UDC 343.1
DOI https://doi.org/10.32849/2663-5313/2022.6.16

Oleh Tarasenko,
Doctor of Law, Associate Professor, Professor at the Department of Operational and Investigative Activities, National Academy of Internal Affairs, 1, Solomianska square, Kyiv, Ukraine, postal code 03035, o.s.tarasenko@gmail.com
ORCID: *orcid.org/0000-0002-3179-0143*

Tarasenko, Oleh (2022). Legal and theoretical framework for search activities to detect criminal offences related to illegal content on the Internet. *Entrepreneurship, Economy and Law*, 6, 106–111, doi: https://doi.org/10.32849/2663-5313/2022.6.16

LEGAL AND THEORETICAL FRAMEWORK FOR SEARCH ACTIVITIES TO DETECT CRIMINAL OFFENCES RELATED TO ILLEGAL CONTENT ON THE INTERNET

Abstract. ***The purpose of the article*** is to study the legal and theoretical framework for search activities to detect criminal offences related to illegal content on the Internet.

Results. The article considers and analyses the level of ensuring the regulatory and legal framework for the prevention of illegal content on the Internet, in particular in social networks, the creation of a security mechanism to prevent the impact of illegal content on children, as well as the identification of persons who distribute illegal content. The article reviews scientific researches on tactics of detection of criminal offenses, carried out in several areas, and proves that mainly researchers in tactics of detection of criminal offenses distinguish two levels: operative-search and investigative, in accordance with which they consider the methodology of pre-investigative operative-search acquisition and accumulation of primary (intelligence) information to initiate an investigation (about criminal activities) and direct investigation methodology.

Conclusions. According to the results of scientific research, the subject of which were separate issues related to the detection system of the analyzed category of criminal offenses, forensic support for the investigation of criminal offenses committed with the use of information and telecommunication systems, the issue of legal protection of social relations in the field of the undisturbed functioning of such systems, as well as operational provision of combating the specified types of criminal offenses, it is worth concluding about the need for further research and scientific resolution of theoretical and organizational tasks that arise during the detection of criminal offenses related to the circulation of illegal content on the Internet.

Key words: Internet, illegal content, circulation, criminal offences, detection, legal framework, theoretical substantiation.

1. Introduction

Information and communication technologies are one of the most important factors influencing the formation of priority trends in development of the XXI century, which are the achievements of mankind in practical implementation of new electronic information technologies. The processes of informatisation are developing, related to the expansion of access to information resources and means of their production of all categories of population (Dovhan, Doronin, 2017, p. 4). Although modern global trends in development are based on the widespread introduction and application of information and communication technologies, they simultaneously actualise the problem of information security and cyber security (Cabinet of Ministers of Ukraine, 2017). One of the criminal activities that is rapidly progressing with the development of communication computer systems is the criminal use of the Internet through the posting of illegal content. For example, in 2016, there were 124 criminal offences related to illegal content on the Internet; in 2017 – 141; in 2018 – 196; in 2019 – 163; in 2020 – 235 (i. e. in recent years their absolute number almost doubled). Thus, the share of cyber-threats is growing and this trend will increase as information technology develops and converges with artificial intelligence technologies in the next decade. However, the legal literature lacks a unified assessment of the real threats due to the placement of illegal content on the Internet: the positions

of experts on the characterisation of this type of activity are opposite from excessive "blowing up" of negative consequences of the use of such content to statement that the person is free to choose what kind of content on the Internet to perceive. This trend is due in part to the considerable latency of criminal acts; the fact that there is no uniform approach to the need to actively search for facts of criminal offences, causing illegal content posted on the Internet; inability in some cases to calculate causal relationships of illegal content and causing harm in the commission of individual illegal acts due to the placement of said content. Although cyber security processes find gradually legal substantiation, almost no scientific, theoretical perspective on search activity as a result of the adoption of a number of legal regulations in this field, aimed at implementing the provisions of these regulations effectively, exist. This situation calls for an analysis of the existing theoretical rationale for searching activities regarding the detection of criminal offences related to illegal content on the Internet.

The scientists have developed a methodology of detection of individual criminal offences, highlighting elements of search activities: Yu.O. Yermakov has identified certain elements of search: objects as material traces and objects of search activities when detecting criminal offences (Yermakov, 2020, pp. 177–181). Part of the researchers believe that the detection of criminal offences refers only to operative-search activities (Belkin, 2001, p. 792); the same situation continued in modern conditions, for example, A.A. Shapovalov identifies the legal framework for operative search (Shapovalov, 2015, pp. 147–151); sphere and place of search activities (Shapovalov, 2018, pp. 304–314). A number of scholars argue that the detection of criminal offences is the prerogative of all law enforcement bodies. For example, M.B. Borchakovskyi consistently builds a system for detecting criminal offences (Borchakovskyi, 2018, pp. 17–19); persons as objects of search activities (Borchakovskyi, 2017, pp. 57–60); search features of latent criminal offences (Borchakovskyi, 2019, pp. 117–119).

