COMBATING CHILD SEXUAL ABUSE ONLINE IN EUROPEAN UNION AND THE GENERAL PROCESSING OF ELECTRONIC COMMUNICATIONS

Anđela ĐUKANOVIĆ, PhD[1]

The fight against child sexual abuse and exploitation is recognized as a priority for the EU, having in mind the significant increase in detected cases of online child sexual abuse in recent years. In order to resolve issue of online child sexual abuse, EU resorted to voluntary practice of processing online interpersonal communications by service providers, not based on firm legal basis. After extension of the scope of the Privacy and Electronic Communications Directive 2002/58/EC, this voluntary practice was paused, until the adoption of Regulation (EU) 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC. However, it seems that the imposed limitations on the right to private life and protection of personal data do not respect the essence of these rights, there was no detailed analysis of necessity and proportionality of general processing of content data and possible adverse effects on combating online child sexual abuse.

KEY WORDS: online child sexual abuse / private life / protection of personal data / Regulation (EU) 2021/1232 / electronic communications

1. INTRODUCTION

The fight against child sexual abuse and exploitation is recognized as a priority for the EU, having in mind the significant increase in detected cases of child sexual abuse in recent years.[2] In many cases, children are sexually abused by persons

[1] Research Fellow, Institute of Criminological and Sociological Research, andjelasto@sbb.rs

[2] COM(2020) 607 final, p. 1.

they know and trust, and on whom they are dependent. This makes these crimes difficult to prevent and detect, and there are indications that the COVID-19 crisis has exacerbated the problem, especially for children who live with their abusers (WePROTECT Global Alliance, World Childhood Foundation, Unicef, UNDOC, WHO, ITU, End Violence Against Children, UNESCO, 2020:1).

Confidentiality of communications is an essential part of the right to private and family life and protection of personal data. In light of the significant increase in reports of child sexual abuse online over the last decade, the EU approved a controversial law that would allow digital companies to detect and report child sexual abuse on their platforms for the period of three years, without the fear of violating Europe's privacy laws.[3] It will probably cease to be valid before this period, when the permanent regulation on subject is adopted. Temporary derogation was adopted because of the extended scope of the Privacy and Electronic Communications *Directive 2002/58/EC (*hereinafter*:* ePrivacy Directive) resulting from the entry into force of the European Electronic Communications Code Directive (hereinafter: EECC Directive) in December 2020.[4] Providers of certain interpersonal communications services, such as webmail and messaging services, previously used specific technologies on a voluntary basis to detect online child sexual abuse on their services, and report it to law enforcement authorities. This activity was previously governed solely by Regulation (EU) 2016/679 (hereinafter: General Data Protection Regulation). However, this voluntary activities constituted an interference with the right for private and family life and to the protection of personal data of all users of number-independent interpersonal communications services, and cannot be justified merely on the grounds that providers were using certain technologies at a time when number independent interpersonal communications services did not fall within the definition of 'electronic communications services'.[5] Protection of right to private life and personal data however is not absolute, and can be limited under certain circumstances.

2. EU STRATEGY IN COMBATING CHILD SEXUAL ABUSE ONLINE

The fight against child sexual abuse is recognized as a priority for the EU. As a result, EU adopted Strategy for a more effective fight against child sexual abuse, which should be implemented in the period of five years (2020-2025). Numbers

[3] Official Journal of the European Union, L 274/41, 30.7.2021.

[4] Official Journal of the European Union, L 201, 31.7.2002; Official Journal of the European Union*,* L 321, 17.12.2018.

[5] Official Journal of the European Union, L 274/41, 30.7.2021, paras 7-8.

concerning the child abuse online in EU are truly alarming. Some analysis of child sexual abuse online in EU (e.g. images exchanged in the EU, victims in the EU, etc.), suggest that there is an increase from 23 000 reports in 2010 to more than 725 000 in 2019.[6] It seems that the hosting of child sexual abuse URLs is almost exclusively located in Europe (90%), compared to other continents (Internet Watch Foundation, 2020). Also, there is an increase in number of URLs in 2020, compared to 2019 (Internet Watch Foundation, 2020). Interpol also reported increased sharing of child exploitation material through peer-to-peer networks during the COVID-19 pandemic (Interpol, 2020).

