UNIVERSITY OF TIMISOARA
FACULTY OF LAW

UNIVERSITY OF PÉCS
FACULTY OF LAW

JOURNAL OF EASTERN-EUROPEAN CRIMINAL LAW

No. 1/2020

Edited biannually by courtesy of the Criminal Law Departments within the Law Faculties of the West University of Timisoara and the University of Pécs

UNIVERSUL JURIDIC

2020

Universul Juridic Publishing House

Edited by Universul Juridic Publishing House

The journal is indexed in databases SSRN, EBSCO, HeinOnline.

ISSN 2360–4964

Redactor:	Ciprian Radu
Tehnoredactor:	Tania Militaru
Copertă:	Aurelian Leahu

Redacție:
tel.: 0732.320.666
e-mail: redactie@universuljuridic.ro

Distribuție:
tel.: 021.314.93.15
fax: 021.314.93.16
e-mail: distributie@universuljuridic.ro
editurauniversuljuridic.ro
Editura Universul Juridic

Portal:
tel.: 0725.683.560
e-mail: portal@universuljuridic.ro
universuljuridic.ro
Universul Juridic

Librăria UJmag:
tel.: 0733.673.555; 021.312.22.21
e-mail: comenzi@ujmag.ro
ujmag.ro
Ujmag.ro

WEST UNIVERSITY OF TIMISOARA
FACULTY OF LAW

UNIVERSITY OF PÉCS
FACULTY OF LAW

Center of Research in Criminal Sciences
FACULTY OF LAW
West University of Timisoara

JOURNAL OF EASTERN-EUROPEAN CRIMINAL LAW

❍ BOARD OF EDITORS ❍

Streamlining the Fight Against Child Sex Offenders Trough EU Regulation of IP address

Dr. Silvia Signorato*

Abstract

The sexual abuse and the sexual exploitation of children, which includes child pornography, are very serious crimes which must be combated to the highest degree. At present, however, there are still too many legal obstacles in the prevention and the prosecution of these crimes. One of the main obstacles is the difficulty encountered in the collection of IP addresses, which often constitute very important evidence. Each Member State has its own legislation, and there are no clear EU indications regarding the retention period of IP addresses. In this article, a four-year retention period of the IP address is proposed in order to balance the needs of the protection of fundamental rights as well as those of investigative activity. This suggested retention period derives from the analysis of the regulations regarding data retention and the data on the investigative practices of all the Member States, taking into account the need to protect fundamental rights.

Keywords: *IP address, data retention, sexual abuse and sexual exploitation of children, child pornography, cyber investigations*

I. Introduction

This article is aimed at evaluating the significance of IP addresses in the fight against child sex offenders in the European Union. This topic is analysed with regard to data retention laws[1].

In Europe, the proportion of children sexually assaulted during their childhood is between 10% and 20%[2]. The sexual abuse and the sexual exploitation of children, including child pornography, constitute serious violations of fundamental rights. In

* PhD, Assistant Professor in Criminal Procedure – University of Padua (Italy), Lecturer in Criminal Procedure – University of Innsbruck (Austria). E-mail: silvia.signorato@unipd.it.

[1] Data retention is the storage activity of 'traffic data' for a given period (which is called 'retention time') for the purposes of the prevention, investigation, detection or prosecution of criminal offences. Traffic data "means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service" (see article 1, letter d of the Convention on Cybercrime – Council of Europe, 2001). Whenever personal data is stored, there is a violation of the Right to protection of personal data. This also occurs in cases where the processing of personal data takes place by European Agencies or a prosecution office, e.g. the European Public Prosecutor's Office (EPPO). See in this respect P. De Hert, V. Papakonstantinou (2019). Data Protection and the EPPO. *New Journal of European Criminal Law*, v. 10, p. 34-43.

[2] See https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/child-sexual-abuse_en.

particular, they are violations of the rights of children to the protection and the care necessary for their well-being, as provided for by United Nations Convention on the Rights of the Child[3]. Moreover, Article 34 of that Convention provides that "States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse".

These crimes are particularly cruel and cause huge suffering to the victims. Unfortunately, this phenomenon continues to grow, mainly due to four factors: the Internet (in particular, the Darknet)[4]; the ease of international travel aimed at child sex tourism; business related to this kind of crime; and the lack of an adequate legal framework. These factors are described in detail.

