Volodymyr BARANYAK

Lviv Polytechnic National University,
Educational and Rasearch Institute of Law,
Psychology and Innovative Education,
Associate Professor of the Criminal Law
and Procedure Department,
Candidate of Chemical Sciences, Associate Professor
volodymyr.m.baraniak@lpnu.ua
ORCID iD: https://orcid.org/ 0000-0001-6161-7862

DIGITAL FORENSICS IN THE CONTEXT OF DIGITALISATION OF MODERN SOCIETY

The author substantiates the relevance of digital forensics in the context of digitalisation of modern society, notes the active use of digital technologies in solving various types of illegal activities in the field of computer information, and defines the concepts of «digital trace» and «digital forensics».

The author emphasises the need to develop new knowledge and developments in forensic techniques, standards and principles for evaluating and verifying collected evidence (digital traces), to carry out mandatory standardisation when working with digital information, and to consider and develop appropriate methodology for training specialists in the field of digital forensics.

Attention is focused on ethical, legal and privacy issues related to the collection and use of digital data during an investigation, confidentiality and protection of personal information of persons not involved in a criminal offence, compliance of the collection and use of digital data during an investigation with certain legal norms and standards (obtaining court orders for evidence collection, requirements for information storage, observance of the rights and freedoms of persons under investigation), ensuring an appropriate level of protection, storage and transmission of personal information and restricting access to it only on certain grounds.

The role of forensics in improving and increasing the effectiveness of the fight against modern crime, including war and cybercrime, through the active use of digital technologies is emphasised.

Keywords: digitalisation, digital traces, digital forensics, standardisation, privacy.

Formulation of the problem. Today, the development of advanced digital technologies in modern society implies their mandatory implementation in various areas of social relations. However, along with the development of the digital economy, it is necessary to note the active use of digital technologies in solving various types of illegal activities by criminals.

Criminal offences related to information and communication technologies or in the field of computer information are becoming more and more common. That is why, in recent years, the proportion of criminal offences committed with the use of high information technologies has increased. The legislator has provided for a separate Chapter XVI in the Criminal Code of Ukraine, which emphasises the relevance and danger of criminal offences in the field of digital technologies [1].

Analysis of the study of the problem. Today, the development of advanced digital technologies in modern society implies their mandatory implementation in various areas of social relations. However, along with the development of the digital economy, it is necessary to note the active use of digital technologies in solving various types of illegal activities by criminals.

The issues of theoretical and methodological aspects of digital forensics and forensic examination in the digital age have been studied by such domestic scholars as S. Buzyna, R. Kravchenko, I. Petrova, V. Shepitko, I. Goliash, S. Yevdokimenko, I. Rohatuk, G. Avdeyeva and others.

The purpose of the article is to substantiate the relevance of digital forensics in the context of digitalisation of modern society.

Presenting main material. Legal regulation of Ukraine's digital transformation is at an early stage of development. At the same time, the accumulated experience, practical results of digital transformation, as well as the large existing body of legislation in the field of information technology, allow us to assess the current state and prospects for the development of law in the field of digital transformation [2].

Electronic means of payment are increasingly being used and enable financial transactions. At the same time, electronic funds are not sufficiently protected from illegal encroachments by criminals. The most common method of fraud is for criminals to obtain an electronic wallet password through unauthorised interference with electronic computers.

In situations where criminal offences are committed by means of remote access, the evidence base, i.e. the presence of trace evidence that reflects the characteristics of the object that left them (fingerprints, breakage marks, wheel prints, etc.), is significantly reduced. However, when committing fraudulent acts with the use of digital technologies, a new type of traces appears - digital traces of a criminal offence. A digital trace should be understood as a unique set of actions that have been committed in the information and telecommunications space, as well as information left as a result of browsing the web [3].

Taking all of the above into account, it can be concluded that digital forensics includes the detection, collection and analysis of electronic traces in order to combat cybercrime. A computer or smartphone may be an instrument or means of committing an unlawful act, or the subject of a criminal offence, or may be used to store important electronic evidence of a criminal offence.

Modern forensics must adapt to the level of development of modern technologies in order to facilitate law enforcement activities. As of today, the term «digital forensics» is often mentioned. This is due to the fact that the commission of criminal offences with the use of digital devices leaves electronic traces in them, and secondly, because pre-trial investigation bodies have technical and forensic means (personal computers) that allow them to produce procedural documents in electronic form on electronic media.

The emergence of the concept of «digital forensics» has made it possible to distinguish independent areas of forensic examination. Depending on the source, other terms such as «computer forensics» or «computer systems forensics» are also used to refer to this field. At the same time, some scientists consider computer forensics as an applied science for the investigation of crimes (incidents) related to computer information, examination of digital evidence, as well as research, obtaining and recording of these methods of evidence.

In addition, forensic science is actively developing in the context of digitalisation and the expansion of knowledge about digitalisation [4]. Digital evidence requires new ways of collecting, storing, using and verifying evidence in criminal proceedings. When using digital evidence, the principles of professional training, expert assistance and reasonable care should be followed. It must be verified and authenticated. Digital evidence, in particular, poses unique challenges for authentication compared to traditional evidence due to the volume, speed, variability and vulnerability of the data available.

