ISSN 2029-1701
ISSN 2335-2035 (Online)

Mokslinių straipsnių rinkinys
VISUOMENĖS SAUGUMAS IR VIEŠOJI TVARKA
PUBLIC SECURITY AND PUBLIC ORDER
2018 (21)
Scientific articles

POLICY OF EUROPEAN UNION ON THE SAFETY OF CHILDREN IN CYBER SPACE

Aurelija Pūraitė[1]

[1] *Mykolas Romeris university Academy of Public Security Department of Law*
V. Putvinskio 70, LT-44211 Kaunas, Lithuania
Telephone (+370 37) 303655
E.mail: aurelija.puraite@gmail.com

Natalja Prokofjeva [2]

[2]*State Police of the Republic of Latvia*
Ciekurkalna 1st line 1, k – 4, LV – 1026 Riga, Latvia
Telephone 67829456
E.mail:natalija.prokofjeva@vp.gov.lv

DOI: 10.13165/PSPO-18-21-09

Summary. The usage of Internet by children is increasing, both with regard to the number of children going online and time spent on Internet, as well as it became a dominant and primary channel through which they communicate with one another. It is obvious, that ICTs can open a door to a better future for children, offering greater access to learning, interests contents and other benefits that can help them fulfil their potential, but in addition to that, the expansion of availability and accessibility of ICTs has also created a number of threats to person's and especially to children's safety, who are particularly vulnerable to ICT-facilitated crimes or cybercrimes.[1] While increased and more frequent usage of ICTs entails a heightened risk of infringements on privacy and safety for all users, children are at particular risk, as they often do not fully understand the threats associated with these technologies, especially when it comes to sharing of personal information, photos or videos. Each EU country has own law system based on its historical and cultural aspects, but cybersecurity is equally important for all of them. It proves the fact that cybercrimes were recognized as one of the EU Policy Cycle's priorities and a special role in this list belongs to improving the safety of children online. The main aim of this priority is combating child sexual abuse (CSA) and child sexual exploitation (CSE), including the production and dissemination of CSAM and CSEM. The aim of the article is to identify main threats to children's safety in cyberspace and to evaluate the EU's normative acts which put an order in this problem for promoting the understanding of the EU security policy and to evaluate opportunities of cyberspace improvement for children's safety. To achieve the mentioned aim, further tasks are settled: to analyze ICT solutions, international legal acts, and tools, which provide the opportunity for the EU's police organizations to enhance the possibility to detect, investigate and prevent CSA and CSE in cyberspace; to provide recommendations for improving methods of detection, investigation and prevention of CSA and CSE in cyberspace; to reveal what can be improved in the field of international police cooperation in order to ensure successful detection and investigation of CSA and CSE in cyberspace.

Keywords: cybercrimes, child exploitation, legal regulation of cyber space

[1] UNICEF, "*Child Safety Online. Global challenges and strategies*", United Nations Children's Fund (UNICEF), 2011, p. 3;

INTRODUCTION

Fast-paced technological innovation as well as widespread and increasing accessibility of information and communication technologies (ICTs), including high-speed Internet and smart devices have transformed societies around the world.[2] An open and free cyberspace has broken down barriers between countries, communities and citizens, allowing interaction and sharing of information and ideas cross-border. This process can be compared with unstoppable force, touching virtually every sphere of modern life, from economies to societies and shaping everyday life. There is no wonder, childhood is not exception in this process. When children enter the world, they are steeped in a steady stream of digital communication and connection from the way their medical care is managed and delivered to the online pictures of their first precious moments. As children grow, the capacity of digitalization to shape their life experiences grows with them, offering seemingly limitless opportunities to learn and to socialize, to be counted and to be heard.[3]

The usage of Internet by children is increasing, both with regard to the number of children going online and time spent on Internet[4], as well as it became a dominant and primary channel through which they communicate with one another.[5] It is obvious, that ICTs can open a door to a better future for children, offering greater access to learning, interests contents and other benefits that can help them fulfil their potential, but in addition to that, the expansion of availability and accessibility of ICTs has also created a number of threats to person's and especially to children's safety, who are particularly vulnerable to ICT-facilitated crimes or cybercrimes.[6] While increased and more frequent usage of ICTs entails a heightened risk of infringements on privacy and safety for all users, children are at particular risk, as they often do not fully understand the threats associated with these technologies, especially when it comes to sharing of personal information, photos or videos.[7]

The modern world is no longer possible and imaginable without new technologies and global networks that is why governments across the World should work on coherent

[2] CEOP, "*Threat Assessment of Child Exploitation and Sexual Exploitation and Abuse*", Child Exploitation and Online Protection Centre, 2013;
[3] UNICEF, "*The State of the World's Children. Children In a Digital World*", UNICEF Division of Communication, 2017 ; ITU, "*Use of Information and Communication Technology by the World's Children and Youth*", International Telecommunication Unit, 2008;
[4] UNICEF, 2011, *op.cit*., p. 4;
[5] Hinduja, S., Patchin, J.W., "*Bullying beyond the schoolyard: Preventing and responding to cyberbullying*", Cyberbullying Research Center, 2009;
[6] UNICEF, 2011, *Ibid*;
[7] *Ibid*, p.5;

understanding of cybersecurity policy and to consider cyberspace as an increasingly important international issue with unlimited opportunities not only for adults, but also for children. It is also a great challenge and responsibility for policy makers, police and public organizations as well as teachers and parents to encourage children to take advantages of Internet ensuring that they are aware of dangers, which they can meet in cyberspace.

