CONCEPT OF DIGITAL FORENSICS AND OPEN DATA SOURCE INFORMATION IN THE INVESTIGATION PROCESS

Kateryna LATYSH,
PhD in Law, Assistant Professor, Vilnius University,
Lithuania, Vilnius, Universiteto g. 3
Yaroslav Mudryi National Law University,
Ukraine, Kharkiv, Pushkinska street, 77,
Phone: +38 (098) 900-05-31,
Email: latysh78@gmail.com

SUMMARY

The digital forensics concept's main provisions and its role in the investigation process, especially as to the open-source information context (OSINT data use), are the article's subject. It should be said that it is a rather complex multidisciplinary task to do digital evidence search, collection, extraction and analysing, because a person doing that must have both thorough forensic, criminal procedural, and technical (digital) knowledge. Therefore, also the peculiarities of using specialized knowledge and procedural possibilities for engaging NGOs, that have been involved into collecting information about the event for a long time, are discussed.

Information technologies are increasingly used in all legal processes, including during pre-trial and trial. However, the techniques, tactics and methods of search, storage and research in the digital plane and with the help of digital technologies are either completely absent or quite outdated due to their continuous development. Criminals use the latest digital methods of committing crimes and disguise them well, which makes the identification processes quite complicated and costly. These research and formation processes are the task of digital forensics, whose content and place have been the scientific debate subject.

Digital gadgets used for investigative purposes demand constant operational updates, which require significant financial and time costs, including training of specialists, investigators, operative workers and experts.

The armed aggression by the aggressor-country against Ukraine has led to new needs in the field of forensic science to record traces of crimes due to the lack of access to the crime scene due to hostilities, mining, and occupation. All the participants' safety ensuring, under such circumstances is quite a difficult and sometimes even impossible task. Digital technologies, remote methods of scene inspecting and evidence trace collecting are going to solve these issues, so as open databases (OSINT) use.

Keywords: Digital Evidence, OSINT, Special knowledge, Forensics Science, Investigation of crimes, Digital technologies.

Constant digitization and technologization have led to new scientific branches and directions of traditional forensics emergence – they are digital, genotyscopic, aerospace and nuclear forensics[1]. The very concept of digital forensics, which has not had clearly defined boundaries and definitions yet, though it is extremely important due to its strategic nature for the development of forensic science[2], is explored within this article. Some scientists, along with this, limit this strategic nature of digital forensics, defining it as an "applied science", the provisions of which are directed to the investigation of computer crimes (incidents), as well as to search for methods of collecting, fixing and researching the digital evidence obtained[3]. However, such a restrictive approach is difficult to agree with due to the fact that digital forensics

[1] Шепітько В. (2021). Теоретико-методологічна модель криміналістики та її нові напрями. *Теорія та практика судової експертизи і криміналістики*. Вип. 3 (25). С. 9-20. DOI: 10.32353/ khrife.3.2021.02. С. 17.

[2] Шепітько В., Шепітько М. Формуванняцифрової криміналістики як стратегічний напрямок розвитку науки. *Kriminalistika a Forenzné Vedy: Veda, Vzdelávanie, Prax*. Zborník príspevkov 17 Medzinárodný kongres (Bratislava, Slovenská republika, 16-17.09.2021). Bratislava, 2021. С. 190.

[3] Гриців О. І. Криміналістика в комп’ютерних системах: процеси, готові рішення. *Вісник Національного університету «Львівська політехніка». Автоматика, вимірювання та керування.* 2013. №774. С. 120-126. URL: http://nbuv.gov.ua/UJRN/VNULP_2013_774_22 (дата звернення: 28.11.2021).

boundaries are much wider and not limited to computer crimes investigation only. The Russian Federation's armed aggression against Ukraine confirmed the fact once again, since, just with the help of digital forensics tools, it had been established and proved the commission of certain war crimes on the territory of Ukraine by the Russian military forces. Therefore, digital forensics should not be considered limited to only a certain category of crimes that can be investigated with its help.

Moreover, in addition to conducting investigative (research) actions, V. Shepitko points out the possibilities of applying special knowledge when working with digital evidence and conducting relevant forensic examinations[4], which can also be included in the content of digital forensics. V. Shevchuk also emphasizes digital forensics prospects for the development of forensic knowledge and forensic expert activity[5]. Forensic knowledge should not be limited only by criminal justice, especially in the area of digital forensics, but must also be extended to other justice types – administrative, civil, economic[6] - and other areas of legal activity[7].