In the modern world, digital forensics is a new type of activity aimed at working with digital traces of offences. The development of new standards and principles for the evaluation and verification of collected evidence (digital traces) requires new knowledge and developments in forensic technology [5].

Avdeyeva G. K. notes that digital traces in forensics are imperceptible material traces that contain important forensic information stored in digital form on various material carriers. These traces can be detected, recorded and examined using specialised digital devices.

The main sources of digital footprints are various tangible digital information carriers, such as computers, integrated circuits, microcontrollers, telecommunications network equipment, digital cameras, voice recorders, plastic card readers, mobile phones and tablets. Some electronic components of these devices can even store information about the place and time of their use. For example, a geolocation system can be used to pinpoint the exact location of a computer, tablet or mobile phone in real time, including information about their owners. Geolocation data can also be used to establish the fact of the simultaneous presence of two or more people in one place, which may indicate their interaction [3, p. 91-92].

The main problem with collecting digital traces is that they can change instantly, making them visually invisible, and they can only be detected and recorded using special methods and special computer equipment. After the collection of computer information, it must be stored unchanged, which is the primary task of forensic research, only if these rules are followed, the information will have evidentiary value [5].

Cybercrime often involves direct attacks on computers and other similar devices to disable them. Sometimes, the attacked computers are used to spread malware, computer viruses, illegal information, various kinds of images, and cyberbullying. The legal literature distinguishes the following types of cybercrime: mercenary cybercrime (including phishing, cyber extortion, financial fraud, etc.); personal data theft; cyber espionage; copyright infringement and some others.

When considering them, it should be borne in mind that in modern conditions, «non-traditional» types of property, including websites, cryptocurrencies, mobile communication technologies, Internet property, etc. are actively entering the legal economic circulation. As they have the ability to generate high incomes, the criminal environment reacts accordingly. As a result, new types of criminal offences are emerging.

Issues and challenges arising in the field of digital forensics include ethical, legal and privacy issues related to the collection and use of digital data during an investigation. Ethical aspects include the duty to respect the confidentiality and protect the personal information of individuals who are not involved in a criminal offence. It is also important to avoid misuse of digital data for personal gain or political manipulation. Furthermore, the collection and use of digital data during an investigation must comply with clearly defined legal norms and standards.

This includes issues such as obtaining court orders to collect evidence, requirements for the retention of information, and respect for the rights and freedoms of persons under investigation. Failure to comply with legal regulations can lead to illegal data collection and violations of citizens' rights. The collection and analysis of digital data may violate the privacy and confidentiality of individuals whose data is collected. It is important to ensure an adequate level of protection of personal information and to restrict access to it only on certain grounds. This also applies to the storage and transmission of this data to ensure its security.

Today, forensic science is in line with the development of digital technologies, creating means and methods for extracting forensically relevant information from a new type of media. Thanks to scientific and technological progress, it is possible to use digital technologies in law enforcement, which accelerates the process of pre-trial investigation, allows for a more complete formation of the evidence base in the investigation of criminal offences, and subsequently ensures the quality of the trial of criminal proceedings.

In today's military realities, the main task of forensic science is to develop and apply tools, techniques and methods that allow collecting, investigating and using evidence in the context of war and global threats. The system of pre-trial investigation bodies, prosecutors, and criminal justice authorities face new challenges related to the need for rapid, comprehensive and high-quality documentation and collection of evidence of mass criminal violations of international humanitarian law, including ensuring the security environment in Ukraine, which has chosen the European course of development and is currently confronting the military aggression of the Russian occupation forces.

Today, there is an urgent need to increase the role of forensics in promoting and ensuring security in our country, as well as in improving and increasing the effectiveness of the fight against modern crime, including war and cybercrime, through the active use of digital technologies. In this context, a new scientific field, digital forensics, is emerging.

In military realities, artificial intelligence technologies have taken a central place in digital forensics to ensure the security environment in Ukraine and collect evidence of war crimes. In modern warfare conditions, the following areas of digital forensics are of particular importance: obtaining information from mobile devices of seized phones from participants in criminal proceedings; obtaining information from personal computers of individuals and legal entities; obtaining information from servers and other storage devices in organisations and institutions; obtaining information on radio frequency identifiers, GPS trackers, sensors, stationary and mobile measuring devices using geo-location, video surveillance and positioning systems; obtaining information from network services that establish voice and video communication between computers via the Internet, such as ICQ, Skype, WhatsApp, Viber, Telegram and others; obtaining information from banking systems on appropriate digital media (SD-disks, flash cards, etc.).); obtaining information from cellular operators on the details of subscriber communications and establishing the subscriber's location by geolocation; obtaining information from CCTV cameras of various commercial and governmental entities; obtaining information from cameras and video cameras seized from participants in criminal proceedings.