Each EU country has own law system based on its historical and cultural aspects, but cybersecurity is equally important for all of them. It proves the fact that cybercrimes were recognized as one of the EU Policy Cycle's priorities and a special role in this list belongs to improving the safety of children online. The main aim of this priority is combating child sexual abuse (CSA) and child sexual exploitation (CSE), including the production and dissemination of CSAM and CSEM[8]. While neither offline nor online CSE or CSA meet the criteria to be considered "organized crime" this is still a high priority crime due to the degree of physical and psychological damage to one of society's most vulnerable groups – children.

Taking into the consideration before mentioned facts, it is possible to conclude that the concept of children's safety in cyberspace is actual for all the EU countries, and as far as this concept has the tendency for development, for promoting deep and coherent understanding of this phenomenon, it is vitally important to continue to conduct researches into this field.

Previous studies in the field of children's safety in cyberspace (Açar, 2017[9]; Cohen-Almagor, 2015[10]; Leary, 2009[11]; Livingstone & Smith, 2014[12]; UNICEF, 2011; UNODC[13], 2015; UNICEF 2017) mostly payed the attention to the dynamics of children's use of the internet, effects of new ICT on CSE or CSA, the main treats, victim's and offender's psychological aspects as well as international legislation in this field. In the same time, it was

[8] European Commission, "*Resilience, Deterrence and Defense: Building strong cybersecurity in Europe*", 2017 ;
[9] Açar, Y., et al., „*Security Developer Studies with GitHub Users: Exploring a Convenience Sample*", Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017), USENIX Association, 2017;
[10] Cohen-Almagor, R."*Confronting the Internet's Dark Side: Moral and Social Responsibility on the Free Highway*", Woodrow Wilson Center Press and Cambridge University Press, 2015. DOI: 10.1017/CBO9781316226391.
[11] Leary, M. G. „*Sexting or Self-Produced Child-Pornography-The DialogContinues-Structured Prosecutorial Discretion within a Multidisciplinary Response*". // Va. J. Soc. Pol'y & L., Vol. 17, p. 486. Available from: https://www.researchgate.net/publication/313201734_Sexual_Extortion_of_Children_in_Cyberspace [accessed Nov 17, 2018].
[12] Livingstone, S., & Smith, P. K. „*Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age*".// Journal of child psychology and psychiatry, Vol. 55(6), pp. 635-654. Available from: https://www.researchgate.net/publication/313201734_Sexual_Extortion_of_Children_in_Cyberspace [accessed Nov 17, 2018].
[13] United Nations Office on Drug and Crime. „*Operation Strikeback*". Available from http://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/phl/operation_strikeback.html. [accessed Nov 17, 2018].

identified that there is not enough information about tools, which provide the possibility to collect the pieces of evidence, organize undercover operations as well as there is not a clear vision of mechanisms of international cooperation.

The aim of the article is to identify main threats to children's safety in cyberspace and to evaluate the EU's normative acts which put an order in this problem for promoting the understanding of the EU security policy and to evaluate opportunities of cyberspace improvement for children's safety. To achieve the mentioned aim, further **tasks** are settled: to analyze ICT solutions, international legal acts, and tools, which provide the opportunity for the EU's police organizations to enhance the possibility to detect, investigate and prevent CSA and CSE in cyberspace; to provide recommendations for improving methods of detection, investigation and prevention of CSA and CSE in cyberspace; to reveal what can be improved in the field of international police cooperation in order to ensure successful detection and investigation of CSA and CSE in cyberspace.

The object of the research is the concept of children's safety in cyberspace provided in legal regulation of the EU level.

Methodology. To achieve aforementioned purpose in this essay were applied theoretical (description, analysis, comparison, induction, deduction) and empirical research methods.

THE WIDESPREAD OF INFORMATION AND COMMUNICATION TECHNOLOGIES AS A THREAT TO CHILDREN'S SAFETY

Social networks and messengers have opened up our lives and homes to virtual strangers who can pretend to be anyone, any age or sex. They can talk to children in complete secrecy, even entice a child to meet in person, which could lead to a risk of abuse. Throughout cyberspace, pedophiles and bullies can find victims now without leaving their physical security space at a little risk of being caught. Children may not feel any threat by "talking" to someone online, and after a few weeks or months of communication, they are not strangers anymore. In the same time, the widespread use of ICTs and the immediacy of online interactions can lead perpetrators to engage in a direct contact with victims or targeting them, to the point that they may solicit sexual contact after only a few brief interactions, unconcerned about offending or alienating victims, or resorting to threatening them into compliance.[14] For example, perpetrators

