

Protecting minors from Internet threats. Legal instruments or alternative measures?

ABSTRACT

Article about protection of minors from Internet threats provides a review of main questions within this problematic aspects. It focuses on issue concerning a dilemma of a choice the adequate way of safeguard their security in a new – determined by a stride of new communication technologies – environment. First, some basic definitions pertaining a legal perspective of the audiovisual media services and other Internet audiovisual services has been mentioned; as well as a description of notion of minors and their development, which is the particular subject of the protection. Then it is important to point out the different status of a child as a receiver of AMS and as a user of Internet and its implications to the scope and characteristics of the threats. Regarding a growing impact of Internet on children, from the criminological point of view, the threats should be divided into traditional and new risks. Relating to the basic premises of chosen legal and/or alternative methods of protection of minors, especially European soft and hard law and OECD recommendations have to be questioned. The core of the opportunity to solve the escalating problem of the protection of minors in Internet is to combine legal instruments and other methods in adequate way, taking into consideration the needed level of regulation and cooperation (international, domestic), technical criteria as well as kind and seriousness of threats.

Keywords: minors, internet threats, safety, legal instruments, alternative measures

1. Introduction

The issue of a protection of minors from Internet threats is aimed at a presentation of changing picture of them as well as at dilemma of a choice the adequate, effective way of safeguard their security in a new technical, social and cultural environment. Regarding the wide sphere of on-line rapidly growing services it is to be mentioned that due to the changing paradigm of communication (see: Potter W. J., Cooper R., Dupagne M, 1993, pp. 317–321), three forms of it: interpersonal, mass and mass self-one coexist and complement each other within the “composite, interactive, digital hypertext” (M. Castels, 2009, p. 55). The heading problem is going to be more and more complex as it has been ‘located’ in a multi-dimension milieu, determined by a ‘myriad’ of flexible factors, where reciprocal overlap of personal and mass level of communication has occurred.

In particular it is tough to categorize certain services as audiovisual media services (AMS) or other Internet ones, within the wide, diversified and permanently growing spectrum of them, all the more that indeed digital media are located between interpersonal and traditional mass communication. The classification is fundamental insofar as they have subjected to the different legal regimes. Thus, the considerations should be preceded by introducing, some basic notions pertaining a regulative perspective of them. The online environment concerns both audiovisual services within the meaning of art. 1.1. of a directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 *on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive)* and other on-line audiovisual services even though they do not fulfill criteria of mass media.

Audiovisual media services (AMS) are defined by art. 56–57 of the *Treaty on the Functioning of the European Union*; they within are under editorial responsibility of a media service provider, with a principal purpose to provide programs in order to inform, educate and entertain to the general public by electronic communications networks (art. 2 of directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 *on a common regulatory framework for electronic communications networks and services – Framework Directive*). Directive 2010/13/EU encompasses linear

(television broadcast – art. 1.1 (e)) and non-linear (on – demand – art. 1.1 (g)) services (programs and audiovisual commercial communications).

Besides, in a global area network which connects computer systems (as well as, used mainly by young people, mobile devices like tablets and smartphones) across the world a lot of – sometimes difficult to unambiguous classification of their private, semi-private or public character – services have been appearing, e.g. social media, online gaming etc. (see especially: Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states *on a new notion of media*, Proposal for a Directive of the European Parliament and of the Council *amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities*, Brussels, 25.5.2016). In such cases general, in principle internal law provisions are applied. This, some kind of smoothness, ambiguity and permanent development of AMS and other Internet services evokes problems in setting up common European framework, regulatory provisions concerning the systemic aspects of children protection.

Regarding the notion of minors, according to the art. 1 of the *Convention on the Rights of the Child* of 20 November 1989, it encompasses every human being below the age of eighteen years (which is a threshold for different legal and systemic regimes). The need for a guarantee them security and safeness in Internet environment required a special attention and should be in core of all considerations relating to the problem, bearing in mind differences of particular age groups (generally children and youth, also referred to as minors or kids and adolescents, teenagers, young people)¹, varieties of solutions across countries and contexts. Because of their immaturity they ought to be protected from any interference with their spiritual, moral and social well-being, including physical and mental health (see: Dodge R., Daly A., Huyton J., Sanders L.D., 2012, pp. 222–235; *Media and the Well-Being of Children and Adolescents*, Jordan A. B., Romer D. eds., 2014). Their normal development, including appropriate socialization is the subject of a protection in – playing the important function in it – audiovisual media sector.

¹ The terms: ‘children’, ‘children and youth’ and ‘minors’ are used interchangeably in this article.

2. Internet threats` review

Contemporary: “our societies are increasingly structured around the bipolar opposition of the Net and the Self” (M. Castels, 1996, p. 3). The Net is based on the pervasive use of networked communication media, when Self is the way of reaffirming, reconfiguring peoples` identities under the structural, especially technological and cultural change conditions, which is in the contrast to their primary (biologically) forms (M. Castels, 1996, p. 5, *idem*, 1997, p. 6). Internet constitutes a timeless and placeless space of flows, introducing a real virtuality culture: “(...) the informational paradigm and the network society, induce systemic perturbation in the sequential order of phenomena performed in that context” (M. Castels, 1996, p. 464). In the ‘Information Age’, the Internet is becoming an integral part of daily life of minors and even essential element of youth culture (Ferrell J., 2009, pp. 219–227). Children are spending more and more time online (they are ‘in’ more often and longer); a growing frequency of using Internet, starting it at a younger age, with a wide spectrum of devices comprise some kind of fusion of online and offline world. It is even more important when taking into consideration the major purposes of minors Internet activity, which are social networking; they communicate and create interactions; besides they learn, e.g. do homework/schoolwork and entertain, e.g. play games (see: Livingstone, S., Mascheroni, G., Ólafsson, K.& Haddon, L., 2014).

