SUGGESTIONS FOR THE REALISATION OF THE PREVENTIVE PURPOSE OF CRIMINAL SANCTIONS REGARDING THE CRIME OF CHILD PORNOGRAPHY COMMITTED USING INFORMATION SYSTEMS

Gabriela-Aura FODOR*

Abstract

Modern legislation embraces the idea that the sentence corresponding to a certain criminal offence is not merely a form of organized social retribution against a wrongdoer, but rather a way of preventing future transgressions, either by way of intimidation, example, or rehabilitation of the offender. The offence of child pornography committed using information and communication technology is relatively new in the Romanian legal landscape and the sanctions prescribed by the text of the Criminal Code are not necessarily a reflection of this principle of prevention. Also, there is no clear provision which might permit a judge to ban certain activities regarding the use of computers or the internet once a person is found guilty of such a crime. This restriction, however, although already applied by other states, raises a series of problems regarding supervision by probation officers and also from a human rights perspective, since the internet has now become almost essential for expressing basic rights and freedoms. As such, an indiscriminate ban from accessing the internet might prove to be even a harsher punishment that a jail sentence.

Key Words: *Information systems / child pornography / penalty / internet access*

JEL Classification: *[K14]*

1. Introduction

It is known that in modern criminal legislation, the punishment issued is not just a form of repression towards the person that has transgressed the community's rules, but rather its purpose is to prevent similar transgressions in the future. The Romanian Criminal code of 1968 clearly stated this in paragraph 1 of article 52. Even if the current Criminal code did not reiterate this provision, the principle it is based on remains as a guide to both lawmakers and courts when establishing a suitable punishment. It has been stated in doctrine that the preventive effect derives from the very basis of the punishment, which is to protect society against crimes (Andreescu, 2011, p.159)[1]. The coercion and the re-education roles contribute to the

* Judge - Cluj-Napoca Court of First Instance (Judecătoria Cluj-Napoca), PhD student, Faculty of Law of the „Babeş-Bolyai" University of Cluj-Napoca.

[1] The author considers, however, that the purpose of the sanction should be explicitly state by the legislator, even if in a concise form, because its absence form the Criminal code may lead to different interpretations in doctrine and jurisprudence, which would have implications of the sentencing process (p.160).

realisations of the aim of the criminal punishment, representing a warning as to its inevitability in case a new crime is committed (Mitrache & Mitrache, 2007, p.189). In some situations, in order to ensure sanctioning efficiency, it is also necessary to remove the element which facilitated the perpetration, by prohibiting the law breaker form being in certain locations, such as cities, form contacting certain persons, or form carrying out some activities.

Crimes committed using information systems have a series of particularities not only regarding their detection and investigation, since discovering the traces of the crime, in the sense of alterations of the scene of the crime as a material result of a person's actions (Labo, 2014, p.73), involves specific knowledge of information technologies, but they can also determine the need for a distinct approach to sanctioning from the classic model. The impact of such crimes and the number of victims are difficult to determine and the environment where they were perpetrated allows for an easy recurrence of the offence. The virtual space does not permit a simple removal of the guilty person and banning all access to the Internet is a drastic measure, which could affect many aspects of the social and professional life of the one involved. However, there is legislation which permits such restrictions, under specific conditions, as it will be further shown.

2. Penalties for the crime of child pornography committed using information systems

The penalties for the crime of child pornography committed using information systems have been lowered in the new Criminal code, as opposed to article 51 paragraph 1 of Law no.161/2003, which established a jail sanction form 3 to 12 years and restriction of certain rights for producing in order to spread, offering or providing, spreading or transmitting, procuring for personal use or for others of pornographic materials depicting minors using information systems, or a data storage device. According to article 374 paragraph 2 of the Criminal code, all form of perpetration of this crime which involve information systems or data storage devices, respectively producing, possession for exposing or distributing and also acquisitioning, storing, exposing, promoting, distributing and providing pornographic images of minors are punishable with a jail sentence from 2 to 7 years, except the act of illegally accessing such materials, for which the text of paragraph 3 of the same article settles a punishment of 3 months to 3 years jail or a fine. The only aggravating circumstances introduced by Emergency Government Ordinance no.18 of 2016 were regarding the actions listed in paragraph 2 of article 374, so with the exclusion of illegal access, and involved the commission of the offence by a family member, by a person who ensures care, education, security or treatment for the child, or who abused his position of trust or authority over the child, or if the action endangered the child's life.