[14] Choo, K.-K.R., "*Responding to online child sexual grooming: An industry perspective*", Australian Institute of Criminology, No. 379, 2009. Available from https://aic.gov.au/publications/tandi/tandi379 [accessed Nov 17, 2018];

may convince children to share a compromising image and then threaten to send it to their parents or to upload it to a public website in order to extort more graphic content or in-person meetings.[15]

It must be taken into consideration that ICTs also enable perpetrators to have increased access to information about victims, because children through social networks freely share personal and biographical information, they often don't care about discretion and rely on a false sense of privacy and safety. Some of them don't even know that new features in social networking-sites such as geotagging of images and "checking-in" to places via mobile devices can further enhance offenders' knowledge of their location.[16] There are also some services and applications which make it easier for offenders to gather personal information about their prospective victims. For example, the "cree.py tool" extracts information associated with a single e-mail address from diverse social networking sites, providing the user with a dossier of information on potential victims, including geolocation data when available.[17]

ICTs also contribute greatly to the implementation of a large range of cybercrime affecting child safety[18], by expanding the territorial range and ways how it could be done. For example, sexual abuse material might be both recorded and distributed solely using smart devices. Similarly, by using ICTs, cyberstalkers, harassers and bullies can abuse their victims with less effort and lower risk of detection. Child sex tourists can make use of cloud computing to store images or videos of their encounters, avoiding the risks associated with physically transporting child sexual abuse material. Moreover, mobile telephone technology connects organizers, victims and consumers of child sexual exploitation and abuse, thus reducing the need for producers and distributors to be physically present at transactions, which in turn serves to better insulate them from detection.[19]

Many offenders now use both local and remote storage services that include built-in encryption technology to evade detection and complicate the work of law enforcement agencies. Providers and consumers of child sexual abuse material may also have access to new technologies that reduce permanent digital evidence. Applications such as "SnapChat" and

[15] CEOP, 2013, *Op.cit.*;
[16] Livingstone, S., Ólafsson, K., & Staksrud, E. *Social networking, age and privacy. EU Kids Online*, London, UK. Available from http://eprints.lse.ac.uk/35849/1/Social%20networking%2C%20age%20and%20privacy%20%28LSERO.pdf. [accessed Nov 17, 2018].
[17] *Ibid*;
[18] UNICEF, 2017, *Op. Cit*., p.81;
[19] Koops, T.U, et al., „*Child sex tourism – prevalence of and risk factors for its use in a German community sample*"// BMC Public Health, Vol. 17, 2017, DOI: 10.1186/s12889-017-4270-3;

"Wickr", for example, enable users to distribute temporary images that disappear within seconds following receipt.[20]

The magnitude and pervasiveness of bullying have also been exacerbated in the current technological environment. Bullies use websites and social media to broaden their audience and to increase their impact on victims. Use of the Internet and other ICT platforms enables perpetrators to quickly and easily enlist others to join in bullying activities.[21]

The use of ICTs affords unprecedented provision of social affirmation for offenders. Readily available child sexual abuse material online may create the false impression of social acceptability. Online communities can also provide forums for sharing strategies to gain access to victims and to evade law enforcement.[22]

It is obvious, that children are at particular risk as they often do not fully understand threats associated with the use of ICTs, or are not sufficiently aware of that, once shared, control over such material is effectively waived, and, if we evaluate the peculiarities of this stage of development, coupled with the lack of personal experience, it becomes clear why children so often suffer from cyber threats such as child sexual abuse material (child pornography) production; commercial sexual exploitation of children; cyber-enticement, solicitation and grooming; cyberbullying, cyber-harassment and cyberstalking, as well as exposure to harmful content and sexting. Unfortunately even very young children are increasingly victimized in child sexual abuse material and child sex trafficking and exploitation, but adolescents face the highest risk of cyber-enticement, exposure to harmful material and cyberbullying.[23]

Based on the researches on children's security in cyberspace[24], it is clear that cybercrimes threatens children regardless of location, gender and age, and the threat that was previously not

[20] Henn, S., „*Teens Dig Digital Privacy if SnapChat is any Indication*", 2013, Available from https://www.npr.org/sections/alltechconsidered/2013/12/10/249731334/teens-dig-digital-privacy-if-snapchat-is-any-indication?t=1542444936090 [accessed Nov 17, 2018].

[21] Shariff, S. „*Child Safety Online. Defining the Lines on Cyberbullying: Navigating a Balance Between Child Protection, Privacy, Autonomy and Informed Policy*", UNICEF, 2013. Available from https://www.unicef-irc.org/article/839-defining-the-lines-on-cyberbullying-navigating-a-balance-between-child-protection.html [accessed Nov 17, 2018];

[22] Choo, K.-K.R., 2009, *Op.cit.*;

[23] IWF, "*Annual report. 2014*", Internet Watch Foundation, 2014, p. 11. Available from https://www.iwf.org.uk/sites/default/files/reports/2016-02/IWF%202014%20Annual%20Report%20%28web%29.pdf [accessed Nov 17, 2018]; The Berkman Center for Internet & Society at Harvard University, 2008 "Child Safety & Online Technologies";