Thus, it is important to point out the transformation of a status of a child from a receiver of AMS to a user (and – on the other hand – a consumer) of Internet services, where children and youth go beyond watching and listening (TV or radio, video etc.) and start to be a participant, actor, author of user generated content. Generally speaking, Internet has turned out to be a ground for individuals to create, access and share information, worldwide. This change influences a scope and characteristics of the threats.

The OECD² overview of online risks faced by children on Internet, has shown the following categories of them: technology ones, when the Internet is the medium through which the child is endangered by contents or where unsafe interactions (contacts) take place and risks related to children as consumers (connecting in particular with their

² See: point I. ii of the recommendation of the OECD *The protection of children online*, 2012; also OECD Council report *on risks faced by children online and policies to protect them*, 2012, p. 24.

exposure to aggressive marketing practices or excessive advertising) as well as information privacy and security threats (especially unintentional dissemination of personal data without understanding the consequences of such activities). In similar manner, within the EUkids online researches the: inappropriate content, contact and conduct risks (generally speaking harmful interactions with other minors and, especially with adults) have been distinguished. First category is connected with a receiver status of mass media, second and third with user`s participation and acting (Livingstone, S., Mascheroni, G., Ólafsson, K.& Haddon, L., 2014, p. 3).

Regarding a growing impact of Internet on children, from the criminological point of view, the threats should be considered within the traditional related to the content, e.g. pornography or violence and new concerning the Internet milieu, type of risks.

For traditional mass media (broadcasting), the exposure at inappropriate for particular age groups of children, content should be pointed out. More precisely, they concern any programs which might seriously impair development of minors, in particular that involve pornography or gratuitous violence, as well as those which are likely to impair it, but which scope is set up at internal level, showing sometimes significant differences in perception and defining of what content is appropriate and acceptable for particular age groups between countries (art. 27.1., Chapter VIII *Protection of minors in television broadcasting*, directive 2010/13/EU; see: Badźmirowska-Masłowska, K., 2012, *Ochrona dzieci i młodzieży przed negatywnym wpływem mediów audiowizualnych w świetle dokumentów Unii Europejskiej...*, pp. 71–117).

In the Internet environment access to the abovementioned content has been broadened, which constitutes a crucial modification of the scope of risks and potentially tougher harmful impact on minors` development, from this category of threats. It is due to the fact that: “The ease of accessibility and search-ability of information contained in computer systems, combined with the practically unlimited possibilities for its exchange and dissemination, regardless of geographical distances, has led to an explosive growth in the amount of information available and the knowledge that can be drawn there from” (*Explanatory Memorandum to the Convention on Cybercrime*, 23.11.2001, *Introduction point 4*). This means also a digital migration or rather extension of existing offline

threats to the virtual sphere, bearing in mind their mutual dependence and influence; the good example of bad behavior is online: bullying, harassment or grooming.

Regarding the abovementioned *Internet technology risks* (OECD report, 2012), the most dangerous is illegal content, especially if it concerns the sexual crimes against child (Badźmirowska-Masłowska, K., *Fighting against child sexual abuse and child sexual exploitation in Europe...*, 2013, pp. 147–160); in particular the early sexual abuse, may be detrimental to a child's and young adult's psycho-social development and destructive to minors' health (see: Recommendation No. R (93) 2 *on the medico-social aspects of child abuse*). There is no doubt that: “many more child pornography images [are] available now and many more individuals [are] accessing those images than would have been the case had the Internet not existed. (...); [It] is an active cause of child pornography” (Wortley R., Smallbone S., 2012, p.15), exacerbating the abovementioned problem by increasing: the volume of the images and the efficiency of dissemination of them.

In line with art. 9.1. of the Council of Europe (COE) *Convention on Cybercrime* (Budapest, 23.11.2001; *Title 3 – Content-related offences*), committed intentionally and without right: producing, offering, distributing or transmitting, procuring as well as possessing child pornography should be established as a criminal offences under State-Parties domestic law³. The

³ See: Recommendation 1065 (1987) of the Parliamentary Assembly of the Council of Europe *on the traffic in children and other forms of child exploitation*; Resolution No. 3 *on sexual exploitation, pornography and prostitution of, and trafficking in, children and young adults of the 16th Conference of European Ministers of Justice* (Lisbon, 1988); Recommendation No. R (89) 7 *concerning principles on the distribution of videograms having a violent, brutal or pornographic content*; Recommendation No. R(91)11 *on sexual exploitation, pornography and prostitution of and trafficking in, children and young adults* Adopted by the Committee of Ministers on 9 September 1991 at the 461st meeting of the Ministers' Deputies. Recommendation No. R (2000) 11 *on action against trafficking in human beings for the purpose of sexual exploitation*; Recommendation (2001)16 *on the protection of children against sexual exploitation*; Resolution 1099 (1996) *on the sexual exploitation of children*.

In particular Resolution 1307 (2002) *on sexual exploitation of children: zero tolerance*; see also Doc. 9535, report of the Social, Health and Family Affairs Committee, rapporteur: Mr Provera; Doc. 9573, opinion of the Committee on Legal Affairs and Human Rights, rapporteur: Mr Piscitello; and Doc. 9575, opinion of the Committee on Culture, Science and Education, rapporteur: Baroness Hooper). *Text adopted by the Assembly on 27 September 2002 (32nd Sitting)*.

term is understood as material that visually depicts: “a. a minor engaged in sexually explicit conduct; b. a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct” (art. 9.2).