From this we can notice that the legislator does not chose to make a structured difference, based on the degree of social danger of each activity, but only considers the use of information technologies as an aggravating circumstance for the "classic" ways of committing this crime, which also include acquisition of the materials, showing that illegal access, which is specific cu the virtual environment, is considered even less dangerous.

This perspective does not correspond with the mode suggested by Directive 2011/92/EU 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/JHA. According to article 5, paragraph 2 of the directive, acquisition or possession of child pornography shall be punishable by a maximum term of imprisonment of at least 1 year. Paragraph 3 of the same article establishes that knowingly obtaining access, by means of information and communication technology, to child pornography shall be punishable by a maximum term of imprisonment of at least 1 year. As such, acquisition and obtaining access to the forbidden material are considered as equally grave, which is understandable, since both actions represented involve simply receiving the materials. Paragraphs 4 and 5 suggest a maximum term of imprisonment of at least 2 years for distribution, dissemination or transmission of child pornography, or for offering, supplying or making available child pornography. The most severe punishment, of a term of imprisonment of at least 3 years, is reserved for production of child pornography. One can notice that the maximum penalty level increases as the transgression is more associated with the source of the illegal material, the manufacturers, the purveyors or suppliers being also considered as representing a high degree of social danger, while the consumers would be the ones that deserve a more lenient treatment. Of course, this differentiation, which is based on the abstract degree of danger of each act, is justified, seeing as in most cases the production of pornographic materials implies different forms of sexual exploitation of the minors depicted.

Usually, for the legal individualization of punishments, the legislator builds upon a general evaluation of the social danger, using data which reflect the importance of the protected values, the seriousness of a possible transgression, the potential outcome, the characteristics of the perpetrator, and the frequency of similar occurrences (Ivan, 2011, p.139). Having all this is mind, however, as a judge form Portland observed, mere possession of child pornography contributes to the exploitation of children, because it creates demand for the exploitive images (The United States Attorney's Office – District of Maine, 2015). In a Report to Congress form the years 2010 (United States Department of Justice, 2010, p.17), The United States Department of Justice remarked that for the years 2008-2009, complaints registered by the Internet Crimes Against Children Task Force were mostly related with distribution and possession, rather than the production of

illicit images, this development of the market for pornographic images involving minors being responsible for new forms of abuse. Because of the rise in demand, some individuals are encouraged either to commit sexual offences against minors, or to "order" such abuses in order to make profit or to gain status within a community. From this perspective, a possible means of preventing new crime would be to enhance the punishment for the acts of illegal access and possession of such images, in order to diminish the demand for the forbidden materials. Such an approach would focus more on the intimidating factor of punishment, which has been sometimes considered to be one of the main, if not the only way to realise prevention, especially for those that are occasional offenders and who have broken the law as a result of a series of fortuitous events, since their moral structure does not need to be submitted to a process of transformation and reconstruction which would influence their psyche (Daneş, 2004, p.161). However, a heavier punishment did not always prove to be an efficient way to prevent crime. In addition, the point of punishing is not to cause the offender a suffering equivalent with the evil committed, which was considered to be no more than "legalised revenge" (Daneş, 2004, p.156), and any punishment, once actually applied, represents a sufficient example for others, by proving that the threat is not just symbolic (Daneş, 2004, p.162).

3. About prevention of the crime and human rights

Taking into consideration the specificity of the criminal acts involving information systems, more than incarceration, preventing the perpetrator form committing new deeds could be achieved by restricting certain rights for a determined period. Even if the text in the Criminal code did not retain the compulsoriness of restricting certain rights alongside the main punishment, the court could still apply complementary and accessory punishments by referring to article 67 paragraph 1 of the Code, when it considers that the nature and seriousness of the offence, the circumstances of the case and the offender's person justify them. Some restrictions can also be the result of a suspended sentence under probation, when it is considered that it would not be advisable to remove the offender form his social surroundings and that the purpose of the punishment can be achieved without incarceration.

Complementary and accessory penalties or surveillance measures which can be applied during probation are listed in a restricting manner by articles 66 paragraph 1 and 93 paragraphs 1 and 2 of the Criminal code. Of these, none is adapted to this new kind of crime, since the most important restriction which must be imposed if forbidding the offender from using the Internet, or just the system used to commit the crime, within the limits demanded by the need to prevent new crimes. Even if by way of a generous interpretation one could consider that this

sanction might be included in the category of forbidding to conduct the activity which aided the commission of the offence, not in every instance the mere use of a personal computer or of the Internet could be classified as conducting an activity, as prescribed by article 66 of the Criminal code.

