UDC 343.1
DOI https://doi.org/10.32849/2663-5313/2022.8.15

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). Objects and measures of search during detection of criminal offenses related to illegal content on the Internet. *Entrepreneurship, Economy and Law*, 8, 94–99, doi: https://doi.org/10.32849/2663-5313/2022.8.15

OBJECTS AND MEASURES OF SEARCH DURING THE DETECTION OF CRIMINAL OFFENSES RELATED TO ILLEGAL CONTENT ON THE INTERNET

Abstract. ***Purpose.*** The purpose of the article is to identify the objects and measures of search during the detection of criminal offenses related to illegal content on the Internet. ***Results.*** It is noted that the objects of search during the detection of criminal offenses related to illegal content on the Internet include persons, items, documents and an optional object – electronic information. During detection of criminal offenses related to illegal content on the Internet, mainly measures involving the use of certain technical means and software, search algorithms (sources, means, search areas, tools and search procedures) and enabling the use of open sources and search services in order to collect information on illegal content on the Internet are applied. It is determined that the effectiveness of search for information that the searcher can use to detect, investigate an illegal act and expose the perpetrators is determined by two factors: effectiveness of the search engine used in the search process; experience of the person conducting the search (the experience of the person depends crucially on his/her awareness of modern search tools and techniques, as well as the skills of their effective use when working with search engines). ***Conclusions.*** It is concluded that the objects of search during the detection of criminal offenses related to illegal content on the Internet include persons, items, documents and an optional object – electronic information. During detection of criminal offenses related to illegal content on the Internet, mainly measures involving the use of certain technical means and software, search algorithms (sources, means, search areas, tools and search procedures) and enabling the use of open sources and search services in order to collect information on illegal content on the Internet are applied.

Key words: Internet, illegal content, circulation, criminal offenses, detection, search objects, search measures.

1. Introduction

According to the materials of the International Forums in Davos (2018–2019), the problem of cybersecurity, which affects almost all sectors of human life and activities, is increasingly acute (Bykov, Burov, Dementiievska, 2019, p. 313). The large-scale virus attack "WannaCry", which took place on May 12–13, 2017, affected tens of thousands of computers around the world: in the UK, a number of medical institutions across the country were forced to refuse to provide services to patients even in emergency cases due to the failure of most computer systems; in Spain, the Ministry of Energy and a telecommunications company were attacked; in Germany, the computers of the railway concern's dispatch centres were infected, resulting in the failure of dispatch control systems; in France, the automaker "Renault" was subjected to a large-scale cyberattack; in Portugal, the largest provider of telecommunication services "Portugal Telecom" suffered; computer systems of shopping and office centres, networks of hospitals and gas stations, postal service, railway stations, as well as government agencies were attacked (Dovhan, Doronin, 2017, p. 41). These actions become possible due to the uneven development of cybercrime capabilities (which in turn are based on the rapid spread of computer technology) and scientific, technical and legal support for the search activities of law enforcement agencies. Detection of illegal content and the use of criminologically significant information on the Internet is important

for the detection and investigation of criminal offenses. Given the virtually unlimited amount of Internet resources that contain illegal content in the public domain, law enforcement agencies can acquire and use it to combat crime. Relying on the analysis of the system of detection of criminal offenses related to illegal content on the Internet, it can be argued that law enforcement officers can already perform the task of searching for information on the Internet in the following areas: the search for information about the event (confirmation or refutation of information about the event, the search for the author of the information); the search for information about the person (identification of the person based on the available information, the search for the location of the identified person); systematic tracking of changes in the accounts of individuals or groups, comments to articles, publications, news, posts; systematic survey of Internet users (based on own and their anonymity) (Sumskyi, Romanko, 2016, p. 113). A number of issues remain unresolved related to the specification of search measures permitted in the detection of these offenses and the targets of these detective measures.

Previous research was carried out in two main areas. In the first area, scientists considered ways to detect certain criminal offenses in the field of computer technology: N.S. Kozak investigated the types and methods of tactical and forensic techniques for detecting computer crimes (Kozak, 2011); V.V. Poliakov systematised high-tech methods ensuring more effective conduct of investigative actions (Poliakov, 2008); D.M. Tsekhan came to the conclusion that the introduction of high information technologies in the practice of operational units determines the use of a technological approach to the detection of high-tech crimes (Tsekhan, 2011). In another area, scientists have developed a methodology for detecting individual criminal offenses, highlighting the elements of search activities: Yu.O. Yermakov singled out certain elements of search: items as material traces and objects of search activities during the detection of criminal offenses (Yermakov, 2020), documents evidencing criminal activity as an object of search for criminal offenses (Yermakov, 2020), methods of search activities during the detection of criminal offenses (Yermakov, 2019); O.O. Shapovalov identifies the objects of search activities (Shapovalov, 2018); persons of operational interest as the object of operational search (Shapovalov, 2016). As for the objects and search measures in the context of detecting criminal offenses related to illegal content on the Internet, no research has been carried out.