Then, following the mentioned regulation, COE has established a convention strictly devoted *on the Protection of Children against Sexual Exploitation and Sexual Abuse to...* (Lanzarote, 25.10.2007), underlying a: “worrying proportions at both national and international level, in particular as regards the increased use by both children and perpetrators of information and communication technologies (ICTs), and that preventing and combating such sexual [crimes]” (*Preamble*). It might be treated as a basic standard for other legal instruments from the described scope of problems. Within the context of the convention, minors are treated as a victims (art. 3c) of the following, precisely defined, crimes: sexual abuse (art. 18), offences concerning: prostitution (art. 19), child pornography (art. 20), participation of a child in pornographic performances (art. 21) and corruption of children, solicitation of children for sexual purposes. Moreover, State-Parties were committed to settle the age below which engaging in sexual activities with a child is prohibited (age of consent).

Similarly standards has been settled in existing legislation of European Union (EU). Directive 2011/92/EU of the European Parliament and of the Council of the 13 December 2011 *on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA*, emphasizes that: “Sexual abuse and sexual exploitation of children (...), constitute serious violations of fundamental rights” (point 1 of the *Preamble*). It includes detailed provisions concerning the definition of criminal offences in the area of sexual exploitation – recruiting, forcing, knowingly attending pornographic performances, as well as causing or recruiting, forcing a child into a prostitution (art. 4–5). A sexual abuse of children has been also distinguished – causing for sexual purposes, a child-victim who has not reached the age of sexual consent, within the meaning of art. 2b (determined by national law), to witness sexual abuse, activities, even without having to participate or engaging the abovementioned child in sexual activities (art. 3); in particular the solicitation of children for sexual purposes has been indicated (art. 6). It also refers to incitement,

aiding, abetting, attempt and consensual sexual activities aspects of problem, as well as aggravating circumstances of the offences (art. 7–9).

The new, typical for the Internet environment threats are not only connected with a much wider access to an on-line potentially harmful content and simultaneously possibility to create it and share. It concerns, sometimes with the intention to harm the child, contacts, e.g. cyber-grooming (see: Badźmirowska-Masłowska, K., 2015, pp. 171–208) or exposure to hateful interactions, as cyberbullying) too; also bothering behaviors, like self-harm, self-inflicted injury, eating disorders advices websites etc. (see e.g. Andrzejewska A., 2014). On the other side a game, computer and cell addictions as a new kinds of Internet dangers have appeared (see e.g.: Weinstein A, Lejoyeux M., 2010, pp. 277–83).

Taking into consideration the macrosocial perspective of the threats, mainly a problem of digital exclusion should be mentioned (see: Livingstone S., Bober M., Helsper, E., 2005). Besides, it is important to mark the negative, both in individual and social dimension, consequences of unified pop-culture patterns, determining, irrespective of country, regional, local traditions, values, faiths etc., children`s views, believes opinions, attitudes, behaviors, which is clearly expressed within problematic aspects of body image issue (see e.g.: Clay, D., Vignoles, V. L., Dittmar, 2005) as well as wide-spreading of sexting phenomena among youth (see e.g. Andrzejewska A., 2014). Finally, regarding the discussed perspective, it is to be mentioned that directive 2011/92/EU should be fully complementary with directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 *on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA*: “as some victims of human trafficking have also been child victims of sexual abuse or sexual exploitation” (point 7 of the *Preamble*).

3. Legal instruments and/or alternative measures?

Minors face a broad spectrum of risks when they use new technologies, but risk have to be distinguish from harm, since not all children encounter it, and not all threats result in harm (Livingstone S., Haddon L., Görzig A., Ólafsson K., 2011, pp. 3-4). As they are more vulnerable than adults at the

potentially negative influence, they need a comprehensive, coherent support to be able to cope with the risks, to give a resilient reaction, especially based on an ability to recognize and identify dangerous content, situations and interactions; their approach should be connected with the wide scope of technical and social digital skills (Livingstone S., Haddon L., Görzig A., Ólafsson K., 2013, p. 26). *OECD Report on risks faced by children online and policies to protect them* has indicated the various dimensions of child protection policy: multi-layered, multi-stakeholder and multi-level (pp. 40–49).

The first one comprises direct and indirect policy tools, blending legislative measures with alternative measures such as: self and co-regulatory, technical, awareness raising and education, including positive content within child safety zones. It should be mentioned that: “Most countries would subscribe to the statement that what is illegal offline should be illegal online and champion a normative approach to child protection online. In such countries, the main challenge is to enhance the compliance with and enforcement of existing instruments rather than adopt additional laws and regulations” (*OECD Report on risks faced by children online and policies to protect them*, p. 41).

This approach seems to be justifiable, thus subjects to consideration, in particular bearing in mind the significance of net neutrality principle (see: N. van Eijk, 2011, pp. 7–19).

It has to be indicated that minors are entitled to get an exceptional care, given from all stakeholders: public authority, representatives of businesses as well as of a civil, information society, in particular the teachers and parents (guardians). Thus multi-stakeholder policy of an online child protection refers to their various roles, commitments and shared responsibilities. The policy purposes should be adopted at the government level to coordinate and monitor their implementation, initiate national campaigns, cooperation within platforms and awareness centers, as well as to facilitate other subjects' efforts, like self and co-regulation of private sector and activities of non-profit organizations.