[24] Choo, K.-K.R., 2009, *Op.cit.*; Cooper, S. „Medical Analysis of Child Pornography". In Cooper, S. et al. „*Medical, legal and social science aspects of child sexual exploitation—a comprehensive review of pornography, prostitution and internet crime*". GW Medical Publishing Inc., 2005; Department of State, "*Trafficking in Persons Report. 2018*", Department of State of the United States of America, 2018. Available from https://www.state.gov/documents/organization/282798.pdf [accessed Nov 17, 2018]; Ringrose, J. et al. „*A qualitative study of children, young people and 'sexting'. A report prepared for the NSPCC*", NCPCC, 2012.

so widely available to children, is currently only one click away. The prevalence of child sexual abuse material may also fuel a vicious cycle[25]. If it was previously thought that the home is like a fortress where the child is protected from the outside's world influence, then the home can now be compared to a park with a lot of secret places and where strangers walk freely.

Analysis on children's hazards in cyberspace identified that not all forms of ICT-facilitated child abuse and exploitation fundamentally diverge from those that are not ICTs. In many cases, ICTs only serve to facilitate already-known types of crimes and forms of criminality as it involves the same dynamics, patterns and structures.[26] On the other hand, new ICTs have also given rise to some new forms of crimes such as made-to-order child sexual abuse material, user-generated content, self-generated content, including "sexting" and broadcasting of live sex abuse, that are enabled exclusively through the use of ICTs. The EU offers three categories to explain forms of behavior related to ICT-facilitated child abuse and exploitation.[27]

Internet is difficult to control as it is not governed by anyone and it does not respect any boundaries. In the same time, complex nature of cybercrime, as one that takes place in the borderless realm, is compounded by the increasing involvement of organized crime groups. Cybercrime perpetrators and their victims, are often located in different regions, and its effects ripple through societies around the world. This highlights the need to mount an urgent, dynamic and international response.[28]

Available from https://www.researchgate.net/publication/311806257_A_qualitative_study_of_children_young_people_and_'sexting'_English [accessed Nov 17, 2018]; Cross-Tab Marketing Services & Telecommunications Research Group for Microsoft Corporation,"*Online Bullying Among Youth 8-17 Years Old – Worldwide. Executive Summary*", 2012. Available from http://download.microsoft.com/download/e/8/4/e84beeab-7b92-4cf8-b5c7-7cc20d92b4f9/ww%20online%20bullying%20survey%20-%20executive%20summary%20-%20ww_final.pdf. [accessed Nov 17, 2018]; Ybarra, M.L., Mitchell, K.J. "Exposure to Internet Pornography among Children and Adolescents: A National Survey"// *Cyberpsychology & Behavior*, Vol.8, No.5, 2005. Available from https://pdfs.semanticscholar.org/6111/5e99668a9f2b9da2db0ee5c066c1117a156b.pdf. [accessed Nov 18, 2018]; OECD, „*The Protection of Children Online. Risks Faced by Children Online and Policies to Protect them*", OECD, 2012. Available from https://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf. [accessed Nov 18, 2018].

[25] Howitt, D., Sheldon, K. "The Role of Cognitive Distortions in Paedophilic Offending: Internet and Contact Offenders Compared"// *Psychology Crime and Law*, 13(5), 2007, pp. 469-486.

[26] UNICEF, 2011, *Op.cit.*;

[27] Livingstone et al., 2009, *Op.cit.*, p.10;

[28] UNODC, "*Global Programme on Cybercrime*", UNODC, 2016. Available from https://www.unodc.org/ropan/en/IndexArticles/unodc-global-programme-on-cybercrime-participates-in-safer-internet-day-commemoration-in-el-salvador.html [accessed Nov 18, 2018].

The Council of Europe notes, for example, that: "[n]one of these new technologies are in and of themselves harmful" but they-inadvertently-provide criminals with "new, efficient, and often anonymous" ways and means of exploiting children.[29]

THE EU POLICY ON THE SAFETY OF CYBERSPACE FOR CHILDREN

The EU Agenda for the Rights of the Child [30] underlined, the long-term effects of not investing enough in policies affecting children may have a profound impact on our societies. Whereas the Digital Agenda for Europe [31] aims to have every European digital, children have particular needs and vulnerabilities on the Internet, which must be addressed specifically so that the Internet becomes a place of opportunities for children to access knowledge, to communicate, to develop their skills and to improve their job perspectives and employability.[32] In the same time, together with the digitalization, cybercrimes against children become a huge and global issue as advances in ICTs are giving new way for perpetrators to find their victims. The phenomenon will continue to be a threat for today's children until there will be taken measures by policy makers, police officers, teachers and parents to restrict, educate and be aware against them.

