** or of **unauthorised use of electronic communications systems** in a democratic society, in accordance with Article 13(1) of Directive 95/46/EC". To this end, Member States may provide by law that **data** be retained **for a limited period of time** for the reasons set out in this paragraph. Any measures referred to in this paragraph shall comply with the general principles of Community law, including those set out in Article 6(1) and (2) of the Treaty on European Union."* [33]

---

31 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 (Privacy Policy for Electronic Communications), Available on: EUR-Lex - 32002L0058 - DE (europa.eu).

32 loc. cit., Art. 5 para. 1.

33 loc. cit., Art. 15.

4. Previous case law on Articles 7, 8, and 11 of the CFR and Article 15 of Directive 2002/58/EC

So far, there is no case law on Articles 7, 8, and 11 of the CFR and Article 15 para. 1 of the ePrivacy Directive with regard to preventing and combating sexual abuse of children. Consequently, this paper presents the previous case law in comparable factual situations, in particular data retention, taking into account the factor of proportionality.

4.1. Articles 7, 8, and 11 of the CFR

The ECJ considers that Directive 2006/24/EC of the European Parliament and of the Council 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 (the Data Retention Directive)[34] is disproportionate in the strict sense of the term, as it provides for the retention of data without prior notice and on a permanent basis. [35]

Interference with fundamental rights occurs, among other things, when communications services make traffic data accessible [36] to national authorities and when communications services "retain data on a person's private life and communications for a specified period of time". [37] The VDS-RL directive provides for such interference. Moreover, in doing so, it affects all people who are in the EU and use means of communication "without, however, the persons whose data are retained being even indirectly in a situation that could give rise to criminal prosecution". [38] Moreover, data retention is carried out without informing users, thereby "creating the feeling among data subjects that their private lives are subject to constant surveillance". [39] The **aim** of the VDS-RL measures is to increase security. At the same time, data retention is, at least in the abstract, **suitable** for achieving increased security. [40] In terms of **necessity** and **adequacy**, however, data retention represents an interference of a great degree and conveys a disturbing sense of omnipresent surveillance of the individual.

---

34 Directive 2006/24/EC of the European Parliament and of the Council 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. Official Journal L 105/54 of 13 April 2006. Available on: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:DE:PDF.

35 Ziebarth, Wolfgang: Data retention in transition. In: ZUM 2017, 398 ff. [401].

36 ECJ, Judgment of 21 December 2016 - C-203/15, C-698/15 - Tele2 Sverige -, para. 92.

37 ECJ, Judgment of 08 April 2014 - C-293/12, C-594/12 - Invalidity of EU Directive -, para. 34.

38 ECJ, Judgment of 08 April 2014 - C-293/12, C-594/12 - Invalidity of EU Directive -, para. 48.

39 ECJ, Judgment of 21 December 2016 - C-203/15, C-698/15 - Tele2 Sverige -, para. 100.

40 ECJ, Judgment of 08 April 2014 - C-293/12, C-594/12 - Invalidity of EU Directive -, para. 41, 49.

41

For this reason, the principle of proportionality is only respected if the interference is limited to what is absolutely necessary. It is up to the competent national authorities to *“ensure in each individual case that both the category or categories of data collected and the duration for which access to them is requested are limited, in the light of the specific circumstances, to what is strictly necessary for the investigations in question”.* [42] However, the VDS-RL directive does not contain any provisions “which are capable of ensuring that the interference is actually limited to what is absolutely necessary”. [43] General and indiscriminate data retention thus exceeds the limits of what is absolutely necessary. [44]

In its rulings, the ECJ confirmed the prohibition of the storage of mass data without any reason. [45] In addition, there is a need for effective protection against risks of abuse. [46] There is a need for clear and precise provisions regulating the scope and use of the act *“and to establish minimum requirements so that persons whose data have been retained have sufficient safeguards to ensure effective protection of their personal data against risks of misuse and against any unauthorised access to, or use of, such data”.* [47] *The national regulation “must in particular specify under which circumstances and under which conditions a data retention measure may be taken as a preventive measure, so as to ensure that such a measure is limited to what is absolutely necessary”* [48]. Misuse or abuse means accidental or unauthorised destruction, accidental loss, as well as unauthorised access, unauthorised modification or unauthorised disclosure. [49] Unauthorised access occurs when a public authority interferes with Article 8 of ECHR even though the interference is not provided for by law and is not necessary in a democratic society for national security or public safety, for the economic well-being of the country, for the maintenance of order, for the prevention of crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. [50]