Some states have chosen to regulate such a possibility. For example, article 65.10 paragraph 4, b) of the New York Criminal Code states that when imposing a sentence of probation or conditional discharge upon a person convicted of an offense for which registration as a sex offender is required, and the victim of such offense was under the age of eighteen at the time of such offense or such person has been designated a level three sex offender or the internet was used to facilitate the commission of the crime, the court shall require, as mandatory conditions of such sentence, that such sentenced offender be prohibited from using the internet to access pornographic material, access a commercial social networking website, communicate with other individuals or groups for the purpose of promoting sexual relations with persons under the age of eighteen, and communicate with a person under the age of eighteen when such offender is over the age of eighteen, provided that the court may permit an offender to use the internet to communicate with a person under the age of eighteen when such offender is the parent of a minor child and is not otherwise prohibited from communicating with such child. Also, paragraph 5, a) of the same article states that when imposing a sentence of probation upon a person convicted of an offense for which registration as a sex offender is required, the court may require that the defendant comply with a reasonable limitation on his or her use of the internet that the court determines to be necessary or appropriate to ameliorate the conduct which gave rise to the offense or to protect public safety, provided that the court shall not prohibit such sentenced offender from using the internet in connection with education, lawful employment or search for lawful employment.

Many other American states permit such a measure to be imposed by the court, as part of a sentence of probation or conditional discharge, for the crime of child pornography (The United States Attorney's Office – Southern District of Texas, 2015).

In *United States v. Sofsky*, it was considered that a total ban on Internet access prevents use of e-mail, an increasingly widely used form of communication, as well as other common-place computer uses such as doing research, getting a weather forecast, or reading a newspaper online. As such, the condition imposed by the first instance court, prohibiting from accessing a computer or the Internet without his probation officer's approval, inflicts a greater deprivation on the offender's liberty than is reasonably necessary[2]. In other

[2] U.S. v. Sofsky, 287 F.3d 122 (3d Cir. 2002) http://caselaw.findlaw.com/us-2nd-circuit/1249776.html (last accessed April 2016).

situations, like in *United States v. Paul*, a case of child pornography, the aforementioned arguments were dismissed and it was decided that an absolute ban on Internet access was proportional, without the possibility of exercising this right under the supervision of the probation officer. When issuing its decision, the Court of Appel stated that, considering the nature of the offence, the restriction was reasonably necessary to protect the public and to prevent recidivism, without it being *per se* an unacceptable condition of supervised release, simply because such a prohibition might prevent a defendant from using a computer at the library to get a weather forecast or to read a newspaper online during the supervised release term[3].

In the United Kingdom, similar decisions were taken in cases of sexual offences. In *Smith (Paul),* for example, where the offender was found guilty of possessing indecent images of children, the Court of Appeal upheld the measure which prohibited the defendant from downloading, saving or viewing any material form the internet, except when it was for the purposes of lawful employment, study or leisure social interactions with persons over the age of 18 (Walden & Wasik, 2011, p.380)[4.]

Such a solution might seem appropriate, but although it is adapted to the way of committing the crime, the actual supervision of the ban is difficult. The probation officer should possess knowledge of computers superior to that of the convicted offender, otherwise the latter would be able to remove form his personal computer recent traces of the illicit activity (Khilman, 2004, p.71). Moreover, the person on probation is not limited to his personal computer. Of course, this does not mean that such a ban would be completely without efficiency, since there are ways of remotely monitoring a person's activity in the virtual space, by using software which can signal, for example, if certain restricted sites were accessed by a particular user. Also, there are filtering programmes, which can be installed on the devices commonly used by the convicted offender.

The main issue posed by the possibility of forbidding Internet access is that of determining what this implies, in order to correctly establish the limits of the restriction in the process of judicial individualisation of the penalty. In the conclusion of the report presented to the United Nations in 2011, Frank la Rue, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, considered that cutting off users from Internet access, regardless of the justification provided, including on the grounds of violating intellectual property rights law, is disproportionate and a violation of article 19, paragraph 3, of the International Covenant on Civil and Political Rights (La Rue,

[3] United States v. Paul, 274 F.3d 155, 169 (5th Cir.2001) http://caselaw.findlaw.com/us-5th-circuit/1333258.html (last accessed April 2016).
[4] Smith (Paul) [2009] EWCA Crim 1795.