It has been recognized internationally that children as the bearers of rights, and as deserving respect and special protection. Which imply their protection from cybercrimes and engagement of international cooperation stakeholders for investigation and prosecution of such cases.[33] However, the international cooperation and investigation process usually undermined by stakeholders ratification status or by degree, which international measures incorporated into national law. The EU has developed concepts, strategies, normative acts and ordinances aimed at streamlining a cyber security policy, while at the same time it is possible to describe the EU's cybersecurity policy in action as a jazz band, not a classical orchestra: musicians from different states, with different abilities and instruments participating in a permanent jam session, with a basic tune and a general idea of the kind of music they want to produce … a band which finds

[29] Huges, D.,"*The Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation*", European Commission, 2003.
[30] Communication From The Commission To The European Parliament, The Council, The European Social Committee And The Committee Of The Regions, „*An EU Agenda for the Rights of the Child*", COM/2011/0060.
[31] Communication From The Commission To The European Parliament, The Council, The European Social Committee And The Committee Of The Regions, „*A Digital Agenda for Europe*", COM/2010/245.
[32] Husing, T., et al. "Trends and Forecasts for the European ICT Professional and Digital Leadership Labour Markets (2015-2020)"// *Empirica Schriftenreihe*, Nr. 2, 2016. Available at https://www.empirica.com/fileadmin/publikationenseries/documents/Schriftenreihe_2016_Nr_02_eSkills_eLeadership_Skills_Figures_and_Forecasts.pdf [accessed Nov 18, 2018].
[33] UNODC, "*Comprehensive Study on Cybercrime*", 2013, pp. 100-104. Available from https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [accessed Nov 18, 2018];

it hard to agree on a specific arrangement, but which can eventually sound harmonious – though not necessarily completely homogeneous.[34]

That is a fairly good description of the EU Member States' overall performance as an actors on the global arena of cybersecurity because there is variation how countries address cybercrimes against children. Some countries criminalize acts of child sexual abuse material production, but could have a different definition of a "child". While other countries rely on general criminal laws against abuse and exploitation and enacted laws that are specific to the commission of child exploitation offences using ICTs. As noted in the Comprehensive Study on Cybercrime [35], although 80% of countries in Europe report sufficient criminalization of cybercrime acts, in other regions of the world, up to 60 % of countries report that criminalization of cybercrime acts is insufficient.[36]

It was identified, that in the EU only Spain has specific legal regimes that address online harassment offences, such as cyberstalking, harassment or cyberbullying. With respect to cyberstalking, many countries do not consider voyeurism or invasion of privacy to be criminal offences, particularly when they occur exclusively online. Nearly all countries do, however, criminalize stalking conduct that escalates into kidnapping, threats of violence, or any kind of contact offence. Some states have adopted laws that a communication must evidence a serious expression of an intention to inflict bodily harm as perceived by a reasonable person. Nonetheless, the growth of social networks, as well as recent child suicide cases possibly linked with cyberbullying, have raised new concerns about the expansion of the phenomenon. In this context, it is also an open question concerning the appropriateness of any criminal justice response where the perpetrator is also a minor.

It means that the time has come for the EU to step up its actions in this area and in order to improve the cybersecurity level of the EU, each Member State should be ready to challenges imposed by worldwide and ICT's changes and development. In the same time, the EU has to provide a clear vision in this domain, clarifying Member State's roles and responsibilities and setting out the actions required based on strong and effective protection and promotion of children's rights to make the EU's online environment safe for children.

[34] Lasheras, B., et al. "*European Union Security and Defence White Paper*", 2010. Available from http://library .fes.de/pdf-files/id/ipa/07075.pdf [accessed Nov 18, 2018];
[35] UNODC, 2013. *Op.cit*.
[36] *Ibid*, p. 16.

For promoting a coherent understanding of this problem in Europe, several normative acts were implemented. For example, the Council of Europe Convention on Cybercrime[37] and the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse,[38] which provide wide-ranging set of measures to build strong cybersecurity in Europe. Speaking about the EU level, there can also be meant such legislative acts as Communication on a Cybersecurity Strategy of the EU – An Open, Safe and Secure Cyberspace[39] and Resilience, Deterrence and Defense: Building strong cybersecurity for the EU[40], as well as key regulations concerning the issue: the Strategy of the European Commission on combating cyberbullying[41] and it submits directives concerning legal protection of minors in cyberspace: Directive of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography.[42] The European Strategy for a Better Internet for Children[43] was set out to give the EU children digital skills and tools they need to fully and safely benefit from being online. The strategy proposes a series of actions among which are the goals to create a safe environment for children through age-appropriate privacy settings, wider use of parental controls and age rating and content classification as well as to combat child sexual abuse material online and child sexual exploitation. The strategy brings together the European Commission and Member States with mobile phone operators, handset manufacturers and providers of social networking services to deliver concrete solutions for a better internet for children. The tasks of the strategy are carried out mainly through the

[37] The Council of Europe Convention on Cybercrime No.185, available from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 ;
[38] The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse No. 201, available from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/201;
[39] Joint Communication To The European Parliament, The Council, The European Economic And Social And The Committee Of The Regions „Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace“, 52013JC0001, available from https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:52013JC0001 ;
[40] European Commission, “Resilience, Deterrence and Defense: Building strong cybersecurity in Europe”, 2017, available from https://ec.europa.eu/digital-single-market/en/news/cybersecurity-package-resilience-deterrence-and-defence-building-strong-cybersecurity-eu ;
[41] Council conclusions of 27 November 2008 on a concerted work strategy and practical measures against cybercrime, 2009/C62/05, Official Journal of the European Union, 17/03/09.
[42] Directive of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JH, 2011 (2011/92/UE), OJ L 335, 17.12.2011, available from https://eur-lex.europa.eu/legal-content/EN/TXT /?uri=celex %3A320 11L0093 ;
[43] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions „European Strategy for a Better Internet for Children“, 2012 (2012/0196), available from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2012%3A0196 %3AFIN ;

implementation of the Connecting Europe Facility[44], the instrument for co-funding the digital service infrastructure for making a better internet for children, but also through other programs such as Horizon 2020.