---

41 ECJ, Judgment of 08 April 2014 - C-293/12, C-594/12 - Invalidity of EU Directive -, para. 37.

42 ECJ, Judgment of 02 March 2021 - C-746/18 - Preliminary ruling -, para. 38.

43 ECJ, Judgment of 08 April 2014 - C-293/12, C-594/12 - Invalidity of EU Directive -, para. 65.

44 Priebe, Reinhard: Strict requirements of the ECJ for national regulations. In: EuZW 2017, 136 ff. [138].

45 Etteldorf, Christina: ECJ: Clarification of the case law. In: MMR-Aktuell 2022, 448557.

46 Zeitzmann, Sebastian: ECJ: Data retention without cause. In: MMR-Aktuell 2021, 437661.

47 ECJ, Judgment of 08 April 2014 - C-293/12, C-594/12 - Invalidity of EU Directive -, para. 54.

48 ECJ, Judgment of 21 December 2016 - C-203/15, C-698/15 - Tele2 Sverige -, para 109.

49 ECJ, Judgment of 4 December 2008 - 30562/04 and 30566/04 - Marper v. United Kingdom -, para. 103.

50 ECJ, Judgment of 08 April 2014 - C-293/12, C-594/12 - Invalidity of EU Directive -, para. 54.

In its ruling of 2 March 2010 on data retention, the Federal Constitutional Court states:

> *“A global and blanket surveillance in the form of an area-wide recording of telecommunications connections, as represented by the retention of data, is unconstitutional even to avert the greatest dangers. The probability that the stored data would later be needed for security or law enforcement purposes would be infinitesimally small and could not justify such serious interference. Data retention makes it possible to create personality profiles with unprecedented accuracy. The communication data is extremely informative in terms of content. Access to the detailed circumstances of the telecommunication is no less serious than the access to the content of the communication. It allows for comprehensive personality and behavioural profiles. ‘Traffic data’ provides a great deal of information about social relationships. Data retention also increases the risk of being unjustly subjected to investigative measures or innocently convicted, and the danger of data misuse. ‘Traffic data’ could be used specifically against unpopular persons and could be used to control individuals and groups as well as for industrial espionage. Only refraining from data retention would effectively protect against misuse. Data retention impairs the impartiality of communication, which is indispensable for democracy. The protection of human dignity requires a certain degree of unobserved communication, especially in the context of special relationships of trust. The damage caused by the surveillance of the citizen is not outweighed by the associated gain in efficiency. [...] Data retention is disproportionate because the expected benefits are clearly disproportionate to the disadvantages to the data subjects and to society as a whole. The protection of legal interests would only be improved in a few cases. A reduction in the level of crime is not to be expected.”* [51]

In conclusion, it remains to be said that although data retention has not been ruled out per se, the ECJ has placed stringent requirements on a new regulation, which has not been implemented at EU level to date. Accordingly, proportionality is only ensured if data retention is carried out either to combat serious crime or to prevent serious threats to public security, as otherwise the far-reaching interference with fundamental rights is not justified. [52]

4.2. Article 15 para. 1 of the Directive 2002/58/EC

Article 15(1) of Directive 2002/58/EC allows Member States to create exceptions to the basic obligation to ensure the confidentiality of personal data set out in Article 5(1) of the Directive. The prerequisite for this is that such a restriction is necessary, appropriate and proportionate for national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences or the unauthorised use of electronic communications systems in a democratic society. For the purposes referred to above, Member States may provide for data to be retained for a limited period by law for one of those reasons.

---

51 Federal Constitutional Court, Judgment of 2 March 2010 - 1 BvR 256/08 -, BVerfGE 125, 260-385, juris para. 102 et seq.