EU Strategy for a more effective fight against child sexual abuse, is aimed at full implementation of Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography (hereinafter: Child Sexual Abuse Directive), adopted more than decade ago.[7] At the same time, Strategy is directed at assessment of the Child Sexual Abuse Directive implementation in practice, in terms of effectiveness, efficiency, relevance, and particularly assessment of the online aspects of these crimes, where doubts exist as to whether the present framework is adequate after ten years of technological changes and the significant growth of online sharing.[8]

EU Strategy for a more effective fight against child sexual abuse also states that the use of encryption technology for criminal purposes needs to be immediately addressed through solutions which could allow companies to detect and report child sexual abuse in end-to-end encrypted electronic communications, which are beneficial for ensuring privacy, but also facilitate secure channels for perpetrators.[9] The Commission has launched an expert process to find 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.[10]

3. REGULATION ON TEMPORARY DEROGATION

EECC Directive extended the scope of the e-privacy Directive to over the top (OTT) inter-personal communication services such as messenger services and email. The ePrivacy Directive does not contain a legal basis for voluntary process-

6 COM(2020) 607 final, p. 1.

7 Official Journal of the European Union, L 335, 17.12.2011.

8 COM(2020) 607 final, p. 6.

9 COM(2020) 607 final, p. 2.

10 COM(2020) 607 final, p. 16.

ing of content and traffic data for the purpose of detecting child sexual abuse. In the absence of legislative measures under the Article 15 of the e-privacy Directive, measures to detect child sexual abuse undertaken by these providers, which process content or traffic data, would lack a legal basis.[11]

The US National Center for Missing and Exploited Children (NCMEC) showed a 46% drop of reports of EU child sexual abuse-related cases in the weeks after the European Electronic Communication Code entered into force compared to the previous weeks, as a direct consequence of the new EU privacy legislation (US National Center for Missing and Exploited Children). This had led to child rights and other human rights organizations to urge for adoption of a temporary derogation to the ePrivacy Directive (Eurochild, 2021). In July 2021, EU adopted Regulation (EU) 2021/1232 on a temporary derogation from certain provisions of ePrivacy Directive as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse (hereinafter: Regulation on temporary derogation). Regulation on temporary derogation is seen only as a temporary solution to fix an acute emergency, and there is a need for permanent answer to counter a persistent threat against children (European Commission, 2021). However, there are statements that the Swiss Federal Police found that in the vast majority of cases (86%), innocent citizens are reported for having committed an offence due to the unreliable technology (Betruzzi, 2021).

Regulation on temporary derogation provides for a temporary derogation from Articles 5(1) and 6(1) of ePrivacy Directive which protect the confidentiality of communications and traffic data.[12] EECC Directive extended the

[11] COM(2020) 607 final, p. 4. According to Article 15 of the e-privacy Directive, provided rights and obligations can be restricted if this is necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defense, public security, and the prevention, investigation, detection and prosecution of criminal offences or in case of unauthorized use of the electronic communication system, Official Journal of the European Union, L 201, 31.7.2002, Article 15.

[12] Member States shall ensure the confidentiality of communications and the related traffic data, and particularly, prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorized to do so in accordance with above mentioned Article 15(1), Official Journal of the European Union, L 201, 31.7.2002, Article 5 (1); "traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication." Official Journal of the European Union, L 201, 31.7.2002, Article 6(1).

definition of electronic communication services online. Under the EU law, number-independent interpersonal communications service represents "an interpersonal communications service which does not connect with publicly assigned numbering resources, namely, a number or numbers in national or international numbering plans, or which does not enable communication with a number or numbers in national or international numbering plans".[13] This for an example includes popular services as Facebook Messenger, dating applications, emails or any other form of online communication that might develop. According to Regulation on temporary derogation, the term of 'online child sexual abuse material' encompasses definitions of child pornography, pornographic performance, and solicitation of children from Child Sexual Abuse Directive, and 'online sexual abuse' represents online child sexual abuse material and solicitation of children.[14]