The key role ought to be assigned to, directly responsible for children upbringing, parents (guardians). But the growing impact of Internet on children's life (in particular expressed in universality of pop-culture patterns), which is more noticeable than parents' one, has caused a problem of less and permanent reductive meaning of primary, family structures

(groups), define as: “those characterized by intimate face-to-face association and cooperation. (...) [and] (...) fundamental in forming the social nature and ideals of the individual” (Cooley Ch. H, 1910, p. 23). As a matter-of-fact, change of traditional guardians roles, determined by differentiation of the approach and competence of the technical and socio-cultural aspects of Internet, has divided family members into young – ‘digital – natives’ and old – ‘digital immigrants’ categories. The latest one are *de facto* excluded from daily, ‘mobile’ and ‘immerse’ minors life, even though their members have attempted to counteract this growing divide. As families are not able enough to fulfill their duties, the responsibility to guarantee a safety for children online, some-how has shifted on other stakeholders, such as educators, trainers, social workers, other public institutions (like libraries), in particular representing school environment.

Multi-level policy mechanisms at national and international levels regards mainly a realization of goals within the operational national and international collaboration, reflected in settling regulatory frames of soft law and regional legal standards (see: abovementioned conventions and directives), as well as in increasing international co-operation initiatives: “in the areas of law enforcement, exchange of hotline reports about illegal online material (*i.e.* INHOPE) and sharing of best practices for the protection of children online (*i.e.* INSAFE)” (OECD *Report...*, p. 49; see also: *Protecting children’s rights in the digital world: an ever-growing challenge*, 2014).

Concerning the basic premises of chosen legal and/or alternative methods of protection of minors in Internet, primarily the following criteria have to be taken into account:

- 1) seriousness of threats – whether they constitute crimes, in particular sexual offences against children or any other interferences of their development;
- 2) technical aspects of access to danger content, contacts and behavior – dependent on match certain services to the linear or non-linear AMS or to the other Internet services;
- 3) coverage of certain risks – which determines an individual or macrosocial character of threats as well as needed internal or international level of reaction on them;
- 4) age category of children and youth – which required different security means, both in technical and social context.

Overall, legislation pertaining to all illegal content is applying across all offline and online media and it is predominantly regulated on national level within the scope of general laws (e.g. consumer or privacy and information security related risks for minors).

The most anxious issue is connected with a need to counteract (to prevent and to combat) sexual crimes against children and youth and protect their fundamental rights as victims, within the wide national and international co-operation (art. 1 of the Lanzarote Convention, 2007), taking into account the best interest of them⁴. Directive 2011/92/EU establishes precise frame of such activity: “minimum rules concerning the definition of criminal offences and sanctions in the area of sexual abuse and sexual exploitation of children, child pornography [including online pornography and sex tourism – art. 21 of the directive 2011/92/EU] and solicitation of children for sexual purposes. It also introduces provisions to strengthen the prevention of those crimes and the protection of the victims thereof” (art.1). The framework should apply in both transparent and free from ambiguity manner.

Abovementioned instruments provide complementation of criminal (penal) regulations with necessary other legislative or alternative measures, both preventive and undertaken for assistance, support and protect child victims, especially within a scope of criminal investigations and proceedings. *Nota bene*, the direction is reflected in the aims of *the Global Alliance against Child Sexual Abuse Online*, comprise enhancing efforts to identify victims of child pornography and ensure them all kinds of necessary help, as well as to investigate cases, identify and prosecute offenders; then increasing public awareness of the risks posed by minors` activities and reducing the availability of child pornography online against re-victimization of children are indicated (see purposes of the directive 2011/92/UE and: *Global Alliance against Child Sexual Abuse Online: New Report and Threat Assessment*, 2015).

Regarding prevention aspects of the issue, education and training are particularized (art. 23.1 of the directive 2011/92/EU). First encourage

⁴ See: Resolution 1834 (2011) *Combating “child abuse images” through committed, transversal and internationally co-ordinated action*; Recommendation 1980 (2011) *Combating “child abuse images” through committed, transversal and internationally co-ordinated action*; also: Resolution 1835 (2011) *Violent and extreme pornography*; Recommendation 1981 (2011) *Violent and extreme pornography*.

awareness of the protection and children`s rights, among employees professionally engaged in contacts with them, in the area of education, health, social protection, judicial and law – enforcement (including front-line police officers), also in culture, sport, leisure, should be pointed out; by the way, when recruiting persons for organized voluntary or professional activities involving direct and regular contacts with minors, employers are entitled to check whether they have been convicted for sexual offences against child (art. 10.2. of the directive 2011/92/EU). Taking into consideration broader perspective, awareness raising campaigns addressed to the general public should be performed as well as programs or similar initiatives (projects) involving minors, representatives of public authorities, private sectors (e.g. media in particular through self-regulation or co-regulation) and civil society. Moreover, children as a special category of end-user within the frame od primary and secondary education have to be given an adequate information about the online risks, connected with sexual offences against them (Chapter II, art. 5–9 of the Lanzarote Convention; art. 23.2 and 23.3 of the directive 2011/92/EU).

The specialized authorities and adequate bodies are expected to designate mechanisms for data collection or focal points and coordinate on national or local level all activities of the organizations playing on the field (Chapter III, art. 10 of the Lanzarote Convention). Furthermore, combating this kind of criminality (delinquency) national public authorities at least within their territory are obliged to undertake measures against websites containing or disseminating child pornography such as prompt removal them or block access to them (art. 25 of the directive 2011/92/EU).

Protective measures of child victims of the sexual crimes are targeted at establishing a system of the necessary assistance and support for victims, their families and caregivers, within the scope of prosecution and jurisdiction process (art. 17–18 of the directive 2011/92/EU), bearing in mind on one hand that some of them are victims of organized crime (even human trafficking) and significant role of the Internet in producing and disseminating incriminated materials, on the other. This is crucial, that investigation and prosecution are not dependent only... “a report or accusation being made by the victim or by his or her representative, and that criminal proceedings may continue even if that person has withdrawn his or her statements” (art. 15.1 of the directive 2011/92/EU).