52 ECJ, Judgment of 06 October 2020 - C-511/18, C-512-/18, C-520/18 - La Quadrature -, para. 140.

However, the power to derogate from the rights and obligations provided for in Articles 5, 6 and 9 of Directive 2002/58/EC cannot justify making the exception to this fundamental obligation to ensure the confidentiality of electronic communications and the associated data and, in particular, to the prohibition on storing such data expressly provided for in Article 5 of the Directive, the rule. [53]

The ECJ has held in several decisions [54] that Article 15(1) of Directive 2002/58/EC would conflict with a provision providing for general and indiscriminate retention of all communication and location data. [55] Only in the case of a serious, real and current, or at least foreseeable, threat to national security should it be possible to make exceptions. [56] Article 15 (1) of Directive 2002/58/EC, taking into account Articles 7, 8 and 11 of the CFR, thus precludes a regulation which provides for *"general and indiscriminate retention of communication and location data as a preventive measure to combat serious crime and to prevent serious threats to public security"*. [57] A restriction of the obligations laid down in the Directive can only be limited taking into account the principle of proportionality as well as the fundamental rights of the EU Charter of Fundamental Rights. [58] In this respect, reference is made to the case law on Art. 7, 8 and 11 CFR (see 4.1).

5. Evaluative analysis of the draft regulation 2022/0155 (COD)

Taking into account the previous case law on data retention, the draft regulation 2022/0155 (COD) is examined and analysed.

5.1. Proportionality of the envisaged interference of the draft regulation 2022/0155 (COD)

Taking into account the ECJ's rulings on data retention, constitutional concerns are raised with regard to the draft regulation of the European Parliament and of the Council establishing provisions to prevent and combat the sexual abuse of children. The draft law pursues the legitimate aim of protecting children. This is indisputably to be done by interfering with the privacy of communication. The regulations affect "*confidentiality and secrecy of communications*". [59]

---

53 ECJ, Judgment of 06 October 2020 - C-511/18, C-512/18, C-520/18 - Data retention without cause only in case of significant risk -, para. 110.

54 ECJ, Judgment of 21 December 2016 - C-203/15 and C-698/15 - Tele2 Sverige -, para. 96.

55 Etteldorf, Christina: ECJ: Clarification of case law. In: MMR-Aktuell 2022, 448557.

56 Etteldorf, Christina: ECJ: Clarification of case law. In: MMR-Aktuell 2022, 448557.

57 ECJ, Judgment of 05 April 2022 - C-140/20 - G. D./Commissioner of An Garda Síochána -, 536.

58 Zeitzmann, Sebastian: ECJ: Data retention without cause. In: MMR-Aktuell 2021, 437661.

59 Zurawski, Paul: EU Commission: Proposal "Chat control". In: ZD-Aktuell 2022, 01240.

Interferences with the privacy of communications include the “automated scanning of all content” [60] or errors resulting from automated chat controls, whereupon the private message reaches the European coordination authority. [61]

5.1.1. Legitimate objective

The aim of the draft regulation is to preventively combat sexual abuse of children on the internet. In order to achieve this goal, the Commission would like to make messenger services such as WhatsApp, Signal or Threema more accountable and demands that they scan all private messages of their users and report any anomalies. The previously voluntary scanning activities of the large internet companies (including Facebook/Meta, Microsoft, Google/Alphabet) of unencrypted messenger and email messages as well as hosted files and posted content for child abuse depictions is to be made obligatory and expanded to include previously inactive providers and non-scanned services. The draft regulation 2022/0155 (COD) also aims to combat “so-called ‘grooming’, i.e. initiation of contact by an adult with a child, with the aim of sexual abuse, and the dissemination of child pornography files”. [62]

5.1.2. Suitability

Concerns could already arise with regard to the suitability of the measures of the draft regulation, i.e. whether the intended objective is achieved with the draft regulation. Woerlein, for example, comes to the following assessment in ZD-Aktuell 2022: *“When considering the potential consequences of a chat control, the first question to be addressed is whether the Commission’s intended plan is connected to any actual added value for the objective pursued. This is questionable in the case at hand. It is already doubtful whether the relevant messenger services have played a major role in the distribution of child pornography files.* Even if this turns out to be true, the presumption is that the services will no longer be used to distribute the files at the latest when it becomes known that the providers carry out chat control reliably.” [63]

5.1.3. Necessity

The question of necessity can also give rise to concerns about the extent to which a permanent and indiscriminate surveillance can be considered the least intrusive means to achieve the desired goal. However, this point will not be explored further as the main concerns raised relate to adequacy.