Regulation on temporary derogation does not apply to the scanning of audio communications. Articles 5(1) and 6(1) of ePrivacy Directive do not apply to the confidentiality of communications involving the processing by providers of personal data, if certain conditions are met. This is possible if "processing is strictly necessary and proportionate for the use of specific technology for the sole purpose of detecting and removing online child sexual abuse material and reporting it to law enforcement authorities and to organizations acting in the public interest against child sexual abuse and of detecting solicitation of children and reporting it to law enforcement authorities or organizations acting in the public interest against child sexual abuse".[15]

Compared to initial Proposal on temporary derogation, there is an extensive list of other conditions that must be met.[16] The technologies used for the stated purpose, must be "in accordance with the state of the art in the industry and are the least privacy-intrusive", and "to the extent that they are used to scan text in communications, they are not able to deduce the substance of the content of the communications but are solely able to detect patterns which point to possible online child sexual abuse". Therefore, the scanning is strictly limited to detecting patterns, which is a significant improvement compared to initial Proposal on temporary derogation.

Also, in respect of any specific technology used, prior data protection impact assessment must be conducted, the technologies used must be sufficiently reliable

---

13 Official Journal of the European Union, *L 321, 17.12.2018, Article 2(7).*

14 Official Journal of the European Union, L 335, 17.12.2011, Article 2 (c), Article 2 (e) and Article 6.

15 Official Journal of the European Union, L 274/41, 30.7.2021, Article 3 (a)i.

16 COM/2020/568 final.

and limiting to the maximum extent possible errors, patterns of possible solicitation of children are limited to the use of relevant key indicators, and objectively identified risk factors such as age difference and the involvement of a child in the scanned communication.[17] Providers are also obliged to ensure human oversight of and, where necessary, human intervention in the processing, to establish appropriate procedures and redress mechanisms, and to inform users of the fact that they have invoked the derogation.[18] Where suspected online child sexual abuse has been identified, providers must report it to competent authorities without delay, block the account, or suspend or terminate the provision of the service, and to create a unique, non-convertible digital signature ('hash') of data reliably identified as online child sexual abuse material.[19] The data is stored no longer than strictly necessary for the relevant purpose, but no longer than 12 months from the date of the identification.[20]

File Hashing is the most elementary technology used to detect online child sexual abuse, used to automatically detect content and/or behaviors, the intermediate category is Computer Vision and the most innovative is Artificial Intelligence which is the most advanced type of artificial intelligence and can potentially cope with the most complex scenarios (Council of Europe, 2021). Regulation on temporary derogation does not include end-to-end encryption communication, however this may be the case in the planed long-term legislation, and the processing of data will probably be mandatory for the providers. End-to-end encryption represents a method of secure communication that prevents third parties from accessing data, meaning that only data sender and receiver are able to read the massage. There are technologies that are able to access targeted data contained in end-to-end encryption, like the client-side scanning. This technology implies that every relevant device must have installed softer that will monitor activities and alert authorities. However, this particular technology is being criticized as less secure for the users, prone to abuse from unauthorized or authorized parties, with possibility of false positive results (Abelson et al, 2021).

---

17 Official Journal of the European Union, L 274/41, 30.7.2021, Article 3 (c), Article 3 (e-f).

18 Where users content has been removed or their account has been blocked or a service offered to them has been suspended, to inform users of the avenues for seeking redress from them, and to provide possibility of lodging a complaint and the right to a judicial remedy, Official Journal of the European Union, L 274/41, 30.7.2021, Article 3 (f)i-vi.

19 Official Journal of the European Union, L 274/41, 30.7.2021, Article 3 (h)i-iii.

20 Official Journal of the European Union, L 274/41, 30.7.2021, Article 1 (h)i.

4. INTERFERENCE WITH THE RIGHT TO PRIVATE AND FAMILY LIFE, AND THE PROTECTION OF PERSONAL DATA

Since the Regulation on temporary derogation recognizes that voluntary activities of Providers of interpersonal communications services in detection of online child sexual abuse represent an interference with the right for private and family life and to the protection of personal data (even before the entry into force of the EECC Directive), it is necessary to assess whether this interference is in accordance with Article 52(1) of the EU Charter of Fundamental Rights. Article 52(1) of the Charter sets out specific criteria that must be met by any legislation that seeks to limit the exercise of the rights and freedoms provided by the Charter. These criteria are that: 1) the limitation must be provided for by law; 2) it must respect the essence of the rights and freedoms; 3) Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others.[21] In addition, under a relatively new right to protection of personal data, such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.[22] Usually, courts do not explore and interpret the right to protection of personal data independently from the right to private life, which is seen as a well-established fundamental right, and also, these right are closely linked (Pia & Bonnici, 2014: 142).