In particular reporting suspicion of children sexual exploitation or sexual abuse, setting up information services (helplines) and wide assistance to victims, including such elements like legal advice and physical, psycho-social care and recovery, applied before, during and for an appropriate period of time after the conclusion of criminal proceedings, regardless on the child victim's willingness to cooperate in the criminal investigation, prosecution or trial are the core of the system combating sexual criminality against children (Chapter IV, art. 11-14 of the Lanzarote Convention; art. 19-20 of the directive 2011/92/EU). Finally, it is important to add that intervention programs or other measures are also dedicated to the persons convicted of any of the sexual offences against child, provided by the relevant provisions (Chapter V, art. 7, 15–17 of the Lanzarote Convention; art. 22, 24 of the directive 2011/92/EU).

According to the provisions of the art. 27.1 of the directive 2010/13/EU (*Chapter VIII Protection of Minors in Television Broadcasting – Audiovisual Media Services Directive*) for linear services the ban of including content which might seriously impair the development of minors (in particular programs that involve pornography or gratuitous violence) has been sustained (as the standard was introduced under the *Television without Frontiers*” (TVWF) directive⁵). The prohibition should also applied to: “other programs which are likely to impair the (...) development of minors, except where it is ensured, by selecting the time of the broadcast or by any technical measure, that minors in the area of transmission will not normally hear or see such broadcasts” (art. 27.2 of the directive 2010/13/EU). Moreover, un-encoded programs ought to be preceded by an acoustic warning or are identified by the presence of a visual symbol throughout their duration (art. 27.3 of the directive 2010/13/EU).

⁵ Council Directive 89/552/EEC of 3 October 1989 *on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities*, OJ 17.10.1989 L 298; Directive 97/36/EC of the European Parliament and of the Council of 30 June 1997 *amending Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities*, OJ 30.07.1997 L 202

Regarding the 'on-demand' AMS restriction of access mainly technical means are applied; precisely services: "which might seriously impair (...) development of minors are only made available in such a way as to ensure that minors will not normally hear or see such on-demand audiovisual media services (art. 12 *Chapter IV Provisions applicable only to on-demand AMS*, of the abovementioned directive). There is no reference to a potentially harmful content. The differences of approaches to the linear and non-linear audiovisual media services (similar to other Internet services) are determined by distinctive technical specification of them. The mentioned provisions encourage to sustain broadcasting content ratings system, based on evaluation of the appropriateness of certain programs for different categories of age groups of minors. They also concern media content labeling schemes, including the issue of selecting time to broadcast content unsuitable for children.

In summary, most States include Internet within the scope of updated content regulations: "The regulation of child inappropriate content often has its origins in television regulation, which some countries (gradually) expanded in order to capture television-like formats (linear) transmitted over the Internet and certain on-demand services, with a few countries abolishing any distinction between old and new media (*i.e.* horizontal content regulation)" (OECD *Report...*, 2012, p. 62). Furthermore, "content regulation takes a two-pronged approach: a general ban on illegal content and [applied] national regulation [which expresses particular cultural and societal values] of child-inappropriate content up to defined age levels" (OECD *Report on risks faced by children online and policies to protect them*, 2012, p. 41); while the minimum rules concerning the definitions of criminal sexual offences against child (and sanctions) have been settled at European level, so they subject both to the international/ transnational (COE, EU) and national regulations.

Regarding contact and conduct – related risks (communication acts), some of them had been remarked within the scope of European soft law (e.g. Recommendation Rec(2006)12 of the Committee of Ministers to member states *on empowering children in the new information and communications environment*; Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States *on the protection of human rights with regard to social networking services*; Recommendation CM/

Rec(2014)6 of the Committee of Ministers to member States *on a Guide to human rights for Internet users*)⁶ and following that have been progressively introducing to the internal law solely as a new criminal offence or a new type of existing crime (e.g. bullying – harassment), but committed via electronic communications. Thus, for example cyber-grooming and cyber-bullying might become new versions of offline grooming and bullying, whereas harmful advice and sharing of problematic content expose children to threats connecting dangerous practices such as self-harm or sexting (nude or semi-nude photographs, video etc.), are considered within the criminal law or image rights provisions (Badźmirowska-Masłowska, K., 2015, pp.171–208). It is to be mentioned that in order to mitigate contact and conduct – related threats for minors online, introducing measures such mandatory monitoring of social media (e.g. chats) might be effective.

International and national legislation directed to guarantee the children safeness and security in the Internet environment, have been accompanied with a variety of so-called alternative methods, which are especially particularized and described within the soft law:

- 1) self and co-regulation – e.g. recommendation REC (2001) 8 of the Committee of Ministers to member states *on Self-regulation concerning cyber content*;
- 2) technical means – e.g. recommendation CM/Rec(2008)6 of the Committee of Ministers to member states *on measures to promote the respect for freedom of expression and information with regard to Internet filters*;
- 3) awareness raising and educational measures – e.g. recommendation 1586 (2002) *The digital divide and education*; recommendation Rec(2006)12 of the Committee of Ministers to member states *on empowering children in the new information and communications environment*.

⁶ See also: Resolution 1191 (1999) *Information society and a digital world*; Recommendation 1332 (1997) *on the scientific and technical aspects of the new information and communications technologies*;
Resolution 1843 (2011) *The protection of privacy and personal data on the Internet and online media*; Recommendation 1984 (2011) *The protection of privacy and personal data on the Internet and online media*;
Resolution 1877 (2012) *The protection of freedom of expression and information on the Internet and online media*; Recommendation 1998 (2012) *The protection of freedom of expression and information on the Internet and online media*.