---

60 Zurawski, Paul: EU Commission: Proposal “Chat control”. In: ZD-Aktuell 2022, 01240.

61 Flamme, Florian: EU Commission: Draft law on chat control. In: MMR-Aktuell 2022, 448870.

62 Woerlein, Andreas: Proposed legislation in the fight against child abuse. In: ZD-Aktuell 2022, 01251.

63 Woerlein, Andreas: Proposed legislation in the fight against child abuse. In: ZD-Aktuell 2022, 01251.

5.1.4. Adequacy

In the context of the adequacy of the measures of the draft regulation - proportionality in the narrower sense - various concerns are raised:

Thus, the current definition on “grooming” not only brings advantages for the minors, but it also has some disadvantages. The plan could have an impact on the communication behaviour of the minors, which would lead to an impairment of communication or to a restrained approach to communication and thus also have an impact on the development of the minors. One view highlights that *“the mass invasion of communication privacy endangers the healthy development and communication behaviour of children whose privacy and protective spaces are invaded, for example, by making consensual ‘sexting’ between minors the trigger for prosecution”.* [64] In this context, the Child Welfare Association also considers the plan to be *“disproportionate and not expedient”.* [65] According to the Federal Commissioner for Data Protection and Freedom of Information, the draft regulation *“offers hardly any protection for children, but would be Europe’s entry into unjustified and blanket surveillance of private communications”.* [66] In this context, permanent surveillance does not even stop at children, which can lead to the aforementioned consequences.

The draft regulation 2022/0155 (COD) is now also intended to cover previously end-to-end encrypted services, i.e. services that were previously invisible to providers and third parties. The obligation to monitor such services leads to a further, serious interference and thus, in effect, to the end of confidential communication. Zurawski explains in ZD-Aktuell 2022:
“The service providers can only monitor this in two ways. On the one hand, through the encryption, which would mean abolishing or at least weakening the encryption, which would then also allow third parties to take note of the communication content. Or bypassing encryption, through so-called client-side scanning, which the EU Commission implicitly proposes in its comments on the proposal, but which would entail codified, provider-side backdoors into the devices used, which third parties could in turn exploit. The hopeful formulations of the proposal and the remarks about having to design all technical measures according to the state of the art and security here fail to recognise the simple reality that any access into a system can always be gained by third parties.”

---

64 Zurawski, Paul: EU Commission: Proposal “Chat control”. In: ZD-Aktuell 2022, 01240 [01240].

65 Child welfare association EU-Info: Child welfare association against the scanning of encrypted messages without any reason. Report dated 08/05/2022. Available on: https://www.eu-info.de/dpa-europaticker/316232.html.

66 The Federal Commissioner for Data Protection and Freedom of Information: The Federal Commissioner for Data Protection and Freedom of Information demands compliance with fundamental rights in chat control. Available on: https://www.bfdi.bund.de/SharedDocs/Pressemitteilun- gen/DE/2022/09_Chatkontrolle.html.

[67]

The **actual implementation** by the companies, however, remains **open** in the draft, and so it is unclear how the exact arrangement and the process will turn out. [68] In particular, it is unclear how the implementation of the end-to-end encryption obligation will look like. [69] Moreover, Zurawski expects indirect effects on numerous other fundamental rights. *"So-called 'chilling effects', the withholding of (legal) statements or actions for fear of them being known by the state or third parties, have an intense impact on freedom of expression and freedom of the press (here especially citation and referencing in research work), as well as freedom of association, religion and the general freedom of action."* [70]

In its draft, the EU Commission promises the broadest possible respect for fundamental rights and privacy and obliges service providers to use minimally invasive technical measures. However, the Commission itself assumes errors, as revealed in a published report. [71] When it comes to susceptibility to errors, Woerlein explains that "with the technology used, a general susceptibility to errors still remains. *Even if the error rates are in the low percentage range, they must always be considered in relation to the total number of messages sent. About 100 billion messages are sent worldwide per day via WhatsApp alone (statistics for October 2020 according to Rabe, statista.com [72]). Even an error rate of 0.1% would thus lead to an extremely high number of cases being reviewed."* [73] Moreover, it is questionable how the technologies are supposed to distinguish lawful communication, e.g. harmless holiday photos and consensual sexting, from criminal offences. [74]