2011, par.78). Also, it was said that given that the Internet has become an indispensable tool for realizing a range of human rights, combating inequality, and accelerating development and human progress, ensuring universal access to the Internet should be a priority for all States, which should develop a concrete and effective policy to make the Internet widely available, accessible and affordable to all segments of population (La Rue, 2011, par.85). However, the document does not affirm the existence of a right to Internet access, but rather the fact that such an access is necessary for exercising other fundamental rights and liberties. In other cases, this very connection was considered enough to confer the status of right to the possibility of Internet access, with the negative obligation on behalf of the State to not hinder it without justification (Tenenbaum, 2013, p.30). It cannot be denied that owing to the multitude of activities which are currently carried out online, banning all forms of Internet use could have consequences as serious as a prison sentence. The digital space is often necessary for one's profession; it is used for human interaction, study, obtaining information or as a means of artistic expression, of conveying opinions and beliefs. The effect of such a penalty could be that of marginalisation, removing a person form a part of society that is not necessarily linked with the crime committed. In addition, as it was established in the previous decisions, using the computer and the Internet may be essential to find a job, which is an aspect of the rehabilitation process after being freed from prison (Smith, 2004, p.3).

4. Conclusions

Imposing such a restriction could be a welcomed measure in order to prevent new crimes form being committed using information systems since, similar with banning a person form being in a certain city or other territory, at least temporarily the offender is removed from the environment which facilitated the transgression and where he represents a threat to other users. The possibility to access such technology has indeed become an almost indispensable means of exercising basic rights, but it is also a privilege, and abusing the opportunities offered by this resource should be sanctioned by its withdrawal for a determined period and within proportional limits. In this way, the sentencing process would be extremely important, in order to justly establish the conditions for Internet access.

Bibliography:

1. Andreescu, M., 2011 *Considerații referitoare la individualizarea pedepselor,* Dreptul, October, Issue 10, pp. 159-171.
2. Daneş, Şt., 2004 *Rolul pedepsei în combaterea infracțiunilor,* Dreptul, Issues 12, pp. 155-169.
3. Ivan, G., 2011 *Gravitatea infracțiunii săvârşite - Criteriu general şi principal de individualizare a pedepsei în concepția Noului Cod penal român*, Dreptul, December, Issue 12, pp. 136-160.
4. United States Department of Justice , 2010. *The National Strategy for Child Exploitation Prevention and Interdiction - A Report to Congress.* [Online] Available at: https://www.justice.gov/psc/ docs/natstrategyreport.pdf [Accesed April 2016].
5. Khilman, V., 2004 *Can a Court Lawfully Forbid a Person Access to the Internet as a Term of His Probation?*. [Online] Available at: https://www.fcsl.edu/ sites/fcsl.edu/files/ART%204.pdf [Accessed April 2016].
6. La Rue, F. , 2011. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.* [Online] Available at: http://www2.ohchr.org/english/ bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf [Accessed April 2016].
7. Labo, G., 2014 *Cercetarea criminalistică,* ed. a 2-a Bucureşti: Pro Universitaria.
8. The United States Attorney's Office – District of Maine, 2015. United States Department of Justice. [Online] Available at: https://www.justice.gov/usao-me/pr/berwick-man-sentenced-two-years-possessing-child-pornography [Accesed November 2015].
9. Mitrache, C., Mitrache, C., 2007 *Drept penal român: partea generală,* ed. a 6-a ed. Bucureşti: Universul Juridic.
10. Smith, R., 2004 *Criminal Forfeiture and Restriction-of-Use Orders in Sentencing High Tech Offenders,* [Online] Available at:
http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi286.pdf [Accessed April 2016].
11. Tenenbaum, J., 2013 *503 Error, Service Unavailable - Access to the Internet as a Protected Right.* [Online] Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2422566 [Accessed April 2016].
12. The United States Attorney's Office – Southern District of Texas, 2015. United States Department of Justice. [Online] Available at: https://www.justice.gov/usao-sdtx/pr/dallas-man-sentenced-using-social-media-obtain-sexually-explicit-photos,https://www.justice.gov/usao-dtx/pr/victoria -man- heads-prison-possessing-child-pornography-1 [Accessed November 2015].
13. Walden, I. & Wasik, M., 2011 *The internet: Access Denied Controlled!*. [Online] Available at: https://qmro.qmul.ac.uk/xmlui/bitstream/handle/123456789/3291/
WALDENTheInternet2011FINAL.pdf?sequence=2 [Accesed April 2016].