For implementing the EU policy on the safety of cyberspace for children and improving an investigation of children related cybercrimes, there were also implemented special tools and mechanisms for international cooperation such as mutual legal assistance, informal or operational law enforcement cooperation, multi-agency partnerships and information-sharing forums as well as special EU agencies such as ENISA and Europol, which provide recommendations on cybersecurity, support policy development and its implementation, and collaborates with operational teams throughout Europe, or CERT which is responsible for information security incidents and cyber threats investigation in the EU. It was identified that, the EU specialized agencies and law enforcement authorities have a key role in investigation and combating cybercrimes against children, while private sector's support is also needed to take preventive measures.

Dynamic and global environment impose, that the EU must be a modern provider of collective cybersecurity policy, as the Member States cannot face cyber risks and challenges alone.[45] Also on the Member State's level, it is necessary to analyze new phenomena and trends and to develop new methods and strategies of combating cybercrimes in accordance with the EU internal policy, so the Member States must translate their commitments to mutual assistance and solidarity enshrined in the treaties into action.

Finally, it is a pleasure to recognize that the changes of the last ten years in the EU policy on the safety of cyberspace for children have shown that "the instruments are started to be tuned to the same pitch" and the first steps to safe EU's online environment were taken.

CONCLUSIONS

Historically a broad system of internet governance was spread out across a range of entities, including international bodies, national governments, private sector and civil society, but without central coordination, these entities have over time developed the principles, norms, rules, decision-making procedures and programmes. Initially, internet governance focused

[44] European Commission, Connecting Europe Facility, 2013 (1316/2013), available from https://ec.europa.eu/inea/en/connecting-europe-facility ;
[45] European Commission, *Joint Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions "Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace*", 2013, p. 17;

mainly on technical issues and infrastructure, but it gradually expanded to include issues such as cybersecurity, e-commerce, net neutrality, human rights and other issues.

It is estimated that one-third of internet users are children accounts.[46] Currently international and national internet policies fail to take sufficient account of children's distinctive needs and rights. Policies related to cybersecurity and internet openness looked first and foremost at adult user, but it was a big mistake because today's children are digital natives and the internet is their second home.[47] Therefore, policies and regulatory frameworks must catch up with this reality – especially when it comes to protecting children from the worst risks of connectivity, as those who use the internet to exploit and harm children are eager to find loopholes in such regulations. Moreover, the problem is that whereas criminals can quickly invent, implement and adapt to the commission of technology-facilitated crime, policymakers and investigators must undergo the long process of researching, forging consensus and developing legal and investigative responses in order to address newly emerging forms of ICT-facilitated crime.

Despite all the difficulties, it is a great pleasure to recognize that the EU also has made some progress in formulating policies and approaches to eliminate the most egregious online risks to children's safety in cyberspace and there has been significant progress in law enforcement and support for victims, but there still a lot of steps what needs to be done at the levels of policy and governance, criminal justice, international cooperation, societal change, industry engagement and ethical and informed media reporting.

It was identified that making the digital space better and more secure for children requires collaboration and cooperation among governments, EU agencies, police and law enforcement organizations as well as other international children's organizations, civil society, the private sector, academia and the technical community, families and children themselves. Besides international guidelines and agreements, it requires child-focused national policy, coordinated response and sharing of best practice models, scaling up approaches to help law enforcement stay ahead of online offenders, and working with the private sector to develop ethical standards that protect children.

No doubts that efficient cooperation between the EU investigation institutions often depends on at least partial unified definitions of cybercrimes against the children, thus the key

[46] Mascheroni, G., Olafsson, K., "*Net Children Go Mobile: risks and opportunities*", Second Edition. Milano: Educatt, 2014.
[47] *Ibid*, pp. 9-16.

aim remain the works on harmonization and amending legal regulations of the Member States in the area. Constantly appearing new threats in cyberspace oblige to implement additional legal regulations and their unification in all Member States.

There could be identified several opportunities for the EU policy makers to enhance the safety of cyberspace for children. Firstly, governments and national authorities should focus on a fundamental child protection approach that fully respects human rights, in the same time it is necessary to ensure that national laws keeps pace with technological innovation. Secondly, it is vitally important to focus on recruiting, training and maintaining specialized ICTs personnel within law enforcement agencies. Finally, law enforcement structures should gain access to state-of-the-art technological resources, develop effective mechanisms for accessing third party data, and improve the conduct of undercover investigations that are consistent with the rule of law as well as develop policy guidance on children's safety in Internet. The formulation of policies in this area is best based on a multidisciplinary approach that draws on research findings and best practices from social science, legal policy and public policy.