1. The Internet facilitates the commission of serious crimes such as the sexual abuse and the sexual exploitation of children, including child pornography[5]. This is because the Internet makes these actions easier: grooming[6]; solicitation of children for sexual purposes; production, distribution and use of child pornography; arranging and booking trips aimed at child sex tourism (CST); incitement and aiding such crimes. Furthermore, the use of anonymisation programs or of the Darknet[7], which makes investigations more difficult, helps to guarantee the anonymity of those who commit crimes.

2. The existence of organised international travel aimed at child sex tourism is extremely worrying. This phenomenon started in the second half of the 20th century[8] and shows no sign of abating. On the contrary, it is increasingly organized and difficult to combat.

---

[3] See Preamble of such a Convention. See also Article 24 Charter of Fundamental Rights of the European Union. In addition, see Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography of 2000, the Council of Europe's Convention on the Protection of Children against Sexual Exploitation and Abuse of 2007 (a.k.a., the Lanzarote Convention), and the Directive 2011/92/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.

[4] According to Meter (2018). Annual Report. Pedophilia and child pornography, p. 17, these different types of paedophiles which use the Internet can be identified: Closet collector; Isolated collector; Cottage collector; Commercial collector; Pedo-crime (organized).

[5] See P. Torretta, C. Bonucchi. M. Cotroneo, E. D'Amato (2016). White paper on child sex offenders. Treatment and diagnostic profile of online sex offenders to the detriment of minors for the prevention of and fight against this phenomenon (CSE Project HOME/2012/ISEC/AG/4000004373, Co-funded by Prevention of and Fight against Crime Programme of the European Union), p. 10-25. A system for automatic recognition of child grooming in online chat conversations is proposed by P. Anderson, Z. Zuo, L. Yang, Y. Qu, 2019. Intelligent Online Grooming Detection System Using AI Technologies. 2019. Paper presented at 2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), New Orleans, United States.

[6] Grooming is the enticement of children or the solicitation of children for sexual purposes. Grooming is the process by which an adult befriends a child in order to commit sexual abuse. See A.-M. McAlinden, (2012). 'Grooming' and the Sexual Abuse of Children: Institutional, Internet and Familial Dimensions, 1st ed. Oxford: Oxford University Press.; S. Ost, (2009). Child pornography and sexual grooming: legal and societal responses. Cambridge: Cambridge University press, p. XIII-273.

[7] The Darknet is an application and protocol layer riding on the Internet where the user navigates in a completely anonymous way. See e.g. J. Pace (2017). Exchange Relations on the Dark Web. *Critical Studies in Media Communication*, 34(1), p. 1-13.

[8] See Commission of the European Communities, 1996: 2, which states that "The sexual exploitation of children in tourism is perpetrated not only by paedophiles, who constitute the hard core of child sex abusers, but also by preferential abusers and occasional abusers. (…) However, the distinction should in no way disguise the unacceptable nature of any such practices".

3. The increase related to sexual abuse and the sexual exploitation of children is enormous and constitutes a real business activity on an international scale. For this reason, such cruel crimes have become attractive even for organized crime networks which have an increasing role in their commission.

4. Finally, the legal framework does not seem entirely adequate and its improvement appears to be urgently needed. The sexual abuse and the sexual exploitation of children are increasingly transnational crimes. They can only be prosecuted on the basis of fast and effective investigative cooperation between states[9]. At the European level, some acts aimed at improving investigative cooperation were issued. Among these acts, there is the one that established the European Investigation Order (EIO)[10]. However, investigators still tend to use this tool too little[11]. Furthermore, although the EIO speeds up the evidence collection time, the collection of e-evidence is still generally too slow. Since an e-evidence is characterised by potential instability and can therefore quickly undergo alteration, degradation, or loss[12], its collection must be timely[13].

The sexual abuse and the sexual exploitation of children, including child pornography, are very serious crimes, which must be combated to the highest degree. Therefore, it is necessary and urgent to remove the legal obstacles to the prosecution of these crimes. In particular, the diversity of the regulations of the various Member States regarding IP Address retention is a significant legal obstacle. This problem is examined in this article, where a possible solution is also suggested.

