SÉRIE “Právní vědy”

[https://doi.org/10.52058/2695-1592-2022-1\(8\)-189-193](https://doi.org/10.52058/2695-1592-2022-1(8)-189-193)

Yana Naidon

*PhD student at the Department of Information, Economic
and Administrative Law
Faculty of Sociology and Law
National Technical University of Ukraine
«Igor Sikorsky Kyiv Polytechnic Institute,
Kyiv, Ukraine,
<https://orcid.org/0000-0002-8187-6623>*

ISSUES OF THE INVESTIGATION INTO CYBERCRIME RELATED TO THE CREATION AND DISSEMINATION OF PORNOGRAPHIC CONTENT

Abstract. The modern development of Ukrainian society is conditioned, on the one hand, by the dynamics of internal social processes that began with the advent of democracy and, on the other, by globalization. Under the influence of a complex set of innovations, there are fundamental changes in the economic, social, political, cultural and other spheres of public life, and a new level of social reality has been formed. However, against the backdrop of positive changes, a number of socially negative phenomena, such as pornography, have appeared. With the emergence of new ways of producing and distributing pornographic products, such as virtual pornography, which has intensified the commercialization of the intimate side of people's lives and the exacerbation of other social problems there have been clear trends in the uncontrolled increase in the flow of pornography and the involvement of new social groups in its circulation. In addition, the distribution of pornographic materials or objects in some cases is related to sexual exploitation, trafficking in human beings, coercion to prostitution, and other crimes, which several times increases the public danger of such acts. An essential place in the investigation of crimes related to the creation and dissemination of pornographic content belongs to the initial stage, where it is vital to establish the information nature of the circumstances, to choose the right direction of the investigation and means and methods of performing investigative actions. Inaccurate assessment of information obtained at the initial stage of the investigation is likely to complicate the process of establishing the truth in criminal proceedings. The article addresses the problem

issues of investigating cybercrime related to the creation and dissemination of pornographic content.

Keywords: IP address, cybercrime, pornography, pornographic content.

Introduction. Currently, trafficking in pornographic materials or objects is concentrated mainly in organized crime groups. People engaged in the aforementioned activity have an established market for the sale of manufactured products throughout the territory of Ukraine and abroad. According to Art. 3 of the United Nations Convention against Transnational Organized Crime, adopted by General Assembly resolution 55/25 of November 15, 2000, is transnational if committed in more than one State or a substantial part of its preparation, planning, direction or control in another State [1]. These circumstances make it possible to attribute the distribution of pornographic material or objects to transnational crimes.

Lack of a single international document in this area is also negatively counteracted by the current forms of trafficking in pornographic products. The provisions of the International Convention on the Suppression of Trafficking in and Trafficking in Pornography, adopted on September 12, 1923 (the annexation of Ukraine on July 8, 1935), are still in force and are mostly outdated and contrary to the current criminal law of most countries, including Ukraine. The widespread distribution of pornographic products has led to a reassessment of attitudes towards it: a significant part of the population has become loyal to the presentation of pornography through media, which is a prerequisite for the spiritual impoverishment of society. It should be noted that now there are no effective mechanisms to protect the individual from inconsistent contact with pornographic products, whose demonstration and advertising are increasingly aggressive. It has become apparent that the current legal framework and social mechanisms for combating pornography do not meet current conditions and need reforming. Today, analyzing the official statistics for reproducing the crime of import, production, sale, and distribution of pornographic items in Ukraine, we can speak of an increase in the number of crimes related to the distribution of pornographic materials or objects in 2017-2018. Thus, in 2015, under Article 301 of the Criminal Code of Ukraine, 1022 criminal offenses were registered, in 2016 - 923, in 2017 - 1538, in 2018 - 1662, in 2019 - 1012 [2].

Analysis of research and publications. The results of the analysis of scientific publications indicate that the issues of information and legal aspects of counteracting cybercrime have been partially the subject of research. In national legal literature, V. Brizhko, V. Butuzov, V. Pylypchuk, K. Titunin, M. Shvets, O. Yurchenko, and others have paid particular attention to these issues at various times. The problems of investigation of pornography crimes were investigated directly in the works of S. Denisov, R. Djindzholi, S. Kondranin, A. Starushkevich, I. Sugakov, O. Khabarov, and S. Khilchenko.

Purpose of the article. This article aims at the problematic issues of investigating cybercrime related to the creation and dissemination of pornographic content, the emergence of which is related, firstly, to the substance of the information and, secondly, to the lack of legal regulation of information and law enforcement activities.

Presentation of the main material. Note that current criminal procedural and information legislation does not sufficiently take into account the capabilities of modern information technology, which complicates the fight against cybercrime. So for today, “gathering evidence in e-form is a difficult enough process due to the complexity of the objects ... not every investigator has specialized knowledge in the field of computer technology enough to organize the investigation successfully... a specialist should hold opportunities” [3].