Thus, the process of digitalisation of forensics is a natural stage in the development and formation of modern forensic knowledge, which involves the introduction of digital technologies in various fields of forensic science and forensic examination. In today's realities, it is necessary to update the development of digital forensics issues in modern conditions. Particular attention should be paid to enhancing the role of forensic didactics, in particular, forensic training of investigators, prosecutors, courts, detectives, investigators, criminalists, and forensic experts in the field of digital technologies.

Conclusions. Thus, the issue of digital forensics in the context of digitalisation of modern society is relevant. Modern forensics must adapt and adapt to the level of development of modern technologies to be able to use them for law enforcement purposes. The development of new standards and principles for the evaluation and verification of collected evidence (digital traces) requires new knowledge and developments in forensic technology. In this regard, it is necessary to carry out mandatory standardisation when working with digital information, as well as to consider and develop an appropriate methodology for training specialists in the field of digital forensics.

REFERENCES

1. *Kryminalnyi protsesualnyi kodeks Ukrainy* [Criminal Procedure Code] : Zakon Ukrayiny vid 13.04.2012 r. № 4651-VI. Zakonodavstvo Ukrayiny. URL. *https://zakon.rada.gov.ua/laws/card/4651-17/conv* [in Ukrainian].

2. Polyakova T. A., Bojchenko I. S., Troyan N. A. (2021). ***Informacijno-pravovi mehanizmi elektronnoyi vzayemodiyi u sferi pravovoyi informaciyi v umovah cifrovizaciyi***. [Information and legal

mechanisms of electronic interaction in the field of legal information in the context of digitalisationl]. *Monitoring pravozastosuvannya.* No 1 (38). P.24-27 [in Ukrainian].

3. Avdyeyeva G. K. (2018). *Sutnist cifrovih slidiv u kriminalistici.* [The essence of digital traces in forensics]. *Aktualni pitannya sudovoyi ekspertizi ta kriminalistiki: zb. materialiv mizhnar. naukovo-prakt. konf., prisvyach. 95-richchyu stvorennya Harkiv. NDI sud. ekspertiz im. zasl. prof. M. S. Bokariusa* (Harkiv, 10–11 zhovtnya 2018). Harkiv, 2018. P. 90–93 [in Ukrainian].

4. *Didzhitalizaciya kriminalnogo procesu: v Ukrayini planuyut perevesti provadzhennya v elektronnij format.* [Improving the criminal justice process: Ukraine plans to transfer criminal proceedings to an electronic format]. Retrieved from: https://uazmi.org/news/post/bReTCc20Q04 a1jCN6zj9y2 [in Ukrainian].

5. Koval S. M. (2020). *Strategiyi rozvitku bezpeki cifrovih komunikacij sluzhbi kriminalistiki.* [Strategies for the development of digital communications security for the forensic service].*Yuridichnij naukovij zhurnal.* No 3 (2). P.83-87 [in Ukrainian].

Володимир БАРАНЯК

Національний університет «Львівська політехніка»,
Навчально-науковий інститут
права, психології та інноваційної освіти,
доцент кафедри кримінального права та процесу,
кандидат хімічних наук, доцент
volodymyr.m.baraniak@lpnu.ua
ORCID ID: https://orcid.org/ 0000-0001-6161-7862

ЦИФРОВА КРИМІНАЛІСТИКА В КОНТЕКСТІ ДІДЖИТАЛІЗАЦІЇ СУЧАСНОГО СУСПІЛЬСТВА

Обґрунтовується актуальність цифрової криміналістики в умовах цифровізації сучасного суспільства, відзначено активне використання цифрових технологій у вирішенні найрізноманітніших видів протиправної діяльності у сфері комп'ютерної інформації, дано визначення поняття «цифрового сліду» та «цифрової криміналістики».

Наголошено на необхідності вироблення нових знань і напрацювань криміналістичної техніки, стандартів і принципів оцінки та перевірки зібраних доказів (цифрових слідів), проведенні обов'язкової стандартизації під час роботи з цифровою інформацією, розгляді та розробці відповідної методики для підготовки фахівців у сфері цифрової криміналістики.

Акцентовано увагу на етичних, правових та питаннях приватності, пов'язані із збором та використанням цифрових даних під час проведення розслідування, дотриманні конфіденційності та захисту особистої інформації осіб, що не мають відношення до кримінального правопорушення, відповідності збору і використання цифрових даних під час розслідування визначеним правовим нормам і стандартам (отримання судових ордерів для збору доказів, вимоги щодо збереження інформації, дотримання прав і свобод осіб, які перебувають під слідством), забезпеченні належного рівня захисту, збереження та передачі особистої інформації та обмеженні доступу до неї лише на визначених підставах.

Акцентовано на ролі криміналістики у покращенні та підвищенні ефективності боротьби з сучасною злочинністю, включаючи військові та кіберзлочини, шляхом активного використання цифрових технологій.

Ключові слова: цифровізація, цифрові сліди, цифрова криміналістика, стандартизація, конфіденційність.