II. The IP Address: Basic Technical Knowledge

The term IP address means Internet Protocol address. An IP address is a numerical label connected to a computer network that uses the Internet Protocol for

[9] For example, in Operation Tantalio, Interpol, Europol, and Law Enforcement Agencies from fifteen countries in Central America, South America, and Europe, cooperated in the investigation of child sexual abuse material distributed via WhatsApp.

[10] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters. A discussion on EIO can be found in L. Bachmaier Winter (2015). Towards the Transposition of Directive 2014/41 regarding the European Investigation Order in Criminal Matters. *Eucrim*, p. 47-60; M. Daniele (2015). Evidence Gathering in the Realm of the European Investigation Order: From National Rules to Global Principles. *New Journal of European Criminal Law*, p. 179-194; and A. Mangiaracina (2014). A New and Controversial Scenario in the Gathering of Evidence at the European Level: The Proposal for a Directive on the European Investigation Order. *Utrecht Law Review*, p. 113-133.

[11] There are cases where the Judiciary prefers not to request evidence by means of EIO. This is due to several reasons. For example, some judiciaries do not know how to request an EIO; in some cases the judiciary finds the procedure to obtain the EIO too difficult or the preliminary authorization by his/her head is required and this becomes an obstacle.

[12] See S. Signorato, S. (2017). Types and features of cyber investigations in a globalized world. Paşca, V., Ciopec, F. (Eds), *Probleme actuale în dreptul penal european*: Universul Juridic, p. 60.

[13] At present, there are two proposals for a Community act aimed at improving the speed and effectiveness of e-evidence collection. The first one is the Proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final – 2018/0108 (COD). The second one is the Proposal for a directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings COM/2018/226 final – 2018/0107 (COD).

communication. It serves two main functions: host or network interface identification and location addressing. Therefore, on the one hand it enables devices to communicate with each other, and on the other, it is a sort of fingerprint of the device. Each device connected to the network has a specific IP address, different from the one used by all other devices[14].

There are currently two versions of the IP address: IPv4 and IPv6. An IPv4 is a string of four dot-separated numbers between 0 and 255, therefore encoded with 8 bits, for a total of 32 bits[15]. A typical IPv4 address is 192.0.2.53. Version 4 allows the definition of just over four billion unique IP addresses, which are now largely assigned, leading to the risk of their exhaustion[16]. To overcome this problem, version 6, i.e. IPv6, was introduced. An IPv6 is a string of eight colon-separated groups of 4-bit hexadecimal digits, for a total of 128 bits. An example of IPv6 is 2001:0db8::53[17].

Every time a user sends an email, visits a site, participates in a video conference, or performs any online operation, its IP address can be stored by the server[18]. This happens, of course, also in the case of automatic access to the Internet by a device.

The IP address retention is very important for investigation purposes. For example, in the case of a child pornography website, the identification and prosecution of its users is critically based on the knowledge of the IP addresses of those who have connected to it[19]. This is because the IP address allows the unique identification of the device from which the connection to the network occurred.

---

[14] It should be noted that the development of the Internet of Things leads to a significant increase in the number of devices that are connected to the network. See G. Fortino, P. Trunfio (2014). Internet of Things Based on Smart Objects. Berlino: Springer 2014.

[15] ICANN (2011). Beginner's Guide to Internet Protocol (IP) Addresses, p. 5.

[16] ICANN (2011). Beginner's Guide to Internet Protocol (IP) Addresses, p. 5.

[17] Two colons side by side in an IPv6 address means that all the segments between them contain only zeros. If the two colon notation is not used, the address shown in the example becomes 001:0db8:0000:0000:0000:0000:0000:0053.