Procedures for the detection of criminal offences related to illegal content on the Internet in the context of their legal and theoretical framework have been largely unsubstantiated.

The purpose of the article is to study the legal and theoretical framework for search activities to detect criminal offences related to illegal content on the Internet.

2. Legal and regulatory framework for countering cybercrime

Given the almost unlimited amount of Internet resources containing illegal, open-access content, law enforcement bodies can acquire and use it to counter crime. Law enforcement practice shows that offenders actively use social media as a platform for committing criminal offences, exert psychological influence on Internet users, manipulate their behaviour, finally, turning them into victims of crime. Therefore, the search for illegal content and the use of criminologically significant information on the Internet is of great importance for the detection and investigation of criminal offenses. An effective response to these offences requires the legal framework to clearly define the actors involved in countering and their functions to actively search for signs of criminal offences related to illegal content on the Internet. On the basis of these regulations, the necessary scientific research on their further practical implementation should be carried out.

Considering the need for active response to cybercrime, a strategic planning document was adopted on March 15, 2016, the Cyber Security Strategy of Ukraine (President of Ukraine, 2016). Later, the Laws of Ukraine, such as "On Basic Principles of Cyber Security of Ukraine" (Verkhovna Rada of Ukraine, 2017), "On National Security of Ukraine" (Verkhovna Rada of Ukraine, 2018), were adopted and legitimised the status of the Cyber Security Strategy. In the development and adoption of the Strategy, the leadership of the State took into account the trends in global security policy, since over the past five years, such strategies as strategic planning documents, have been adopted in virtually all States of the world (Dovhan, Doronin, 2017). Law of Ukraine "On Basic Principles of Cyber Security of Ukraine" (Verkhovna Rada of Ukraine, 2017) in its content and essence is a concept of the development of cyber security and cyber protection, defines the categorical and conceptual apparatus, objects, actors and principles of cyber security, objects of cyber protection, the structure of the National Cyber Security System and tasks of its main components, mechanisms of public-private and State-public partnership. The content of the provisions of the Law defines the legal and organisational framework for the provision of protection in cyberspace; the main objectives, areas and principles of public policy; the powers of the actors and the basic principles of coordination of their activities (Verkhovna Rada of Ukraine, 2017). The Strategy identifies the sphere of "ensuring cyber security and information resources security" out of "ensuring information security" and determines its priorities: development of the information infrastructure of the State; creation of a cyber security system, development of a Computer Emergency Response Team (CERT); monitoring

of cyberspace with a view to timely detection, prevention and neutralisation of cyber-threats; development of law enforcement investigative capabilities (it should be noted that investigation itself, not detection – *O. T.*) cybercrime; ensuring the security of objects of critical infrastructure, state information resources from cyberattacks, protection of state information resources, electronic government systems, technical and cryptographic protection of information. Both the Strategy and the Law identify elements of the cyber security system, their common functions and tasks, but the organisation of their interaction is almost undefined, that is, it is implied that this should be governed at the level of legal regulations (in particular by-laws) of executive authorities. In view of this, it should be noted that although the Cyber Security Strategy, its general issues have already been addressed and are in the process of being implemented, but a number of practical implementation issues remain unaddressed, given the near absence of a system to detect both general criminal offences committed in cyberspace and those committed in the flow of illegal content on the Internet.

It can be stated that the legal framework for countering cybercrime is established but the important (given the latency of criminal offences related to illegal content on the Internet) issue of active search for their signs remains.

Information on these criminal offences can be obtained from different sources. This may include statements and reports from citizens, enterprises, institutions and organisations, officials, and authorities on the preparation of a criminal offence. In some cases, such information may lead to criminal proceedings for preparation of a criminal offence. However, given that only 10% of the facts of these actions become known to law enforcement bodies, the spread of these criminal offences can have serious, and sometimes even irreparable consequences for the state. The latency of criminal offences related to illegal content on the Internet requires adequate measures to detect them. These factors necessitate the development and scientific substantiation of tactics for detecting the signs of these offences.