2. Categories of objects of search related to illegal content on the Internet

In our opinion, the objects of search during the detection of criminal offenses related to illegal content on the Internet include persons, items, documents and an optional object – electronic information (Tarasenko, 2021, pp. 284–294).

Allowing for the perspectives of scientists and the specifics of detecting criminal offenses related to illegal content on the Internet, we conditionally group persons (as an object of search activities) into the following categories:

1. Persons who may be involved in criminal activities: those who, due to the appropriate "criminal specialisation", can commit (commit) actions to create and/or disseminate illegal content on the Internet; who, as a result of their professional activities, have acquired knowledge in the field of computer technology and can apply them for the criminal purpose of committing offenses related to illegal content on the Internet; persons who have access to electronic computing equipment, through the use of which actions to create and/or disseminate illegal content on the Internet (such persons should be considered by subcategories (information managers (on the basis of a contract or on behalf of the owner of the information); system owners; system administrators (on the basis of the concluded agreement or on behalf of the system owner); users (consumers of information and telecommunication services); who, due to their professionalism, have the opportunity and motivation to commit actions to create and/or disseminate illegal content on the Internet.

2. Persons who, by virtue of their skills, abilities can assist in obtaining primary information, as well as assist law enforcement officers in identifying actions to create and/or disseminate illegal content on the Internet: professional programmers who develop software (white and black hackers); who maintain the Internet page, physical or virtual server; who study in the specialties "Cybersecurity", "Software Engineering", "Computer Engineering", "Computer Science", etc. (that is, these are persons who, if they have individual, professional skills, knowledge or skills, may have information about the commission of a criminal offense related to illegal content on the Internet, as well as provide advice on finding, fixing, removing illegal content).

3. Persons who, according to their functional duties, are responsible for detecting and recording illegal actions to create and/or disseminate illegal content on the Internet: who, according to their functional duties, are responsible for

detecting and recording illegal actions; who have relevant information, the analysis of which determines the effectiveness of detection; who, by virtue of their professional activities, may receive information about the commission of criminal offenses related to illegal content on the Internet: administrators of the Internet service provider (ISP); employees of service institutions for software configuration of information systems; employees of advertising companies that create content on Internet resources; employees of cinemas that control the implementation of illegal video recording of audiovisual works, which can be further posted on Internet resources), etc. (that is, these are persons who, due to the specifics of their work, are faced with the facts of committing illegal actions that may indicate the commission of an offense or the consequences of these actions may lead to the commission of the criminal offenses under investigation).

4. Persons who may have information about the facts of criminal activity: who may be aware of certain circumstances of the commission of criminal offenses (for example, from among the persons who were present during the commission of a criminal offense) and who can be further considered as witnesses (for example, who were present at certain actions, but were not aware of this fact); who have access to information about sources and ways of creating illegal content; who may have the necessary information: (individuals, representatives of a legal entity); representatives of regulatory authorities; witnesses of the illegal activities of the suspect, working with him/her at the same enterprise, but in other departments, have information about the activities of criminals, their lifestyle, social circle, episodes of criminal activities.

The next type of detection objects is documents. These documents can be conditionally grouped into:

1. Documents that contain content illegally distributed by anyone on the Internet.

2. Documents evidencing the performance of the actor whose technical capabilities or information resources were used in the process of creating and/or disseminating illegal content (copies of the entitlement document of the Internet provider and the agreement on the provision of access to the Internet, as well as materials related to the committed criminal offense (log files; statistics on the download of the dedicated channel of the provider; certificates on who was allocated the established dynamic (or static) IP addresses during the recorded illegal actions, etc.

3. Documents proving that certain technical, hardware and software means belong to certain persons (confirming the right of ownership, i.e. the right to own, dispose of or use computer information, computer, computer system or their network: a written contract for the receipt of Internet services, telecommunications by a specific subscriber number or bank card service in a particular financial institution; a document on the right of ownership (use) of computer software, database, electronic resource of the Internet; documents containing personal data of the person who owns a particular mobile number; certificate from the telecommunications operator or Internet service provider on belonging to the circle of subscribers served; contracts for the provision of telecommunication services and access to the Internet; bills for the communication services provided; technical documentation reflecting the facts of the subscriber's appeal on the services provided to him/her (applications for line repair, etc.).