[18] In several European states a service and content provider within the internet industry can contact, on a voluntary basis, an institutional contact point in order to report either the existence of child sexual abuse material or information relating to child sexual abuse related to its services. The complete list is shown here state by state: Austria: Austrian C4-Cybercrime Competence Centre; Belgium: Central Traficking in Human Beings, Belgian Federal Police; Bulgaria: Intellectual property and illegal content on Internet; Cyprus: Office for Combating Cyber Crime; Czech Republic: Police Presidium, Bureau of Criminal Investigation Service, Cybercrime Department; Germany: German Federal Criminal Police Office (Bundeskriminalamt); Denmark: Danish National Cyber Crime Centre; Estonia: Police and Boarder Guard Board, Intelligence Analysis Division; Spain: Bureau de Investigacion Technologica, Policia Judicial; Finland: Cyber Intelligence Unit, National Bureau of Information; France: O.C.L.C.T.I.C; Greece: Hellenic Cyber Crime Unit; Hungary: National Bureau of Investigation High-Tech Crime Unit; Ireland: Paedophile Investigation Unit, Domestic Violence and Sexual Assault Investigation Unit, National Bureau of Criminal Investigation; Italy: Postal and Communication Police Agency – National Centre for Combating Child-pornography Online – CNCPO; Malta: Malta Police Cyber Crime Unit; Netherlands: Dutch Child Exploitation Team of the National Police of the Netherlands; Poland: Department for Trafficking in Human Beings; Romania: General Inspectorate of the Romanian Police – Countering Organized Criminality Directorate – Countering Computer Crimes Service; Sweden: National Bureau of Investigation; Slovenia: General Police Directorate, Criminal Police Directorate; Slovakia: Slovak Safer Internet Centre; United Kingdom: NCAT Bureau, United Kingdom National Crime Agency; Norway: KRIPOS, National Criminal Investigation Service; Switzerland: CYCO, Federal Criminal Police. Further details about these contact points, in particular their email and phone, can be found in: https://www.europol.europa.eu/report-a-crime/industry-reporting-of-child-sexual-abuse-material.

[19] See J. Davidson (1988). An Introduction to TCP/IP, New York: Springer.

It should be noted that the IP-based identification of the device does not necessarily mean that of those who used it for criminal purposes. This is because the device may be available to several users or may have been stolen, or a hacker may have performed IP spoofing[20]. A further investigation is therefore necessary to identify the offender. In any case, the IP address is always a very important evidence.

III. Retention of IP Addresses and Fundamental Rights

As mentioned above, an IP address can constitute really important evidence. For this reason, the rules of the Member States generally require that the servers store the IP addresses for a specific period of time for the purposes of the prevention, investigation, detection or prosecution of criminal offences or else for the execution of criminal penalties[21].

However, this poses problems with respect to fundamental rights, with particular reference to privacy[22] and the freedom of expression[23]. The fact of being able to

[20] IP address spoofing, or simply IP spoofing, is an attacking technique where the *hacker creates* a false source IP address for the purpose of impersonating another computing system. See M.T. Banday, R.A. Mathangi (2015). Control of IP Address Spoofing – A Comparative Study of IPv4 and IPv6 Networks. Mohammad Tariq Banday (Ed.), Proceedings of 2015 International Conference on Advances in Computers, Communication, and Electronic Engineering, Hazratbal, Srinagar: University of Kashmir, p. 344-351.

[21] Regarding the different problem of the possibility for Computer Security Incident Response Team to keep the IP Address see European Union Agency for Network and Information Security (ENISA) (November 2018), Cooperation between CSIRTs and Law Enforcement: interaction with the Judiciary, p. 21-22: "Under Article 6.1 a) of the GDPR, the processing of personal data, including IP addresses, is permitted for a specific, necessary and proportionate purpose (purpose of legitimate interest pursued by the CSIRTs, as specified on Article 6.1 f) if the data subject (the person concerned, the person whose personal data are processed) gives consent. In the event of an IT incident, there is no consent from the data subject (e.g. IP address holder) who caused the incident. However, according to the GDPR (see Article 13.3) and to Recital 49 it can be considered that the personal information, under certain circumstances, can be processed by the CSIRT even without consent. Recital 49 indeed provides that 'The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), CSIRTs, by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping "denial of service" [DoS] attacks and damage to computer and electronic communication systems."

[22] The Right to privacy was initially conceived as the right to be let alone (see S.D. Warren, L.D. Brandeis (1890). The Right to Privacy. *Harvard Law Review*, 4, p. 193). Subsequently, this right was extended to include the right to have control over access to one's personal information. In essence, a dynamic meaning of privacy was added to the static one. The European Convention on Human Rights provides in Article 8 (Right to respect for private and family life) the protection for both the meanings of privacy. Instead, the Charter of Fundamental Rights of the European Union separately protects private and family life (Article 7) and personal data (Article 8).