The wide spectrum of self-regulatory initiatives, based on a voluntary commitment of certain part of private sector, as well as co-regulatory ones, being a combination of government and private regulation (see *e.g.*: P. Stępką, W. Kołodziejczyk, 2006; Harasz M., 2008; Palzer C., *European Provisions for the Establishment of Co-Regulation Frameworks Co-Regulation*, 2003, pp. 3-13) and modern forms of governance (e.g. public-private partnership, involving mobile network operators and operators of social network sites) are of a major importance to support efforts to protect minors in a new, 'flexible', online milieu: "Countries deploy various strategies to encourage self-and co-regulation such as by *i*) making explicit reference to these mechanisms in legislations; *ii*) giving a mandate to regulatory authorities to negotiate with stakeholders voluntary commitments; *iii*) creating platforms for stakeholders to convene; and *iv*) stirring problematic areas by threatening to resort to "command and control" style regulation" (*OECD Report on risks faced by children online and policies to protect them*, p. 41)⁷.

The initiatives should be strengthen, by a consolidation of existing solutions, extending them from tradition mass media sector to the Internet environment and establish common framework principles across industries, including mobile sector, which within the voluntary commitment, titled: *European Framework for Safer Mobile Use by Younger Teenagers and Children*, 2007 has adopted adequate aims of the activity in a media field. They include classification of commercial content with access control mechanisms for this which is dedicated for adult; besides, the awareness raising campaigns for children and parents and fight against illegal content have been indicated. The cross sectoral solutions might improve the effectivity of the whole system of minors' protection⁸.

As the child-inappropriate content both online and partly offline subjects to access restrictions and control (see *e.g.* Badźmirowska-Masłowska, K., *Ochrona małoletnich jako podstawa ograniczenia retransmisji*

⁷ "Existing models can be classified according to whether *i*) it is co-regulation or self-regulation; *ii*) it is an industry led commitment or it involves all relevant stakeholders; *iii*) it applies to one country or represents a regional agreement; and *iv*) it is a single group's standard or collective agreement", *OECD Report on risks faced by children online and policies to protect them*, p. 68.

⁸ See *e.g.* Pan-European Game Information as an example of solutions for on-line games, <http://www.pegi.info/pl/index/id/364/> (30.06.2017).

audiowizualnych usług medialnych w świetle prawa UE..., 2013, pp. 413–435), the complementary, in regard to legal obligations, role of technical, reliable and usable measures has been raised. “Technologies can be used to *i*) keep certain risks away from children (e.g. filtering technologies); *ii*) keep children out or, the reverse, admit only children to specific websites (e.g. age or identity verification systems); and *iii*) create child safe zones on the Internet (e.g. walled gardens)” (OECD Report..., p. 72).

A wide range of filtering techniques to limit access to or block Internet content are based on distinguishing white and black lists of content: “*whitelists* [recommended for younger children] block access to all Web content except when listed as suitable for the user; (...) *blacklists* [better for adolescents] enable access to all Web content except when listed as inappropriate for the user [in particular illegal, as sexual crimes against child]” (OECD Report..., p. 72). The most important and the most widely used is parental control software, which include: “services that require an installation or pre-installation on the end-user’s hardware; *ii*) service operated only on the server or network side; *iii*) a mix of both (OECD Report..., p. 75). It might be used not only to content filtering but also to control of use of the internet (e.g. social media), taking into account contact and conduct related risks. Future efforts ought to focus on making it more friendly for end-users, to enable parents (guardians) to choose the most effective personal setting to protect the child.

Contemporary, minors are increasingly accessing the Internet via enabled mobile devices (tablets, smartphones, game consoles), sometimes circumventing the filters which have been deployed on the desktop computers placed at home or school. Moreover, whereas children predominantly depend on parents (guardians) and other adult persons (like teachers, priests etc.), treated them as trusted influencers, during adolescence, youth has been under stronger influence of peer or wider offline and online ‘friends’ than ever before. Thus it is important to develop the awareness and educational methods, directed to their self-awareness, self-control and self-copy with meeting threats.

Awareness raising measures are aimed to inform and to make people conscious about the issues of public concern, just as children protection, including promoting active risk mitigation and coping strategies. They are addressed to the different group of users: children and parents, educators,

representatives of industry, civic society and policy makers. They are organized by non-profit organization, business, public bodies and within the frame of public-private partnership (OECD *Report...*, p. 79–80).

Empower end-users (in particular both children and their parents) seems to be a core of the effectiveness of the minors protection against online risks in an audiovisual sector, encompassing recognizing dangerous content, situations and interactions, methods to avoid harm (in particular to stay a victim of sexual offences), as well as finding copy strategies, including the significance of responsible behaviors; *inter alia*, acts which form part of the constituent elements of crimes (when a child – depending on certain age and internal legal solutions – might be treated as a perpetrator of a punishable act or even a crime) or caused harm to other person (in particular related to the minors development) must be avoided. Children must be equipped with useful knowledge and skills necessary to stay safe online. Therefore: “Topics [of the education] range from computer skills, cybersecurity and responsible use to fostering creative and critical capabilities, participation and active citizenship. Digital citizenship is a modern concept of Internet literacy which incorporates a number of elements including digital etiquette, digital literacy and digital security and which emphasizes participatory and creative opportunities of the Internet for children” (OECD *Report...*, p. 81).

The educational policy requires a constructive role for all stakeholders, mainly trainers, educators and teachers, in presenting legal boundaries, axiology (cultural, ethical and moral norms and expectations), risks, even though that there is no universally accepted model of them and significant differences between countries, regions, continents are observed; it seems that both European and national approach should be applied, reflecting in particular the local needs. Following the abovementioned direction, ideas of including media and Internet literacy education in school curricula (starting from primary or secondary level) as well as trainings organized for educators, should be pointed out (see: *e.g.* Badźmirowska-Masłowska K., *Edukacyjne aspekty bezpieczeństwa nowych technologii komunikacyjnych dla małoletnich w świetle Strategii Unii Europejskiej na rzecz lepszego Internetu dla dzieci...*, 2012, pp. 433–472).