3. Features of detection of criminal offences related to illegal content on the Internet

In recent decades, the main source of primary information on the illegal activities of individuals has been the use of confidential information, as well as the acquisition of information from open sources through personal searches by operational units. In the future, the sources of information on illegal activities of persons have included the application of measures on audio and video control of a person, removal of information from transport telecommunication networks, removal of information from electronic information systems, locating of the radio electronic device, etc. However, these means of obtaining information are used either as part of operative-search activities (grounded on the existence of information about a criminal offence being prepared), or as part of covert investigative (search) actions during the pretrial investigation (grounded on the availability of information on the criminal offence that has been or is being committed). That is, the need of law enforcement bodies to use tools that do not restrict the constitutional rights of citizens does not meet the possibilities of obtaining primary information. These features determine the meaningful content of each of search elements when detecting criminal offences related to illegal content on the Internet.

Research on tactics of detection of criminal offenses, carried out in several areas. Basically, researchers in tactics of detection of criminal offenses distinguish two levels: operative-search and investigative, in accordance with which they consider the methodology of pre-investigative operative-search acquisition and accumulation of primary (intelligence) information to initiate an investigation (about criminal activities) and direct investigation methodology. N.P. Yablokov substantiates this theory and argues that the investigation is preceded by a different in terms of time operative search examination of criminal activities, which ends with the transferring of the collected primary information to the investigative bodies or the operation to apprehend suspects (Filippov, 2007, pp. 315–316). According to V.A. Nekrasov, the search activities contain interrelated systems: a well-founded system of features indicating the presence of a certain type of criminal offenses; a system of overt and covert investigative (search) actions to detect such criminal offences (Nekrasov et al., 2008, p. 51). V.H. Petrosian asserts that search activities include the following components: detection of information (data) about committed criminal offenses or preparations for their commission; detection (establishment) of documents and objects, indicating the content of criminal activities or containing indications of such activities; detection (establishment) of persons (incl. legal) who are involved in the commission or preparation of criminal activities, or who may be identified as suspects, witnesses or victims (Petrosian, 2012, p. 129).

Research developments on the topic of our article, that is, detection of criminal offences related to illegal content on the Internet, have been carried out sporadically, as part of the study of other topics.

The first area is their identification in the context of countering illegal actions in high technology, which is revealed in the context of the scientific substantiation of cyber security: O.O. Bakalinska, O.O. Bakalynskyi analyse the prerequisites and features of the formation of the legislation of Ukraine in the field of cyber security, identify the challenges and prospects for its further development in terms of assessing existing risks and threats, highlight the areas of adaptation of domestic cyber security legislation to EU standards under the Association Agreement between Ukraine and the EU (Bakalinska, Bakalynskyi, 2019, pp. 100–109); V.Yu. Bykov, A.Yu. Burov, N.P. Dementiievska consider the cyber security processes from the technical aspects of identifying threats to the protection of information resources (Bykov et al., 2019, pp. 313–331).

A number of scholars consider the procedures for detecting criminal offences by means of criminal technology of illegal content on the Internet: plastic payment cards (Nikolaiuk et al., 2007); computer fraud (Komar, 2013, pp. 168–175) (during which certain elements of the search activity are identified, in particular persons as the object of search activity (Komar, 2011, pp. 146–148).

No more modern research on the basic issues of the theory of detection of criminal offences related to illegal content on the Internet, except one by the author (Tarasenko, 2021), has been carried out, because other scientists use the existing studies, extrapolating them into their own research.

4. Conclusions

Therefore, the regulatory and legal framework for the prevention of illegal content on the Internet, in particular in social networks, the creation of a security mechanism to prevent the impact of illegal content on children, as well as the identification of persons who distribute illegal content have been provided. Moreover, the consideration and analysis of scientific studies on selected issues related to the system of detection of the investigated category of criminal offences, forensic support for the investigation of criminal offences committed with the use of information and telecommunication systems, legal protection of public relations in the field of the inviolable functioning of such systems, as well as the prompt response to these types of criminal offences reveals the need for further research and scientific solution of theoretical and organisational tasks arising in the detection of criminal offences related to illegal content on the Internet.

References:

Bakalinska, O.O., Bakalynskyi, O.O. (2019). Pravove zabezpechennia kiberbezpeky v Ukraini [Legal support of cyber security in Ukraine]. *Pidpryiemnytstvo, hospodarstvo i pravo – Entrepreneurship, economy and law*, no. 9, pp. 100–109 [in Ukrainian].

Belkin, R.S. (2001). *Kurs kriminalistiki: uchebnoe posobie dlya vuzov [Forensic course: textbook for universities]*, in 3 vols. Moscow: Yuniti [in Russian].

Borchakovskyi, M.B. (2017). *Osoby yak obiekt poshukovoi diialnosti pid chas vyiavlennia latentnykh kryminalnykh pravoporushen [Individuals as the object of search activities in the detection of latent criminal offenses]*. Kyiv: Fundatsiia naukovtsiv ta osvitian [in Ukrainian].