[23] See Court of Justice, 8th April 2014, Digital Rights Ireland and Others, Joined Cases C-293/12 and C-59412, paragraph 28. Moreover, see Court of Justice, 21 December 2016 (requests for a

identify those who placed certain information on the Internet, apart from being a violation of people's privacy, can give rise to restrictions on the freedom of expression. In addition, the fact that data storage creates costs for Internet Service Providers should be taken into account.

The preservation of IP addresses is important for both prosecution and defence purposes. As mentioned above, it serves to prevent and combat crimes. Furthermore, it can also be useful for defence purposes since an IP address could also be used by a suspect to prove his innocence.

The need to balance various rights makes it difficult to identify the ideal data storage time of the IP address in accordance with the principle of proportionality. The risk is to lean towards extremes. On the one hand, the exclusive protection of security could lead to the threat of a totalitarian drift. On the other hand, the exclusive attention to privacy could prevent or seriously hinder the prosecution of serious crimes such as the sexual abuse and the sexual exploitation of children.

At the European level there are no directives or regulations establishing a well-defined retention period for the IP addresses. Article 6 of Directive 2006/24/EC generically provided that the period of retention should be "not less than six months and not more than two years from the date of the communication". However, the Court of Justice, 8 April 2014, Digital Rights Ireland and Others, declared Directive 2006/24/EC invalid due to the violation of the principle of proportionality. This important judgement contributed to creating greater sensitivity at the European level towards the respect of fundamental rights, in particular the right to the Protection of personal data.

However, this judgement of the Court of Justice also caused an unforeseen and unwanted consequence, due to the fact that some Member States introduced or interpreted the regulations on data retention too restrictively[24]. The corresponding national regulations were such as to hinder or even prevent the right of defence or, more often, investigative activities. In particular, in some cases, the investigations aimed at combating the sexual abuse and/or the sexual exploitation of children were hindered by unavailability of the necessary IP addresses. This is because the states to which these IP address were requested had already deleted these data due to the too short retention period provided by their own acts. Section 113b German Telecommunications Act is a significant example, worthy of being described in detail. It requires data to be retained for only ten weeks[25]. Such a short retention period has an admirable purpose, namely the protection to the highest degree of fundamental rights, including the right to the protection of personal data. However, European investigative practice has shown that this law causes the violation of other fundamental rights such as child protection, due to the hindering of the prosecution of crimes.

---

preliminary ruling from the Kammarrätten i Stockholm and the Court of Appeal (England & Wales) (Civil Division) — Sweden, United Kingdom) – Tele2 Sverige AB v Post- och telestyrelsen (C-203/15), Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis (C-698/15), joined Cases C-203/15 and C-698/15.

[24] In reference to the first amendments to national data retention laws after the Digital Rights Ireland judgment, see Council of the European Union (6 November 2017), Data retention regimes in Europe in light of the CJEU ruling of 21 December 2016 in Joined Cases C-203/15 and C-698/15 – Report; European Union Agency for Fundamental Rights (FRA) (2017), Fundamental Rights Report 2017, chapter 6 Information society, privacy and data protection, p. 155-172.

[25] In case of location data the retention period is even shorter, i.e. four weeks.

The experience gained thanks to this German law should be the starting point for serious reflection on the subject. It is necessary to take into account the fact that data retention is an extremely sensitive issue and that privacy is a right to be protected to the highest degree. However, this right must be balanced with security and other relevant rights, such as the right of defence.

IV. Searching for a Balance Between Retention Period of IP Address and Fundamental Rights

The Treaty of Lisbon[26] enhances the protection of the right of privacy in many respects. First of all, Article 6 of said treaty provides that the Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union (CFR), which assumes the same legal value as the Treaties. In particular, with the Treaty of Lisbon also Article 7 CFR (Respect for private and family life) and Article 8 CFR (Protection of personal data) reached a stronger meaning. Moreover, the protection of data is dealt in Article 16 of the Treaty on the Functioning of the European Union (TFEU), which provides that "Everyone has the right to the protection of personal data concerning them".

The directive on data protection in the police and justice sectors[27] emphasises the inescapable significance of the protection of personal data in these sectors as well. Moreover, such a directive states that an adequate regulation of the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties contributes to the accomplishment of an area of freedom, security and justice[28]. The fact that the directive seeks to ensure some protection of personal data in the case of data processing for the purpose of prevention and repression of crimes appears appreciable. This is because it is possible to state that "The biggest threat to individual freedom and dignity stems from the excessive informational power of certain companies, or controllers, and the wider, incompressible ecosystem of trackers, profilers and targeters that are able to gather and use this information"[29].