In addition to this, Zurawski describes the future process as follows: *"If content is scrutinised, all content must first be included, because even an automated process cannot determine whether a piece of information is relevant or, for example, is to be assigned to absolute privacy before first taking note of the content. Thus, at least the temporary storage of a piece of content in the working memory is required so that it can be classified automatically. If the technology used, e.g. an algorithm, has made a pre-selection of content, a human review is still necessary to separate the correctly recognised content from the irrelevant content.*

---

67 Zurawski, Paul: EU Commission: Proposal "Chat control". In: ZD-Aktuell 2022, 01240.

68 Montag, Miriam: EU Commission plans new law against child abuse. In: becklink 2023186.

69 Etteldorf, Christina: Proposed Regulation. In: MMR-Aktuell 2022, 449230.

70 loc. cit.

71 Network policy: EU Commission concedes high error rates in chat control. Available on: https://netzpolitik.org/2022/geleakter-bericht-eu-kommission-nimmt-hohe-fehlerquoten-bei-chatkontrolle-in-kauf/.

72 Statistics: Number of WhatsApp messages sent per day worldwide. Available on: https://de.statista.com/statistik/daten/studie/868733/umfrage/anzahl-der-taeglich-verschickten-whatsapp-nachrichten-welt- weit/.

73 Woerlein, Andreas: Proposed legislation in the fight against child abuse. In: ZD-Aktuell 2022, 01251.

74 Montag, Miriam: EU Commission plans new law against child abuse. In: becklink 2023186.

Microsoft, for example, reports an error rate of 12% for its 'grooming detection', which would lead to human readings of the private conversations of hundreds of thousands of EU citizens from several million conversations that are reviewed and reported. The Swiss Federal Police report a similar situation, citing a hit rate of 14 % for machine recognition of known child abuse portrayals; the search for unknown portrayals required by the regulation is expected to be far less accurate. Again, with millions of reports expected, the private images of millions of Union citizens shall be senselessly seen en masse by human reviewers - photos that may not depict child abuse, but may well show intimate scenes. Overall, this shows a violation of the surveillance principles elaborated by the ECJ in its decisions on data retention." [75]

For the reasons mentioned above and against the background of the previous case law of the European Court of Justice on data retention, the mere existence of mass surveillance without any reason speaks for the disproportionate nature of the interference. For data subjects, this creates a feeling of constant surveillance, which actually takes place all the time, which restricts and influences communicative behaviour. [76]

6. Conclusion

Protection against sexual abuse of minors on the internet is becoming more and more important, as the internet and messenger services are playing an increasingly important role in young people's lives and the risk of such abuse is also increasing as a result. For the above reasons, however, it is questionable whether the current draft regulation represents any added value at all for the intended plan. Against the background of the previous case law of the EU Court of Justice on data retention, it can be assumed that stringent requirements are to be met by Regulation 2022/0155 (COD) and that the draft regulation in its current version is unlikely to enter into force in this form. It seems unlikely that a general monitoring of individual communications would withstand the scrutiny of (European) fundamental rights. Moreover, an expansion of surveillance to other areas would be possible and is to be feared. Based on the above-mentioned aspects and problems, the current draft regulation provides for disproportionate interference with the fundamental rights of the CFR under review.

In addition, many questions and requirements for chat control, especially the actual procedure with regard to end-to-end encrypted services, have remained open so far and need clarification. Thus, continued efforts are needed in the course of the legislative process to be able to realise the important goal of child protection without abandoning the principles of encryption of individual messenger messages.

***

75 Zurawski, Paul: EU Commission: Proposal "Chat control". In: ZD-Aktuell (Journal for Data Protection) 2022, 01240.

76 Dörr, Grote, Marauhn: EMRK/GG Concordance Commentary. Tübingen 2022, Section 20 para. 97.