Finally, it is to be said, that the one of the most important European initiatives, taking into account the abovementioned aspects of the heading

problem is *Safer Internet program* (now *Better Internet for Kids*; see: *From a Safer Internet to a Better Internet for Kids*). 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* of 2012 has focused on: creating a safe environment for children online by in particular stepping up awareness and empowerment and fighting against sexual crimes on the one side and promote high-quality content online for minors on the other (see e.g. Badźmirowska-Masłowska, K., *Rozwój nowych technologii komunikacyjnych a bezpieczeństwo dzieci w Unii Europejskiej* (1996–2011). *Perspektywa prawna...*, 2013, t. 1 s. 213–260). It is significant that: “On 7 February, millions of people in 120 countries were marking Safer Internet Day. The European Commission and leading digital players have committed to work towards curbing harmful content, conduct and contact in an Alliance to Better Protect Minors Online” (see: *Safer Internet Day 2017: European Commission welcomes alliance of industry and NGOs for a better internet for minors*).

4. Conclusions

The preceding overview of issues concerning the systemic aspects of the protection of minors against Internet threats brings to mind some general remarks. The mentioned below findings are implicated by the fundamental change of the *communicate on paradigm*, challenged by the dynamic and universally accessible nature of Internet environment.

The heading question of a choice between legal instruments and alternative measures as the adequate way of safeguard the minors security should be reformulated. Instead of connective ‘or’ an adverb ‘how’ might be put. That is because, the analysis of existing policies has indicated that only, depending on the kind of risks and technical method of access and use of the Internet, effective combination or may be proper blend them may fulfil their fundamental aim, which is constructing possibly most secure online environment. They should be set up on national level, but within an international co-operation (regional – COE and transnational – EU) in the complementary, coherent, consistent and multidimensional manner, involving all responsible for the children protection, stakeholders,

in particular, responsible for encouraging initiatives, monitoring and coordination of the activities in the area, public authorities (OECD *Report...*, pp. 50–55).

The considerations, analyses, researches have to take into account an individual perspective of the risks, bearing in mind especially the differences between particular age categories of children and youth, which determine their development period (which is – as it was pointed out – the subject of protection in audiovisual sector) and approach to the various threats, as well as macrosocial aspects of them, including the consequences of digital exclusion and worldwide unification of pop-culture patterns among young people.

While online sexual offences against child are cross-border in nature and so require not only regional but even global legislative attention, mainly national policy approaches to regulating content of linear and non-linear AMS as well as a content of other internet audiovisual services have so far predominantly employed in line with general internal law. By the way, framing media or wider audiovisual content (both illegal and inappropriate for children) within regulation across all media platforms (regardless of way of access to them) seems to be envisaged. Similar, the alternative measures should be applied in more coherent way (e.g. use of rating and content classification).

Finally, it must to be taken into consideration that legal instruments might not be effective enough, if only it is not possible to ban every single activity which potentially exposes minors to online risks. Thus parental care and educational measures are still of the major importance.

Bibliography

Andrzejewska A. (2014). *Dzieci i młodzież w sieci zagrożeń realnych i wirtualnych. Aspekty teoretyczne i empiryczne*, Difin, Warszawa.

Badźmirowska-Masłowska, K. (2012). *Edukacyjne aspekty bezpieczeństwa nowych technologii komunikacyjnych dla małoletnich w świetle Strategii Unii Europejskiej na rzecz lepszego Internetu dla dzieci*, „Journal of Modern Science”, 3(14)2012, s. 433- 472

Badźmirowska-Masłowska, K. (2013). *Fighting against child sexual abuse and child sexual exploitation in Europe. Media and internet perspective*, [in:] *Europe of*

- Founding Fathers. Investment in the Common future*, M. Sitek, G. Dammacco, A. Ukleja, M. Wójcicka (eds.), WSGE, Józefów, pp. 147–160
- Badźmirowska-Masłowska K., (2012). *Ochrona dzieci i młodzieży przed negatywnym wpływem mediów audiowizualnych w świetle dokumentów Unii Europejskiej. Wprowadzenie do analizy prawnej*, [w:] *Przestępczość nieletnich – teoria i praktyka*, S. Ćmiel, J. Zawisza (eds.), WSGE, Józefów, s. 71–118
- Badźmirowska-Masłowska, K. (2013). *Ochrona małoletnich jako podstawa ograniczenia retransmisji audiowizualnych usług medialnych w świetle prawa UE*, „Journal of Modern Science”, 2/2013, 413–435
- Badźmirowska-Masłowska, K. (2015). *Ochrona małoletniego przed zagrożeniami ze strony mediów w świetle amerykańskich standardów prawnych. Przegląd wybranych zagadnień*, [w:] *Prawo i proces karny w obliczu zmian*, J. Godyń, M. Hudzik, L. K. Paprzycki, Sąd Najwyższy, Warszawa, pp.171–208
- Badźmirowska-Masłowska, K. (2013). *Rozwój nowych technologii komunikacyjnych a bezpieczeństwo dzieci w Unii Europejskiej (1996–2011). Perspektywa prawna*, [w:] *Człowiek w świecie rzeczywistym i wirtualnym. Nowy wymiar zagrożeń w świecie realnym i wirtualnym*, A. Andrzejewska, J. Bednarek, S. Ćmiel (red.), WSGE, Józefów, t. 1 s. 213–260
- Castels M., (1996). *The Rise of the Network Society, The Information Age: Economy, Society and Culture*, Vol. I. Cambridge, MA; Oxford, UK: Blackwell
- Castels M., (1997). *The Power of Identity, The Information Age: Economy, Society and Culture*, Vol. II. M. Castells. Cambridge, MA; Oxford, UK: Blackwell
- Castels M. (2009). *Communication Power*, Oxford, New York: Oxford University Press
- Clay, D., Vignoles, V. L., Dittmar (2005). *Body Image and Self-Esteem Among Adolescent Girls: Testing the Influence of Sociocultural Factors*, „Journal of Research on Adolescence” 15(4), pp. 451–477
- Cooley Ch.H (1910). *Social Organization. A Study of Larger Mind*, Charles Scribner’s Sons, New York, 1910, <https://archive.org/details/socialorganizat00cool> (access 30.06.2017)
- Dodge R., Daly A., Huyton J., Sanders L.D. (2012). *The challenge of defining wellbeing*, “International Journal of Wellbeing”, 2(3)/2012, pp. 222–235
- van Eijk N. (2011). *Net Neutrality and Audiovisual Services*, “IRIS plus” 2011–5, pp. 7–19
- Ferrell, J. (2009). *Cultural criminology*, [in:] *21st Century Criminology. A Reference Handbook*, Sage Publications, Inc., 2009, pp. 219–227