It must be noted that there was no impact assessment on fundamental rights for the initial Proposal. European Parliamentary Research Service (EPRS) issued Targeted substitute impact assessment afterwards, on request of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (EPRS, 2021).

When it comes to legal basis of Regulation on temporary derogation, it is stated that "this Regulation does not provide for a legal ground for the processing of personal data by providers for the sole purpose of detecting online child sexual abuse on their services and reporting it and removing online child sexual abuse material from their services, but it provides for a derogation from certain provisions of Directive 2002/58/EC."[23] It is also stated that the Regulation on temporary derogation is based on Article 114 TFEU, which is very general in nature. Article 114 TFEU use as a legal basis is controversial, since it has been successfully challenged before the Court of Justice of the European Union (CJEU) on several occasions,

---

21 Official Journal of the European Union. C 326/391, 26.10.2012, Article 52 (1).

22 Official Journal of the European Union. C 326/391, 26.10.2012, 8 (2).

23 Official Journal of the European Union, L 274/41, 30.7.2021, par. 10.

when the measures in question did not to fulfil the objectives on the establishment and functioning of the internal market (Wållgren, 2016: 5). Also, Regulation on temporary derogation is based on Article 16 TFEU which provides a "specific legal basis for the adoption of rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law".[24] However, it is clear that processing of personal data is being carried by private actors, on voluntary basis.

In addition, Regulation on temporary derogation states that General Data Protection Regulation remains applicable to the processing of personal data.[25] According to General Data Protection Regulation, processing of personal data is possible if one out of six conditions set out in Article 6(1) is fulfilled. [26] It is evident that first two conditions are not applicable, that the data subject has given consent or that the processing is necessary for the performance of a contract (EPRS, 2021: 28-29). According to Opinion of European Data Protection Supervisor, since the derogation concerns voluntary processing of personal data, legal basis also cannot be found in Article 6(1)c of the General Data Protection Regulation, aimed at processing which is necessary for compliance with a legal obligation to which the controller is subject (European Data Protection Supervisor, 2020 §19). Article 6(1)e of the General Data Protection Regulation, which is directed at processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, is not a valid legal basis, since the controllers are not public authorities, and processing on this basis must be explicitly stated in Regulation on temporary derogation, which is not the case (EPRS, 2021: 30).

However, the voluntary practice of processing data in order to protect the vital interest set out in Article 6(1)(d) of the General Data Protection Regulation, might serve as legal basis. Relevant vital interests, are the interests of any child that might be the victim of online sexual abuse (EPRS, 2021: 29). Vital interest is defined as a "interest which is essential for the life of the data subject or that of another natural person", however General Data Protection Regulation suggests that this basis should be used exceptionally, where the processing cannot be manifestly based on other legal basis, and sets out as an example humanitarian emergencies, in particular situations of natural and man-made disasters.[27]

Finally, according to 6(1)(f) of the General Data Protection Regulation processing might be lawful if it is "necessary for the purposes of the legitimate inter-

---

24 Official Journal of the European Union, L 274/41, 30.7.2021, par.15.

25 Official Journal of the European Union, L 274/41, 30.7.2021, paras. 13-14, Article 1.

26 Official Journal of the European Union*, L 119, 4.5.2016. Article 6(1).*

27 Official Journal of the European Union*, L 119, 4.5.2016*, par 46.

ests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child". However, these cumulative requirements need case-by-case balancing exercise, where the controller must ensure that the legitimate interests are not overridden by the interests or rights and freedoms of data subject which require protection of personal data" (EPRS, 2021: 31). This basis might be questionable when the processing is aimed at communication of every subject, and not targeted at possible suspects, and where controller is a private actor. Therefore, it can be concluded that the processing of personal data under the Regulation on temporary derogation, or voluntary processing that took place before entry into force of the EECC Directive, is/was based on a shaky legal ground.