REFERENCES

1. Choo, K. R. (2009). *Responding to online child sexual grooming: An industry perspective Trends and Issues in Crime and Criminal Justice*, 379, 1-6 Australian Institute of Criminology. Available at: http://www.aic.gov.au/publications/current%20series/ tandi /361-380/tandi379.aspx;
2. Chou, C., & Huang, Y.Y. (2010). *An analysis of multiple factors of cyberbullying among students in Taiwan.* Computers in Human Behaviour, 26(6), 1581-1590.
3. Cooper, S. (2005). *Medical analysis of child pornography*. In S. Cooper, A. Giardino, V. Vieth,& N. Kellogg (Eds.), Medical, legal and social science aspects of child sexual exploitation Pp. 213-242. Saint Louis, MO: GW Medical Publishing;
4. Cornell, D.G., & Unnever, J.D. (2004). Middle school victims of bullying: Who reports being bullied? Aggressive Behaviour, 30(5), 373-388;
5. Henn, S. (2013). *Teens Dig Digital Privacy if SnapChat is any Indication*. Available at: http://www.npr.org/blogs/alltechconsidered/2013/12/10/249731334/
6. Hinduja, S., & Patchin, J.W. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. Deviant Behaviour, 29(2), 129-156;
7. Hinduja, S., & Patchin, J. W. (2009). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying.* Thousand Oaks, CA: Sage Publications (Corwin Press);
8. Howitt, D. Sheldon, K. (2007). *The Role of Cognitive Distortions in Paedophilic Offending: Internet and Contact Offenders Compared*, Psychology, Crime, & Law 13:469-486.
9. Hüsing, T., Korte, W. B., Dashja, E. (2015) *Trends and Forecasts for the European ICT Professional and Digital Leadership Labour Markets (2015-2020) empirical Working Paper. Available at:* http://eskills-lead.eu/fileadmin/lead/working_paper_-_supply_demand_forecast_2015_a.pdf
10. Koops, T., Turner, D., Neutze, J., & Briken, P. (2017). *Child sex tourism – prevalence of and risk factors for its use in a German community sample* BMC Public Health. 2017; 17: 344. PMCID: PMC5397735 PMID: 28427370 Published online 2017 Apr 20. doi: 10.1186/s12889-017-4270-3;

11. Li, Q. (2006). *Cyberbullying in schools: A research of gender differences.* School Psychology International, 27(2), 157-170;
12. Li, Q. (2010). *Cyberbullying in high schools: A study of students' behaviours and beliefs about this new phenomenon.* Journal of Aggression, Maltreatment, & Trauma, 19(4), 372-392.
13. Livingstone, S., Haddon, L. (2009). *EU Kids Online: Final Report* P. 16. Available at: http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/EU%20Kids%20I%20(2006-9)/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf
14. Livingstone, S., Olafsson, K., Staksrud, E. (2011). *Social networking, age and privacy. EU Kids Online.* Available at: http:// eprints.lse.ac.uk/35849/1/Social%20 networking%2C%20age%20 and%20privacy%20%28LSERO.pdf;
15. Mascheroni, G & Ólafsson, K. (2014). *Net Children Go Mobile: risks and opportunities*. Second Edition. Milano: Educatt. Available at: http://netchildrengomobile.eu/ncgm/wp-content/uploads/2013/07/DEF_NCGM_SecondEdition_Report.pdf Okazaki & Hiroki, (2001). *Attachment to mobile phones reaching point of addiction*. The Daily Yomiuri, pp. 1-1.
16. Ringrose, J., Gill, R., Livingstone, S., Harvey, L., (2012). *Children, Young People and 'Sexting'. Summary of Qualitative Study*. P. 12. Available at http://www.nspcc.org.uk/ Inform/resourcesforprofessionals/sexualabuse/sexting-researchsummary_wdf89270.pdf
17. Shariff, S. (2011). *Child Safety Online. Defining the Lines on Cyberbullying: Navigating a Balance Between Child Protection, Privacy, Autonomy and Informed Policy*. Available at http://www. unicef-irc.org/research-watch/Child-Safety-Online/839/;
18. Yee, N. (2006) *Motivations for Play in Online Games* CyberPsychology & Behavior 9.6: 772-75. Web. 17 Oct. 2016.
19. Ybarra, M., Mitchell, K., (2005). *Exposure to Internet Pornography among Children and Adolescents: A National Survey*, CyberPsychology and Behaviour 8:473-485;
20. Wolak, J., et al., 2006. Online Victimization of Youth Five Years Later. Available at: http://www.missingkids.com/en_US/ publications/NC167.pdf;