Borchakovskyi, M.B. (2018). Obiekty poshukovoi diialnosti pid chas vyiavlennia latentnykh kryminalnykh pravoporushen [Objects of search activity during detection of latent criminal offenses]. *Aktualni problemy operatyvno-rozshukovoi diialnosti ta vykorystannia spetsialnoi tekhniky [Actual problems of operative-search activity and use of special equipment]*, pp. 140–142 [in Ukrainian].

Borchakovskyi, M.B. (2019). *Poshukovi oznaky latentnykh kryminalnykh pravoporushen [Search signs of latent criminal offenses]*. Kryvyi Rih: KF DDUVS [in Ukrainian].

Bykov, V.Yu., Burov, O.Yu., Dementiievska, N.P. (2019). Kiberbezpeka v tsyfrovomu navchalnomu seredovyshchi [Cyber security in the digital learning environment]. *Informatsiini tekhnolohii i zasoby navchannia – Information technologies and teaching aids*, no. 2, pp. 313–331 [in Ukrainian].

Cabinet of Ministers of Ukraine (2017). Pro skhvalennia Kontseptsii stvorennia derzhavnoi systemy zakhystu krytychnoi infrastruktury: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 6 hrudnia 2017 r. № 1009-p [On approval of the Concept of creation of the state system of protection of critical infrastructure: Order of the Cabinet of Ministers of Ukraine dated December 6, 2017 № 1009-p]. Retrieved from: https://zakon.rada.gov.ua/laws/show/1009-2017-p#Text [in Ukrainian].

Dovhan, O.D., Doronin, I.M. (2017). *Eskalatsiia kiberzahroz natsionalnym interesam Ukrainy ta pravovi aspekty kiberzakhystu [Escalation of cyber threats to the national interests of Ukraine and legal aspects of cyber defense]*. Kyiv: ArtEk [in Ukrainian].

Filippov, A.G. (ed.) (2007). *Kriminalistika: uchebnik [Criminalistics: textbook]*. Moscow [in Russian].

Komar, O.M. (2011). *Neobkhidnist kontroliu derzhavy za vykorystanniam kompiuternykh prohram yak diievyi zasib protydii shakhraistvu u sferi vysokykh tekhnolohii [The need for state control over the use of computer programs as an effective means of combating fraud in the field of high technology]*. Kirovohrad: KIuI KhNUVS [in Ukrainian].

Komar, O.M. (2013). Spryiannia operatyvnym pidrozdilam MVS Ukrainy shchodo protydii shakhraistvam, uchyniuvanym z vykorystanniam elektronno-obchysliuvalnoi tekhniky [Assistance to operational units

of the Ministry of Internal Affairs of Ukraine in combating fraud committed using electronic computing equipment]. *Naukovyi visnyk Natsionalnoi akademii vnutrishnikh sprav – Scientific Bulletin of the National Academy of Internal Affairs*, no. 1, pp. 168–175 [in Ukrainian].

Nekrasov, V.A., Borets, L.V., Myronenko, S.Yu. (2008). *Vyiavlennia lehalizatsii (vidmyvannia) dokhodiv, oderzhanykh zlochynnym shliakhom (operatyvno-rozshukovyi aspekt) [Detection of legalisation (laundering) of proceeds from crime (operational and investigative aspect)].* Kyiv: Skif [in Ukrainian].

Nikolaiuk, S.I., Nykyforchuk, D.I., Tymchenko, L.L. (2007). *Protydiia zlochynam, shcho vchyniuiutsia iz vykorystanniam plastykovykh platizhnykh kartok [Counteraction to crimes committed with the use of plastic payment cards].* Kyiv: KNT [in Ukrainian].

Petrosian, V.H. (2012). Kryminalistychne ta operatyvno-rozshukove zabezpechennia vyiavlennia zlochyniv, vchynenykh subiektamy hospodariuvannia z oznakamy fiktyvnosti [Forensic and operational-search support for detection of crimes committed by business entities with signs of fictitiousness]. *Extended abstract of candidate's thesis*. Irpin [in Ukrainian].

President of Ukraine (2016). Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku "Pro Stratehiiu kiberbezpeky Ukrainy": Ukaz Prezydenta Ukrainy vid 15 bereznia 2016 r. № 96/2016 [On the decision of the National Security and Defense Council of Ukraine dated January 27, 2016 "On the Cybersecurity Strategy of Ukraine": Decree of the President of Ukraine dated March 15, 2016 № 96/2016]. Retrieved from: https://zakon.rada.gov.ua/laws/show/96/2016 [in Ukrainian].