Any restriction must respect the essence of the right that is being restricted, so the restrictions that are extensive and intrusive to the extent that they void a fundamental right of its basic content, cannot be justified. General exclusion of all user's rights with regard to all number-independent interpersonal communications, do not seem justified in this respect. European Data Protection Board was of this opinion in relation to application of restrictions of General Data Protection Regulation. General exclusion of all data subjects' rights with regard to all data processing operations as well as a general limitation of the rights of all users for specific data processing operations, shall be considered unlawful, even without the need to further assess whether it serves an objective of general interest or satisfies the necessity and proportionality criteria (European Data Protection Board, 2020: 6).

Interference with the right for private and family life and to the protection of personal data must meet: a) objective of general interest recognized by the EU, which is in this case the effective prevention, detection and prosecution of related crimes, the protection of victims may be identified as adequate, and b) the need to protect the rights and freedoms of others, in this case the right to such protection is necessary for their well-being of the child (EPRS, 2021: 32).

The interference with the right for private and family life and to the protection of personal data, also must be necessary and proportionate for achieving the objective, and answer to this question is not easy task. Necessity of some measure implies that the measure used, is the least intrusive for achieving one objective. As stated by the CJEU, in order to satisfy the requirement of proportionality, the legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, that legislation must be legally binding under domestic law, and must indicate in under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly neces-

sary.[28] CJEU also stated that the need for such safeguards is all the greater where personal data is subjected to automated processing, and especially where the protection of the sensitive category of personal data is at stake.

There is no elaborate evidence on efficiency of the practice included in Regulation on temporary derogation in fighting sexual abuse online, and that there are no other less intrusive but effective measures. For example, this could lead to increased use of decentralized or encrypted channels of communications by offenders, and in general their effort to reach out from law enforcement authorities (EPRS, 2021: 34). It is highly likely that the practice of offenders will shift to other methods, although Regulation on temporary derogation will have the effect of making the commission of the crime more difficult. The Commission and EU Member States also did not provide information about the actual number of prosecutions and convictions that resulted from existing voluntary practices (EDRI, 2021).

In addition, Regulation on temporary derogation uses terms like "least privacy-intrusive", that technologies used are "sufficiently reliable", and limited to the use of "relevant key indicators", with no further elaboration, except that the technology must not deduce the substance of the content of the communications, but detect patterns. Some of dilemmas might be resolved in future, since the European Data Protection Board will ensure the oversight of the scanning practices and technologies used, and prepare guidelines on which technologies could be used.[29]

There was also no detailed analysis of the reliability of technology's that can be used. Automatic scanning by algorithms of all chat conversations and emails, of all users, without court order or any initial suspicion, can lead to errors, which might further lead to private content being analyzed by private company employees and police authorities. EU is relying on technologies managed by private US organizations, and encouraging them in surveillance of the sensitive personal data.

According to Opinion of European Data Protection Supervisor, general, indiscriminate and automated, analysis of all text-based communication with an aim of identifying new infringements does not respect the principle of necessity and proportionality, even with additional safeguards (EDPS, 2020 §26). Any interception of private communications must target only the person or persons under investigation, and not all users of the service, based on specific, reasonable, individual level suspicion, and any investigation of private communications must be specifically and individually warranted by a judge (EDRI, 2022). European Parliamen-

[28] La Quadrature du Net and Others v Premier ministre and Others, ECLI:EU:C:2020:791, par. 132.