The initial stage of investigating crimes related to the creation and dissemination of pornographic content is in some way associated with the electronic form of information. It is due to the fact that cloud technologies are very widely used to store data today. Here, too, the problem arises of the influence of different jurisdictions when the owner of the information and the owner of the information storage resource are in different states. Therefore, it is essential for law enforcement officials in Ukraine to know and be able to correctly apply the law of the country where the fact or trace of cybercrime is physically stored. Knowledge of the information law of such a state will allow law enforcement officers to request official legal assistance properly. In current realities, there is an urgent need to improve the existing system of exchange of information between the major actors of cybersecurity significantly in real-time. It is also vital to engage in law enforcement and private actors.

According to A. Maruschak, “... Today there is no nationwide database of IP-addresses in Ukraine, the existence of which would facilitate immediate disclosure of committed cybercrime. Establishing a unique IP address and linking it to a criminal (victim) is one of the most important steps in investigating cybercrime. Another problem is that due to the limited number of IP addresses, providers use Dynamic IP Address (Dynamic Host Configuration Protocol (DHCP)). It appears that such a database of IP addresses should be created within the framework of the public-private partnership of the State Secretariat of Communications with operators, Internet access service providers”[4]. In order to stop the process of committing cybercrime and eliminate the consequences, it is necessary to take prompt actions. The procedural law of many States Parties to the Convention on Cybercrime of 23.11.2001 (hereinafter referred to as the “Convention”) contains rules providing for a particular procedure for the interception and disclosure of data on the computer systems for the purpose of investigating cybercrime [5].

However, according to clause 7 of Part 1 of Article 162 of the Criminal Procedure Code of Ukraine (hereinafter referred to as the CPC of Ukraine)

information contained in telecommunication operators and providers, about the connection, subscriber, provision of telecommunication services, including the receipt of services, their duration, content, transmission routes, etc., are covered by law-protected secrecy [6]. So, to obtain the information necessary to end the crime or to establish the perpetrators of the crime, to eliminate the negative consequences of the criminal offense, in particular, the blocking (restriction) of a resource with illegal content, law enforcement agencies spend considerable time in obtaining a proper court decision in criminal proceedings. Therefore, additional powers should be given to law enforcement officers who investigate cybercrime related to access to information relevant to cybercrime investigation. Such authorities are provided for in the Convention. Presidential Decree No. 32 “On Decisions of the National Security and Defense Council of Ukraine of December 29, 2016” On Threats to the State’s Cyber Security and Immediate Measures for their Neutralization” provides for elaboration legislative proposals to improve cybercrime counteraction [7].

Conclusions. Thus, understanding the problematic issues of investigating cybercrime related to the creation and dissemination of pornographic content, including the application of information law, as well as the possibilities of solving them, will increase the effectiveness of cybercrime investigation by Ukrainian law enforcement agencies. Based on the above, it is necessary to develop a single international document in the field of counteraction to modern forms of trafficking in pornographic products, in particular, with regard to cybercrime. In the CPC of Ukraine to define the concept of digital (electronic) evidence; provide an effective and efficient mechanism for restricting or blocking a particular information resource (information service); introduce specific conditions for investigative actions, such as the search and seizure of digital (electronic) evidence, first of all, to provide for the procedurally significant possibility of copying data.

References:

1. Konvencija Organizacii Ob'ednanih Nacij proti transnacional'noi organizovanoi zlochinnosti [United Nations Convention against Transnational Organized Crime]. (n.d). *zakon.rada.gov.ua* Retrieved from https://zakon.rada.gov.ua/laws/show/995_789 [in Ukrainain].
2. Statistichna informacija [Statistical information]. *www.gp.gov.ua* Retrieved from <http://www.gp.gov.ua/ua/statinfo.html> [in Ukrainain].
3. Grebenjuk, M.V. (2017). *Vikorisannja elektronnih (cifrovih) dokaziv u kriminal'nih provadzhennjah* [The use of electronic (digital) evidence in criminal proceedings]. K.:MNDC pri RNBO Ukraïni [in Ukrainain].
4. Marushhak, A.I. (2018). Informacijno-pravovi aspekti protidii kiberzlochinnosti [Information and legal aspects of combating cybercrime]. *Informacija i pravo- Information and law*, 1(24), 127-132 [in Ukrainain].
5. Konvencija pro kiberzlochinnist' [Cybercrime Convention]. *Oficijnij visnik Ukraïni - Official Bulletin of Ukraine*, 65, 253 [in Ukrainain].

6. Закон України “Криминальний процесуальний кодекс України” [The Law of Ukraine “Criminal Procedure Code of Ukraine”]. (n.d). *zakon.rada.gov.ua* Retrived from <https://zakon.rada.gov.ua/laws/show/4651-17#n1048> [in Ukrainain].

7. Ukaz Prezidenta Ukraïni “Pro rishennja Radi nacional'noï bezpeki i oboroni Ukraïni” [Presidential Decree “On the decision of the National Security and Defense Council of Ukraine”]. (n.d). *zakon.rada.gov.ua* Retrived from <https://zakon.rada.gov.ua/laws/show/32/2017#n2> [in Ukrainain].