- Giddens, A. (1991). *Modernity and Self-Identity: Self and Society in the Late Modern Age*. Stanford, CA: Stanford University Press
- Haraszt M. (2008). *The merits of media self-regulation. Balancing rights and responsibilities*, [in:] *The Media Self-Regulation Guidebook. All questions and answers*, OSCE, Vienna, Chapter I
- Ólafsson, K., Livingstone, S., & Haddon, L. (2013). *Children's Use of Online Technologies in Europe. A review of the European evidence base*. LSE, London: EU Kids Online. http://eprints.lse.ac.uk/50228/1/__Libfile_repository_Content_Livingstone%2C%20S_Children%E2%80%99s%20use%20of%20online%20technologies%20in%20Europe%28sero%29.pdf (access 30.06.2017)
- Livingstone S., Haddon L., Görzig A., Ólafsson K., *EU kids online*, September 2011, [http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/EU%20Kids%20II%20\(2009-11\)/EUKidsOnlineIIReports/Final%20report.pdf](http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/Final%20report.pdf) (access 30.06.2017)
- Livingstone S., Bober M., Helsper, E. (2005). *Inequalities and the digital divide in children and young people`s Internet use; findings from the UK Children Go Online project*, <https://www.york.ac.uk/res/e-society/projects/1/UKCGOdigitaldivide.pdf> (access 30.06.2017)
- Livingstone, S., Mascheroni, G., Ólafsson, K.& Haddon, L. (2014). *Children's online risks and opportunities: Comparative findings from EU Kids Online and Net Children Go Mobile*, <http://eprints.lse.ac.uk/60513/>(access 30.06.2017)
- Jordan A. B., Romer D. (ed.) (2014). *Media and the Well-Being of Children and Adolescents*, New York: Oxford University Press.
- Palzer C. (2003), *European Provisions for the Establishment of Co-Regulation Frameworks Co-Regulation*, 2003, [in:] IRIS Special: *Co-Regulation of the Media in Europe*, European Audiovisual Observatory, Strasbourg, pp. 3–13
- Potter, W.J, Cooper, R., Dupagne M. (1993). *The Three Paradigms of Mass Media Research In Mainstream Communication Journals*, *Communication Theory* Three/ Four November 1993, pp. 317–335
- Stępka P., Kołodziejczyk W. (2006). *Mechanizmy samo- i współ-regulacyjne w obszarze mediów*, *Analiza Biura KRRiT*, 14/2006
- Wortley R., Smallbone S. (2012). *Internet Child Pornography: Causes, Investigation, and Prevention*, New York: Praeger Publishing.
- Weinstein A, Lejoyeux M. (2010). *Internet addiction or excessive Internet use*, "The American Journal of Drug and Alcohol Abuse", Aug;36(5): 277–83

Basic documents

- 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*, Brussels, 2.5.2012 COM(2012) 196 final
- Convention on Cybercrime, Budapest, 23.11.2001, *European Treaty Series* – No. 185, <http://www.coe.int/en/web/conventions/full-list> (access 30.06.2017)
- Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Lanzarote, 25.10.2007, <http://www.coe.int/en/web/conventions/full-list> (access 30.06.2017)
- Council Directive 89/552/EEC of 3 October 1989 *on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities*, OJ 17.10.1989 L 298
- Directive 97/36/EC of the European Parliament and of the Council of 30 June 1997 *amending Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities*, OJ 30.07.1997 L 202
- Directive 2010/13/EU of the European Parliament and of the Council *on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive)*, OJ 15.4.2010 L 95/1, p. 1–24
- Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 *on the assessment of the effects of certain public and private projects on the environment*, OJ 28.1.2012, L 26, p. 1–21
- Proposal for a Directive of the European Parliament and of the Council *amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities*, Brussels, 25.5.2016 COM(2016) 287 final 2016/0151 (COD)
- Recommendations and Declarations of the Committee of Ministers of the Council of Europe in the field of media and information society, <https://rm.coe.int/1680645b44>, Media and Internet Division Directorate General of Human Rights and Rule of Law, Strasbourg, 2015 (access 30.06.2017)
- Recommendations and Resolutions adopted by the Parliamentary Assembly of the Council of Europe in the field of media and information society, <https://rm.coe.int/16806461f9>, Directorate General of Human Rights and the Rule of Law, Strasbourg, 2015 (access 30.06.2017)