Shapovalov, O.O. (2015). Pravovi zasady operatyvnoho poshuku [Legal bases of operative search]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia "Pravo" – Scientific Bulletin of Uzhhorod National University. Series "Law"*, iss. 33, pp. 147–151 [in Ukrainian].

Shapovalov, O.O. (2018). Sfery ta mistsia poshukovoi diialnosti operatyvnykh pidrozdiliv [Areas and places of search activities of operational units]. *Yurydychnyi chasopys Natsionalnoi akademii vnutrishnikh sprav – Scientific Journal of the National Academy of Internal Affairs*, vol. 8, no. 1, pp. 304–314 [in Ukrainian].

Tarasenko, O.S. (2021). *Teoriia ta praktyka protydii kryminalnym pravoporushenniam, poviazanym z obihom protypravnoho kontentu v merezhi Internet [Theory and practice of combating criminal offenses related to the circulation of illegal content on the Internet].* Kyiv: National Academy of Internal Affairs [in Ukrainian].

Verkhovna Rada of Ukraine (2017). Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 5 zhovtnia 2017 r. № 2163-VIII [On Basic Principles of Cyber Security of Ukraine: Law of Ukraine dated October 5, 2017 № 2163-VIII]. Retrieved from: https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].

Verkhovna Rada of Ukraine (2018). Pro natsionalnu bezpeku Ukrainy: Zakon Ukrainy vid 21 chervnia 2018 r. № 2469-VIII [On National Security of Ukraine: Law of Ukraine dated June 21, 2018 № 2469-VIII]. Retrieved from: https://zakon.rada.gov.ua/laws/show/2469-19#Text [in Ukrainian].

Yermakov, Yu.O. (2020). Predmety yak materialni slidy ta obiekty poshukovoi diialnosti pid chas vyiavlennia kryminalnykh pravoporushen u sferi vykorystannia ta okhorony nadr [Items such as material traces and objects of search activity during the detection of criminal offenses in the field of subsoil use and protection]. *Yurydychna nauka – Legal science*, no. 6, pp. 177–181 [in Ukrainian].

Олег Тарасенко,
доктор юридичних наук, доцент, професор кафедри оперативно-розшукової діяльності, Національна академія внутрішніх справ, площа Солом'янська, 1, Київ, Україна, індекс 03035, o.s.tarasenko@gmail.com
ORCID: *orcid.org/0000-0002-3179-0143*

ПРАВОВЕ ТА ТЕОРЕТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПОШУКОВОЇ ДІЯЛЬНОСТІ ЩОДО ВИЯВЛЕННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ З ОБІГОМ ПРОТИПРАВНОГО КОНТЕНТУ В МЕРЕЖІ ІНТЕРНЕТ

Анотація. ***Мета статті*** – дослідити правове та теоретичне забезпечення пошукової діяльності щодо виявлення кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет.

Результати. У статті розглянуто та проаналізовано рівень забезпечення нормативно-правового регулювання недопущення обігу протиправного контенту в мережі Інтернет, зокрема в соціальних мережах, створення безпекового механізму недопущення впливу протиправного контенту на дітей, а також виявлення осіб, які поширюють протиправний контент. Розглянуто наукові дослідження стосовно тактики виявлення кримінальних правопорушень, які здійснювалися за декількома напрямами, та обґрунтовано думку про те, що дослідники в тактиці виявлення кримінальних правопорушень здебільшого виокремлюють два рівні (оперативно-розшуковий і слідчий), відповідно до яких розглядають методику дослідчого оперативно-розшукового здобування та нагромадження первинної (розвідувальної) інформації, що дає можливість почати розслідування (про злочинну діяльність), і методику безпосереднього розслідування.

Висновки. Згідно з результатами наукових досліджень, предметом яких були окремі питання, що стосувалися системи виявлення аналізованої категорії кримінальних правопорушень, криміналістичного забезпечення розслідування кримінальних правопорушень, які вчиняються з використанням інформаційно-телекомунікаційних систем, питання правової охорони суспільних відносин у сфері непорушного функціонування таких систем, а також оперативного забезпечення протидії зазначеним видам кримінальних правопорушень, варто зробити висновок про необхідність подальшого дослідження й наукового розв'язання теоретичних та організаційних завдань, які виникають під час виявлення кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет.

Ключові слова: мережа Інтернет, протиправний контент, обіг, кримінальні правопорушення, виявлення, правове забезпечення, теоретичне обґрунтування.

The article was submitted 18.07.2022
The article was revised 08.08.2022
The article was accepted 29.08.2022