In light of the above, the basic problem is to answer the question: What could be an IP address retention period that guarantees both the protection of personal data as well as that of other needs, in particular, that of security?

In order to answer the question, the author of this article conducted two analyses at the European level.

---

[26] See E. De Busser (2014). European initiatives concerning the use of IT in criminal procedure and data protection. *International Review of Penal Law,* p. 115-116.

[27] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. See S. Signorato, S. (2017). The contribution of Directive UE 2016/680 in the implementation of an area of freedom, security and Justice: potential and challenges. International Criminal Law Association (Ed.), *Principi vladavine prava,* Tara: Intermex, p. 417-428.

[28] Directive (EU) 2016/680, recital 2.

[29] European Data Protection Supervisor (2018). Annual Report 2018, p. 8.

a) First of all, the regulation on the retention of IP addresses of each Member State was examined. This analysis showed that retention periods are extremely different between countries and are often too short (e.g. six, twelve, eighteen months). This fact causes many difficulties in those cases where it is necessary to carry out the collection of the IP address in states different from the one carrying out the investigations. It often happens that the State that receives the IP address request has already deleted it on the basis of its own data retention rules.

b) Moreover, the period of time which typically passed between the commission of the crime and the request for IP addresses by investigators was examined. This study showed that IP addresses are often required even after some years from the commission of the crime.

On the basis of this research it emerged that the retention period of the IP address compatible with investigative needs is somewhere in the range between six and ten years. The useful standard for data retention determined by the analysis is very long and, therefore, could cause a significant violation of the right to the protection of personal data.

For this reason, a further analysis was carried out. In particular, it was assessed whether the need to request the IP address after many years following the commission of the crime was related to the crime itself or due to other factors. In this way, it was discovered that, in many cases, such dilated times were due to investigative dysfunctions (e.g. reduced investigator staff, difficulties in coordination between investigators, difficulties in investigative cooperation between States, inadequate legal framework, lack of funds to meet investigative needs) However, it is important to emphasize that the retention period cannot be adapted to investigative dysfunctions. Instead, the investigative dysfunctions must be eliminated or at least reduced, taking into account the laws on data retention.

On the basis of the results of these analyses, it is proposed that the retention period of IP addresses be at least three years or, preferably, four years. This standard seems able to balance the various fundamental rights without compromising the outcome of possible future investigations.

V. Conclusions

The sexual abuse and the sexual exploitation of children, which include child pornography, are very serious crimes, often transnational, that cause enormous suffering to the victims. Furthermore, they also violate the United Nations Convention on the Rights of the Child. This Convention provides, on the one hand, the rights of children to the protection and care necessary for their well-being and, on the other, that the States Parties take the necessary measures to protect children from all forms of sexual exploitation and sexual abuse. These crimes must therefore be combated to the highest degree. At present, however, the effectiveness of investigations is often weakened by certain legal obstacles.

Since these crimes generally cross the borders of single States, as well as those of the European Union, their effective prevention and combat require international rules. In the absence of such rules, it is necessary at least to introduce as soon as possible a legal act of the European Union that allows a rapid collection of evidence between Member States, adequate to guarantee the integrity of evidence and its admissibility in

a Criminal Trial. In addition, new rules on IP address retention are urgently required. This is because the IP address can be a very important evidence in combating these crimes.

However, the drafting of a new regulation regarding IP addresses is complex because the corresponding retention of data, which is necessary for the prevention and the fight against crime, causes a violation of fundamental rights. In order to establish a retention period that respects both investigative needs and fundamental rights, the law on data retention and the investigative practices of each Member State were analysed. The ideal benchmark seems to be reached with a retention period of IP addresses of three or, better still, four years.

Finally, it would be appropriate the introduction of a legal act of the EU aimed at regulating not only IP address retention, but also data retention in general, providing a specific retention period for each type of data. This is because an effective fight against crime can only be achieved through the existence of adequate legislation, common to all Member States, on data retention. For this reason, the European legislature should intervene in this matter with a regulation and not with a directive[30].