[29] Official Journal of the European Union, L 274/41, 30.7.2021, Article 4.

tary Research Service was also against the use of these techniques to monitor all private messages, but to be limited to private messages of persons under suspicion of soliciting child abuse or distributing online child sexual abuse material (EPRS, 2021: 47). The CJEU, retreated that the general and indiscriminate retention of traffic and location data, and the particularly serious interference constituted by the automated analysis of that data, can meet the requirement of proportionality only in situations in which a Member State is facing a serious threat to national security which is shown to be genuine, present or foreseeable, and if the duration of that retention is limited to what is strictly necessary.[30]

Council of Europe Convention on Cybercrime (Budapest *Convention*) seems directed at traffic data, and the collection of this data is regarded in principle to be less intrusive since as such it doesn't reveal the content of the communication.[31] Convention on Cybercrime addresses the subject of real-time collection and recording of traffic data, but for the purpose of specific criminal investigations or proceedings. However, Article 21 of the Convention on Cybercrime is directed to collection or recording of "content data" in real-time, in relation to serious offences determined by domestic law. Term of content data is not defined in Convention on Cybercrime (Baron, 2002: 277). Explanatory Report to the Convention on Cybercrime indicates that this term refers to the content of communication. The conditions and safeguards applicable to real-time interception of content data may be more stringent than those applicable to the real-time collection of traffic data.[32] Importantly, Convention on Cybercrime is directed at "specified communications" (Articles 20-21). Therefore, the Convention does not require or authorize the general or indiscriminate surveillance and collection of large amounts of traffic data, where criminal activities are hopefully sought to be detected, the judicial or other order authorizing the collection must specify the communications to which the collection of traffic data relates.[33] For example, measures from the recently adopted Second Additional Protocol to the Convention on Cybercrime, apply only to specific criminal investigations and proceedings, and do not entail general communications surveillance.[34]

---

30 La Quadrature du Net and Others v Premier ministre and Others, ECLI:EU:C:2020:791, par. 177.

31 Explanatory Report to the Convention on Cybercrime, European Treaty Series - No. 185, par. 29.

32 Explanatory Report to the Convention on Cybercrime, European Treaty Series - No. 185, par. 231;

33 Explanatory Report to the Convention on Cybercrime, European Treaty Series - No. 185, par. 219.

34 Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, CM(2021)57-final, 17 November 2021.

EU and Member States' responses to serious problem of combating online child sexual abuse must invest in prevention, education, victim support, social services, welfare and other methods of addressing the root causes of the issues, and the technological fixes are not solution to complex societal problems (EDRI, 2022). Many Member States faced delays in the implementation of the Child Sexual Abuse Directive into their national law. EU Strategy for a more effective fight against child sexual abuse, recognizes existing challenges in areas of prevention, criminal law, and assistance, support and protection measures for child victims.[35]

In light of the EU accession negotiations of Republic of Serbia, there is no reaction in relation to the implementation of Regulation on temporary derogation. This might be the case since the adoption of permanent legislation is expected in near future. However, domestic law has numerous safeguards in relation to right to private life and protection of personal data, and possible derogations from these rights. Constitution of republic of Serbia recognizes right to confidentiality of letters and other means of communication, and the derogation is possible "only for a specified period of time and based on decision of the court if necessary to conduct criminal proceedings or protect the safety of the Republic of Serbia, in a manner stipulated by the law".[36] In relation to right to protection of personal data "use of personal data for any the purpose other the one were collected for shall be prohibited and punishable in accordance with the law, unless this is necessary to conduct criminal proceedings or protect safety of the Republic of Serbia, in a manner stipulated by the law".[37] Relevant laws are in accordance with this rights', for example investigation can be initiated against a specific person for whom there are grounds for suspicion that he/she has committed a criminal offence, or against an unknown perpetrator when there are grounds for suspicion that a criminal offence has been committed.[38] When it comes to the changes in the number of reported criminal offenses against sexual freedom at the beginning of pandemics, it seems that there are no significant changes in this respect (Đokić & Čvorović, 2014:270).

5. CONCLUSION

It seems that there is lack of timely and complete action of the Commission, in the matter that is recognized as a EU priority. Certainly, there was a focus on find-

35 COM(2020) 607 final, p. 3.

36 Official Gazette of the RS, No. 98/2006, Article 41.

37 Official Gazette of the RS, No. 98/2006, Article 42.

38 Official Gazette of the RS, No. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 - decision CC and 62/2021 – decision CC, Article 295.