4. Documents that reflect the actor's work with specific content – the subject matter of a criminal offense, computer or computer system (computer operator's logs, electronic logs of operations, electronic register of subscriber connections in the computer network or telecommunications (Internet); accounting journals (working hours, access to computer equipment, its failures and repairs, registration of users of a computer system or network); license agreements and contracts for the use of computer software products, hardware and their development; password books for access to the automated system; orders and other documents regulating the use of the automated system, etc. (Nikolaiuk, Nykyforchuk, Tymchenko, 2007, pp. 46).

5. Documents confirming the fact of concluding a contractual relationship with a mobile operator (contract for the provision of communication services, additional agreement to the contract, according to which mobile operators are provided with discounts on mobile phones); certificates from Internet providers about the client who uses a certain place of Internet access; relevant documentation on time accounting and payment for Internet services; contract for Internet services; receipt of payment for Internet services.

The list of these documents can be significantly expanded depending on the forms of criminal activity and the way illegal content is used in the commission of a particular criminal offense.

3. Specificities of items as objects of detection of criminal offenses related to illegal content on the Internet

The items as objects of detection include:

– Hardware and technical means: computers; laptops; various machine media; resources of network service providers (Internet provid-

ers) and information services provided by them (e-mail, www-service); special technical means of obtaining information; various types of printing devices (printers, thermal printers, imprinters); various machine data carriers (floppy disks, disks, magnetic tapes of payment cards); keyboard (fingerprints); external storage devices; individual data carriers (CDs, floppy disks, flash memory devices, etc.).

– User manuals for components and devices; software description.

– Items that were directly used in the preparation and commission of illegal actions (for example: a mobile phone, which is an item that can be identified with a sufficiently high level of confidence, and therefore this circumstance can be used both to prove that the mobile device belongs to a certain person and to prove the fact of content dissemination using a particular phone).

– Items that are the result of criminal actions and can be divided into two blocks: money and material values obtained as a result of a criminal offense; items that indicate the receipt of funds or material values.

– Items that contain signs of a criminal offense (notebooks of criminals with information about computer devices, account numbers, etc., printouts from the printer with similar information; sheets with the offender's notes (names, passwords, addresses, etc.) (attached to the monitor, near the keyboard, under it, in the garbage, etc.); flash cards; components, parts that were used to create special technical means.

– Items that indicate the creation and purpose of using illegal content.

– Software tools used for content processing and manipulation (computer data carriers with software), stolen databases; malicious programs used for unauthorised access to databases or other information resources; software for the operation of peripheral equipment; Internet protocols, most commonly used website and e-mail addresses, e-mail messages (Osyka, 2006, pp. 44).

– Items that indicate appropriate intellectual preparation for the commission of a criminal offense (methodological literature; expert advice; addresses of accomplices (these can be both physical addresses and e-mail, ICQ numbers, etc.), including addresses of any sites and forums where offenders specialising in committing criminal offenses of this type communicate, their correspondence (letters in paper or electronic form) (Reutskyi, 2009, p. 156).

In our opinion, search measures during the detection of criminal offenses related to illegal content on the Internet include:

– Analysis of official reports of state bodies, appeals of citizens about illegal actions.

– Analysis of materials of criminal proceedings on criminal offenses, during the commission of which illegal content was used.

– Study of the information contained in the trace pattern (upon receipt of a report of a criminal offense related to the use of illegal content) (traces on the media used by the offender (hard drives, magnetic and optical media, etc.); traces on "transit" magnetic media, through which the offender directly established a connection with information resources; traces on the victim's magnetic media, namely traces of unauthorised access and unauthorised influence on software and information resources).

– Media monitoring.

– Monitoring of the Internet (Ukrainian sector).

– Obtaining information directly from mobile operators.

– Analysis of information from mobile operators on individual legal entities with whom a contract for the use of a cellular number has been concluded.

– Obtaining information from service providers (if the subject is a temporary user of the network or telecommunications facilities (for example, in PLMN – roaming; in telephone systems – UPT and telephone cards; in Internet services – remote access through other service providers, etc.); when an entity can use certain features to route a communication to other telecommunication services or equipment, including a communication that passes through more than one network operator/service provider before being terminated (Borysova, 2007, p. 106).