References

1. Anderson, P.; Zuo, Z.; Yang, L.; Qu, Y. (2019). An Intelligent Online Grooming Detection System Using AI Technologies. Paper presented at 2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), New Orleans, United States.

2. Bachmaier Winter, L. (2015). Towards the transposition of directive 2014/41 regarding the european investigation order in Criminal Matters. *Eucrim*, p. 47-60.

3. Banday M.T; Mathangi R.A. (2015). Control of IP Address Spoofing – A Comparative Study of IPv4 and IPv6 Networks. Mohammad Tariq Banday (Ed.), *Proceedings of 2015 International Conference on Advances in Computers, Communication, and Electronic Engineering,* Hazratbal, Srinagar: University of Kashmir, p. 344-351.

4. Council of the European Union (6 November 2017), Data retention regimes in Europe in light of the CJEU ruling of 21 December 2016 in Joined Cases C-203/15 and C-698/15 – Report.

5. Daniele, M. (2015). Evidence Gathering in the Realm of the European Investigation Order: From National Rules to Global Principles. *New Journal of European Criminal Law*, p. 179-194.

6. Davidson, J. (1988). An Introduction to TCP/IP, New York: Springer.

7. De Busser, E. (2014). European initiatives concerning the use of IT in criminal procedure and data protection. *International Review of Penal Law*, pp. 115-116.

8. De Hert P., Papakonstantinou V. (2019). Data Protection and the EPPO. *New Journal of European Criminal Law,* v. 10, p. 34-43.

9. European Data Protection Supervisor (2018). Annual Report 2018, p. 8

10. European Union Agency for Fundamental Rights (FRA) (2017). Fundamental Rights Report 2017, chapter 6 Information society, privacy and data protection, p. 155 – 172.

11. European Union Agency for Network and Information Security (ENISA) (November 2018). Cooperation between CSIRTs and Law Enforcement: interaction with the Judiciary, p. 21-22.

[30] A directive is a legislative act that sets out a goal that all EU countries must achieve. A regulation is a binding legislative act. See R.E. Kostoris (2018). European Law and Criminal Justice. R.E. Kostoris (Ed.), *Handbook of European Criminal Procedure*. Berlin: Springer, p. 25 ff.

12. Fortino, G.; Trunfio P. (2014). Internet of Things Based on Smart Objects. Berlino: Springer 2014.

13. ICANN (2011). Beginner's Guide to Internet Protocol (IP) Addresses, p. 5.

14. Kostoris, R.E. (2018). European Law and Criminal Justice. Kostoris, R.E. (Ed.), *Handbook of European Criminal Procedure.* Berlin: Springer, p. 25 ff.

15. Mangiaracina A. (2014). A New and Controversial Scenario in the Gathering of Evidence at the European Level: The Proposal for a Directive on the European Investigation Order. *Utrecht Law Review,* p. 113-133.

16. McAlinden, A.-M. (2012). 'Grooming' and the Sexual Abuse of Children: Institutional, Internet and Familial Dimensions, 1st ed. Oxford: Oxford University Press.

17. Ost, S. (2009). Child pornography and sexual grooming: legal and societal responses. Cambridge: Cambridge University press.

18. Meter (2018). Annual Report. Pedophilia and child pornography, p. 17.

19. Pace, J. (2017). Exchange Relations on the Dark Web. *Critical Studies in Media Communication*, 34(1), p. 1-13.

20. Signorato, S. (2017). Types and features of cyber investigations in a globalized world. Paşca, V., Ciopec, F. (Eds), *Probleme actuale în dreptul penal european*: Universul Juricidic, p. 60.

21. Signorato, S. (2017). The contribution of Directive UE 2016/680 in the implementation of an area of freedom, security and Justice: potential and challenges. International Criminal Law Association (Ed.), *Principi vladavine prava*, Tara: Intermex, p. 417-428.

22. Torretta P.; Bonucchi C.; Cotroneo M.; D'Amato E. (2016) White paper on child sex offenders. Treatment and diagnostic profile of online sex offenders to the detriment of minors for the prevention of and fight against this phenomenon (CSE Project HOME/2012/ISEC/AG/4000004373, Co-funded by Prevention of and Fight against Crime Programme of the European Union), p. 10-25.

23. Warren, S.D., Brandeis L.D. (1890). The Right to Privacy. Harvard Law Review, 4, p. 193.