ing quick solutions to complex issues. It was convenient to find quick solution for growing online child sexual abuse in EU, and the extended scope of ePrivacy Directive just revealed privacy issues of the existing practice. Interference does not have firm legal basis. Also, respect of the essence of the right that is being restricted is questionable. There is no detailed analysis of necessity and proportionality of general processing of data in combating online child sexual abuse, and possible adverse effects on combating online child sexual abuse, especially weather this could make crime more difficult to detect in future, when offenders shift to other, less risky methods. This might lead to inclusion of other online crimes in general data scanning of private communications content. Ultimately, it must be considered why the privacy of online communications is less important than offline communication. If there is no difference, then this might lead to further privacy intrusions, as a legitimate method of fight against serious crimes. Some changes can be expected in close future, since there is a strong indication that the scanning will be mandatory for providers, but more importantly, end-to-end encrypted electronic communications might be included. Although, it must be admitted that the online privacy intrusions are aimed at "detecting patterns", and not full access to content. In this respect, assessment of concrete technology relatability, for processing of certain forms of data is essential.

REFERENCES

1. Abelson H., Anderson R., et al. (2021), "Bugs in our Pockets: The Risks of Client-Side Scanning", arXiv, Cornell University, 2021, pp 1-46., https://doi.org/10.48550/arXiv.2110.07450, accessed on 07. 04. 2022.
2. Baron R. M. F. (2002) A Critique of the International Cybercrime Treaty, Journal of Communications Law and Technology Policy, 10 (2), pp. 263-278.
3. Bertuzzi L. (2021), New EU law allows screening of online messages to detect child abuse, Euractiv, https://www.euractiv.com/section/data-protection/news/new-eu-law-allows-screening-of-online-messages-to-detect-child-abuse/, accessed on 06. 04. 2022.
4. Charter of Fundamental Rights of the European Union. Official Journal of the European Union. C 326/391, 26.10.2012.
5. 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, Brussels, 24.7.2020, COM(2020) 607 final.

6. Constitution of Republic of Serbia, Official Gazette of the RS, no. 98/2006.
7. Council of Europe (2021) Respecting human rights and the rule of law when using automated technology to detect online child sexual exploitation and abuse- Independent experts' report, Directorate General of Human Rights and Rule of Law - DG I and Directorate General of Democracy - DG II
8. Criminal Procedure Code, Official Gazette of the RS, no. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 - decision CC and 62/2021 – decision CC.
9. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast), Official Journal of the European Union, L 321, 17.12.2018.
10. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance, Official Journal of the European Union, L 321, 17.12.2018.
11. 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), Official Journal of the European Union, L 201, 31.7.2002.
12. Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, Official Journal of the European Union, L 335, 17.12.2011.
13. Đokić I., Čvorović D. (2021) Criminal Legal Challenges in Republic of Serbia during COVID-19 Pandemic, Crimen, XII (3), pp. 259–276
14. EDPS (2020) Opinion on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online, https://edps.europa.eu/sites/default/files/publication/20-11-10_opinion_combatting_child_abuse_en.pdf, accessed on 30. 03. 2022.
15. EDRI (2021) Wiretapping children's private communications: Four sets of fundamental rights problems for children (and everyone else), https://edri.org/our-work/children-private-communications-csam-fundamental-rights-issues/, accessed on: 02. 04. 2022.
16. EDRI (2022) Scanning private communications in the EU EDRi's principles for derogating from the ePrivacy Directive for the purpose of detecting online child sexual abuse material, https://edri.org/wp-content/uploads/2022/02/EDRi-principles-on-CSAM-measures.pdf, accessed on: 05. 04. 2022.