Normative regulation, researches and statistical data

1. Conclusion of the Council (2008) 2009/C62/05 Available at:http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ%3AC%3A2009%3A062%3ATOC;
2. Directive of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography Directive 2011/92/UE Available at:https://ec.europa.eu/anti-trafficking/legislation-and-case-law-eu-legislation-criminal-law/directive-201192eu_en;
3. European Commission (2011) *An EU Agenda for the Rights of the Child* Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM%3A2011%3A0060%3AFIN%3AEN%3A PDF;
4. European Commission (2012) *European Strategy for a Better Internet for Children* Available at: https://ec.europa.eu/digital-single-market/en/news/communication-european-strategy-make-internet-better-place-kids;
5. European Commission (2013) *Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace* Available at: https://ec.europa.eu/digital-single-market/en/news /communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace;
6. European Commission (2014) *The EU explained: Digital agenda for Europe* ISBN 978-92-79-41904-1 doi:10.2775/41229 Available at: http://eige.europa.eu/resources/digital_agenda_en.pdf;
7. European Commission (2017) *Resilience, Deterrence and Defence: Building strong cybersecurity in Europe.* Available at: https://ec.europa.eu/digital-single-market/en/news/resilience-deterrence-and-defence-building-strong-cybersecurity-europe-0;

8. European Parliament (2014) *Guidelines for trans-European networks in the area of telecommunications infrastructure and repealing Decision No 1336/97/EC Text with EEA relevance* Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0283;
9. CEOP (2009). *Strategic Assessment 2008-2009*. Available at: http://ceop. police.uk/ Documents/ strategic_overview_2008-09.pdf
10. CEOP (2013). *Threat Assessment of Child Exploitation and Sexual Exploitation and Abuse*. Paragraph 17 Available at: https://www.norfolklscb.org/wp-content/uploads/2015/03/ CEOP_ Threat- Assessment _CSE_JUN2013.pdf;
11. Council of Europe (2003). *The Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation* [EG-S-NT (2002) 9 rev.]. Available at: http://www.coe.int/t/dghl/monitoring/ trafficking/docs/activities/EGSNT2002-9rev_en.asp.
12. Council of Europe *Convencion on Cybercrimes No.185.* Available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf;
13. Council of Europe *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse No. 201* Available at: https://rm.coe.int/16800d3832
14. Cross-Tab Marketing Services & Telecommunications Research Group for Microsoft Corporation (2012). *Online Bullying Among Youth 8-17 Years Old – Worldwide. Executive Summary.* Available at: http://www.microsoft.com/security/resources/ research.aspx#onlinebullying;
15. Funding Programme Horizon 2020 Available at: http://ec.europa.eu/programmes/horizon2020/;
16. ITU (2008). *Use of Information and Communication Technology by the World's Children and Youth* Available at: https://www.itu.int/pub/D-IND-ICT_YOUTH;
17. IWF (2014). *Annual report* P. 11. Available at: https://www.iwf.org.uk/report/2014-annual-report;
18. The Berkman Center for Internet & Society at Harvard University (2008). *Enhancing Child Safety and Online Technologies* Available at: https://cyber.harvard.edu/sites/cyber.law.harvard.edu /files/ISTTF_Final_Report.pdf
19. OECD (2011). *The Protection of Children Online. Risks Faced by Children Online and Policies to Protect them*. Available at http://www.oecd-ilibrary.org/science-and-technology/ the-protection-of-children-online_5kgcjf71pl28-en.;
20. Online Child Safety *Statistics* Available at: http://www.puresight.com/Pedophiles/Online-Predators/online-predators-statistics.html
21. UNICEF (2011) *Child Safety Online. Global challenges and strategies.* Available at: https://www.unicef-irc.org/publications/pdf/ict_techreport3_eng.pdf;
22. UNICEF (2017) *The State of the World's Children 2017 "Children in a Digital world"* ISBN: 978-92-806-4930-7 Available at: https://www.unicef.org/publications/files/SOWC_2017_ ENG _WEB.pdf;
23. UNODC Global Programme on Cybercrime Available at: https://www.unodc.org/unodc/en/cybercrime /global-programme-cybercrime.html;
24. UNODC (2013). *Comprehensive Study on Cybercrime* Available at: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf;
25. U.S. Department of State (2008). *Trafficking in Persons Report.* P. 9. Available at: http://www.state.gov/documents/organization/105501.pdf.

Table of abbreviations

CEOP- Child Exploitation and Online Protection Centre
CERT-EU- the Computer Emergency Response Team for the EU Institutions, bodies and agencies
ENISA- the EU cybersecurity agency

EU- European Union
ICT- Information and communication technology
ITU- International Telecommunications Union
IWF- Internet Watch Foundation
NGO- Non-governmental organization
NSPCC- National Society for the Prevention of Cruelty to Children
OECD- Organization for Economic Co-operation and Development
UNICEF- United Nations Children's Fund
UNODC- United Nations Office on Drugs and Crime

Aurelija Pūraitė[1], PhD, Associate Professor at Academy of Public Security of Mykolas Romeris university. Research Fields: international public law, human rights, public security.

Natalja Prokofjeva[2]**,** Deputy Head of the Information Bureau of the Central Criminal Police Department of the State Police of Latvia, master student of CEPOL European Joint Master Programme „Policing in Europe". Research Fields: cyver security, criminal law, police cooperation in the EU.