– Computer intelligence on the Internet. Given that the information posted and circulating in this network is not subject to legal regulation, computer intelligence can be formally carried out both directly by the forces and means of the CID and through business entities. If conducted by own forces, intelligence programs, which differ from other search and analytical programs in the presence of specific functions aimed at solving purely intelligence tasks, are used (Ovchinskij, 2011, p. 326).

– Analysis of "sites" on the Internet with information on the availability of technologies for creating and using illegal content for committing criminal offenses with further identification and verification of persons who have accessed these sites.

– Data search in telecommunication systems, which consists in detecting data stored in computer memory and is carried out using system functions or special computer programs.

– Use of special programs that during the work of a person monitor the protocols of his/her actions and receive data on the

IP address of this person's access to the Internet, provide an opportunity to obtain a list of contacts of this person and files of his/her communication history with the content of incoming and outgoing messages (Anapolska, 2011).

– Submission of requests using the capabilities of Interpol NCB (such requests may provide information on network addressees, names of domains and servers of organisations and users, electronic information blocked in the manner of operational interaction, providers and distributors of network and telecommunications services, individuals and legal entities involved in criminal offenses (official name of legal entities registered abroad, their legal address, number, date of registration; areas of activities, size of the authorised capital, current financial condition of the legal entity; surnames and names of individuals-managers (founders, shareholders); information on illegal activities of individuals and legal entities, etc.) (Anapolska, 2011, p. 95).

The effectiveness of the search for information that the searcher can use to detect, investigate an illegal act and expose the perpetrators is determined by two factors: effectiveness of the search engine used in the search process; experience of the person conducting the search (the experience of the person depends crucially on his/her awareness of modern search tools and techniques, as well as the skills of their effective use when working with search engines).

4. Conclusions

It is concluded that the objects of detection of criminal offenses related to illegal content on the Internet include persons, items, documents and an optional object – electronic information. During detection of criminal offenses related to illegal content on the Internet, mainly measures involving the use of certain technical means and software, search algorithms (sources, means, search areas, tools and search procedures) and enabling the use of open sources and search services in order to collect information on illegal content on the Internet are applied.

References:

Anapolska, A.I. (2011). Rozsliduvannia shakhraistv i poviazanykh iz nymy zlochyniv, vchynenykh u sferi funktsionuvannia elektronnykh rozrakhunkiv [Investigation of fraud and related crimes committed in the field of electronic payments]. *Candidate's thesis dys.* Kharkiv (in Ukrainian).

Borysova, L.V. (2007). Transnatsionalni kompiuterni zlochyny yak obiekt kryminalistychnoho doslidzhennia [Transnational computer crime as a subject of forensic investigation]. *Candidate's thesis.* Kyiv (in Ukrainian).

Bykov, V.Iu., Burov, O.Iu., Dementiievska, N.P. (2019). Kiberbezpeka v tsyfrovomu navchalnomu seredovyshchi [Cybersecurity in the digital learning environment]. *Informatsiini tekhnolohii i zasoby navchannia – Information technologies and teaching aids, 2,* 313–331 (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: Vydavnychyi dim «ArtEk» (in Ukrainian).

Yermakov, Yu.O. (2019). Metody poshukovoi diialnosti pid chas vyiavlennia kryminalnykh pravoporushen u sferi okhorony ta vykorystannia nadr [Methods of search activities in the detection of criminal offenses in the field of protection and use of subsoil]. *Aktualni problemy operatyvno-rozshukovoi protydii zlochynam – Actual problems of operative-search counteraction to crimes, 2,* 137–138 (in Ukrainian).

Yermakov, Yu.O. (2020). Dokumenty, shcho svidchat pro zlochynnu diialnist, yak obiekt poshuku kryminalnykh pravoporushen u sferi okhorony ta vykorystannia nadr [Documents proving criminal activity as an object of search for criminal offenses in the field of protection and use of subsoil]. *Aktualni problemy kryminalnoho prava. Current issues of criminal law, 3,* 337–340 (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 activities during the detection of criminal offenses in the field of subsoil use and protection]. *Yurydychna nauka – Legal science, 6,* 177–181 (in Ukrainian).

Kozak, N.S. (2011). Kryminalistychni pryiomy, sposoby i zasoby vyiavlennia, rozkryttia ta rozsliduvannia kompiuternykh zlochyniv [Forensic techniques, methods and means of detecting, detecting and investigating computer crimes]. *Extended abstract of candidate's thesis.* Irpin: Nats. un-t derzh. podatk. sluzhby Ukrainy (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).

Osyka, I.M. (2006). *Rozsliduvannia nezakonnykh dii z bankivskymy platizhnymy kartkamy: metodychni rekomendatsii [Investigation of illegal activities with bank payment cards: methodological recommendations].* Kharkiv: KhNUVS (in Ukrainian).