17. EPRS (2021) Commission proposal on the temporary derogation from the e-Privacy Directive for the purpose of fighting online child sexual abuse – Targeted substitute impact assessment, Brussels.
18. Eurochild (2021) Eurochild calls on the EP to keep children safe online by adopting a Temporary Derogation to the ePrivacy Directive, https://www.eurochild.org/news/eurochild-signs-joint-letter-asking-to-adopt-a-temporary-derogation-to-the-eprivacy-directive/, accessed on 31.03. 2022.
19. European Commission (2021) Commissioner Johansson's speech at the plenary debate on the use of technologies for data processing to fight online child sexual abuse, https://ec.europa.eu/commission/commissioners/2019-2024/johansson/announcements/commissioner-johanssons-speech-plenary-debate-use-technologies-data-processing-fight-online-child_en, accessed on 31.03. 2022.
20. European Data Protection Board (2020) Guidelines 10/2020 on restrictions under Article 23 GDPR, Version 1.0, Adopted on 15 December 2020, https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202010_article23_en.pdf, accessed on 02. 04. 2022.
21. Explanatory Report to the Convention on Cybercrime, Budapest, 23.XI.2001, European Treaty Series - No. 185, Council of Europe.
22. Internet Watch Foundation (2020), The Annual Report 2020- Geographical hosting, https://annualreport2020.iwf.org.uk/trends/international/geographic, accessed on 31.03. 2022.
23. Interpol (2020) INTERPOL report highlights impact of COVID-19 on child sexual abuse, https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-highlights-impact-of-COVID-19-on-child-sexual-abuse, accessed on 08. 04. 2022.
24. La Quadrature du Net and Others v Premier ministre and Others, Judgment of the Court (Grand Chamber) of 6 October 2020, ECLI:EU:C:2020:791.
25. Pia J., Bonnici M. (2014) Exploring the non-absolute nature of the right to data protection, International Review of Law, Computers & Technology, 28(2), pp. 131-143.
26. 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, Brussels, 10.9.2020, COM/2020/568 final.

27. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, L 119, 4.5.2016.
28. Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse, Official Journal of the European Union, L 274/41, 30.7.2021.
29. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, CM(2021)57-final, 17 November 2021.
30. US National Center for Missing and Exploited Children, Battle Won, But Not the War in the Global Fight For Child Safety, https://www.missingkids.org/childsafetyfirst, accessed on 29.03. 2022.
31. Wållgren M. (2016) Exploring the Outer Limits of Article 114 TFEU – towards a general power?, Master's Thesis, Uppsala Universitet.
32. WePROTECT Global Alliance, World Childhood Foundation, Unicef, UNDOC, WHO, ITU, End Violence Against Children, UNESCO (2020) COVID-19 and its implications for protecting children online, https://www.unicef.org/sites/default/files/2020-04/COVID-19-and-Its-Implications-for-Protecting-Children-Online.pdf, accessed on: 02. 04. 2022.

Dr Anđela Đukanović
Naučni saradnik, Institut za kriminološka i sociološka istraživanja u Beogradu

BORBA PROTIV SEKSUALNOG ZLOSTAVLJANJA DECE NA INTERNETU U EVROPSKOJ UNIJI I OPŠTA OBRADA ELKTRONSKIH KOMUNIKACIJA[39]

Borba protiv seksualnog zlostavljanja i seksualnog iskorišćavanja dece prepoznata je kao prioritet u okviru EU, s obzirom na zabeležen porast otkrivenih slučajeva seksualnog zlostavljanja putem interneta poslednjih godina. Da bi rešila pitanje seksualnog zlostavljanja dece na internetu, EU je pribegla dobrovoljnoj praksi obrade interpersonalnih elektronskih komunikacija od strane pružalaca usluga, koje nije zasnovano na čvrstoj pravnoj osnovi. Nakon proširenja obima Direktive 2002/58/EC o obradi ličnih podataka i zaštiti privatnosti u elektronskom komunikacionom sektoru, ova dobrovoljna praksa je privremeno obustavljena, do usvajanja Uredbe (EU) 2021/1232 o privremenom odstupanju od određenih odredbi Direktive 2002/58/EC. Međutim, čini se da predviđena ograničenja prava na privatnost i zaštitu podataka o ličnosti ne poštuju suštinu ovih prava, nije izvršena detaljna analiza neophodnosti i proporcionalnosti opšte i neselektivne obrade komunikacija svih korisnika, ali ni mogućih štetnih posledica na suzbijanje seksualnog zlostavljanja dece na internetu.

KLJUČNE REČI: seksualno zlostavljanje dece / privatan život / zaštita ličnih podataka / Uredba (EU) 2021/1232 / elektronske komunikacije

[39] Ovaj rad nastao je kao rezultat istraživačkog angažovanja prema Planu i programu rada Instituta za kriminološka i sociološka istraživanja za 2022. godinu (na osnovu Ugovora broj 451-03-68/2022-14 od 17. 01. 2022 god.)