Ovchinskij, S.S. (2011). Operativno-rozysknaja informacija [Operational-search information]. Moskva: INFRA-MJu (in Russian).

Poliakov, V.V. (2008). Osobennosti rassledovanija nepravomernogo udalennogo dostupa k komp'juternoj informacii [Features of consideration of illegal remote access to computer information]. *Candidate's thesis.* Barnaul (in Russian).

Reutskyi, A.V. (2009). Metodyka rozsliduvannia zlochyniv u sferi vyhotovlennia ta obihu platizhnykh kartok [Methodology for investigating mischief in the sphere of preparing and processing payment cards]. *Candidate's thesis*. Kharkiv.

Shapovalov, O.O. (2016). Osoby, shcho stanovliat operatyvnyi interes yak obiekt operatyvnoho poshuku [Persons of operational interest as an object of operational search]. *Intehratsiia yurydychnoi nauky i praktyky yak osnova staloho rozvytku vitchyznianoho zakonodavstva – Integration of legal science and practice as a basis for sustainable development of domestic legislation, 2*, 245–247 (in Ukrainian).

Shapovalov, O.O. (2018). Obiekty poshukovoi diialnosti operatyvnykh pidrozdiliv [Objects of search activities of operational divisions]. *Nauk. visnyk NAVS – Scientific Bulletin of the NAVS*, 1, 255–264 (in Ukrainian).

Sumskyi, S.A., Romanko, P.S. (2016). Shchodo rozvidky z vidkrytykh dzherel u merezhi zahalnoho korystuvannia – Internet [Regarding intelligence from open sources in the public network – the Internet]. *Kryminalna rozvidka: metodolohiia, zakonodavstvo,zarubizhnyi dosvid – Criminal intelligence: methodology, legislation, foreign experience*, 111–113 (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 illegal content on the Internet]*. Kyiv: Natsionalna akademiia vnutrishnikh sprav (in Ukrainian).

Tsekhan, D.M. (2011). *Vykorystannia vysokykh informatsiinykh tekhnolohii v operatyvnorozshukovii diialnosti orhaniv vnutrishnikh sprav [The use of high information technology in the operational search activities of law enforcement agencies*]. Odesa: Yuryd. lit-ra (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*

ОБ'ЄКТИ ТА ЗАХОДИ ПОШУКУ ПІД ЧАС ВИЯВЛЕННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ З ОБІГОМ ПРОТИПРАВНОГО КОНТЕНТУ В МЕРЕЖІ ІНТЕРНЕТ

Анотація. ***Мета.*** Мета статті – виокремити об'єкти та заходи пошуку під час виявлення кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет. ***Результати.*** Зазначено, що до об'єктів пошуку під час виявлення ознак кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, належать особи, предмети, документи та факультативний об'єкт – електронна інформація. У процесі виявлення кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, застосовуються переважно заходи, що передбачають використання певних технічних засобів, програмного забезпечення, алгоритмів пошукових дій (джерела, засоби, напрями пошуку, інструментарій та процедури пошуку) та забезпечують можливість використання відкритих джерел та пошукових сервісів з метою здійснення збору інформації про обіг протиправного контенту в мережі Інтернет. Визначено, що результативність пошуку інформації, яку суб'єкт пошуку може використати для виявлення, розслідування протиправного діяння та викриття винних осіб, визначається двома чинниками: ефективність пошукової системи, використовуваної в процесі пошуку; досвідченість особи, яка здійснює пошук (досвідченість особи визначальним чином залежить від її обізнаності в сучасному інструментарії й прийомах пошуку, а також у навичках їх ефективного використання під час роботи з пошуковими системами). ***Висновки.*** Зроблено висновок, що до об'єктів виявлення ознак кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, належать особи, предмети, документи та факультативний об'єкт – електронна інформація. У процесі виявлення кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, застосовуються переважно заходи, що передбачають використання певних технічних засобів, програмного забезпечення, алгоритмів пошукових дій (джерела, засоби, напрями пошуку, інструментарій та процедури пошуку) та забезпечують можливість використання відкритих джерел та пошукових сервісів з метою здійснення збору інформації про обіг протиправного контенту в мережі Інтернет.

Ключові слова: мережа Інтернет, протиправний контент, обіг, кримінальні правопорушення, виявлення, об'єкти пошуку, пошукові заходи.

The article was submitted 21.07.2022
The article was revised 11.08.2022
The article was accepted 30.08.2022