Digital forensics is quite often named as Computer Forensics, Forensic Investigation, Internet of Things in the literature. It is because of different interpretations. Digital forensics has been developing into three main branches: 1) a separate scientific field formation, in criminalistics; 2) special knowledge application when working with digital evidence; 3) forensic examination conducting (in particular, computer-technical expertise)[8].

[4] Шепітько В., Шепітько М. Доктрина криміналістики та судової експертизи: формування, сучасний стан і розвиток в України. *Право України*. №8. С. 21.

[5] Shevchuk V. Modern problems of formation and prospects for researchingt he concept of criminalistic innovation. *Tendances scientifiques de la recherche fondamentale et appliquée:* collection de papiers scientifiques «ΛΌΓΟΣ». Strasbourg, 2020. Vol. 2. Pp. 67—72. DOI: 10.36074/30.10.2020. v2.20 (дата звернення: 15.05.2023).

[6] Judzinskytė A. Lietuvos teisinės bendruomenės kriminalistinis švietimas. *Criminalistics Education of the Lithuanian Legal Community.* 2022. Pp. 90. URL: https://vb.mruni.eu/object/elaba:117023592/ (дата звернення: 12.05.2023)

[7] Шевчук, В. (2022). Сучасні проблеми криміналістики в умовах війни та глобальних загроз. *Теорія та практика судової експертизи і криміналістики*. Вип. 3 (28). С. 11—27. DOI: 10.32353/ khrife.3.2022.02. С. 19.

[8] Шепітько, В., Шепітько, М. (2021). Доктрина криміналістики та судової експертизи: формування, сучасний стан і розвиток в України. *Право України*. №8. С. 21.

The object of digital forensics is the patterns of search, identification, collection and further research of digital traces and digital information with the help of appropriate digital tools for the purpose of further use during evidence in the relevant process.

Information gathering and verifying were carried out in two stages: 1) Initial data collecting; 2) Second-level review.

Digital forensics existence relevance is also emphasized by the official introduction of online platforms for the collection of information, which can potentially receive the status of evidence, into the pre-trial investigation. For instance, ICC Prosecutor Karim A. A. Khan KC announces the launch of the OTPLink platform, a new application for advanced online and email-based evidence submissions by all external stakeholders and witnesses to the ICC Office[9].

Taking into consideration the ICC's wide jurisdiction, it is forecasted a vast digital information massive from all external stakeholders and witnesses, that's why except a traditional manual review process, Artificial Intelligence (AI) and Machine Learning (ML) will be used for analyzing information collected. Such a possibility, introduced in ICC only in 2023, has been really a revolutionary step for international justice, because the digital information, collected by victims, witnesses, and international NGOs, has not been evaluated as evidence by courts in most cases, though such a possibility was foreseen "under Article 15 of the Rome Statute, the Office of the Prosecutor ("OTP") may analyze information on alleged crimes within the jurisdiction of the International Criminal Court (war crimes, crimes against humanity, genocide and aggression), submitted to it from any source"[10]. The OTP submission might be done anonymously or named (contact name, email and phone). From the ICC perspective, this submission should include data, the location of the incident, its name and summary, and attachment (a maximum number of files can be uploaded under each submission of 1000 with 3,9 GB total size).

[9] ICC Prosecutor Karim A.A. Khan KC announces launch of advanced evidence submission platform: OTP Link. URL: https://www.icc-cpi.int/news/icc-prosecutor-karim-aa-khan-kc-announces-launch-advanced-evidence-submission-platform-otplink

[10] OTP link. https://otplink.icc-cpi.int

The Ukrainian law enforcement system has also launched remote information collection: there are chat-bots («War Crime Bot», «STOP Russian War», «Stop marauder», «Find the traitor») for centralized storage, secure use and storage in the cloud of information and evidence, integrated into a range of investigative and analytical tools. The system maintains compliance with international evidence handling standards by using a digital chain of custody trail information. It is of urgent importance to use such tools which could secure data according to very high standards:

- collect quickly, safely, and securely,
- reliable use and store in the cloud,
- have centralized store for information and evidence,
- integrate a range of investigative and analytical tools,
- be capable of collecting facts, and maintaining compliance with international evidence handling standards with using a digital chain of custody trail that collects the information.

A very good platform for information collecting was created by Project Sunflowers, initiated by individuals and legal entities representing international and national non-governmental organizations, the Polish Bar Association. Project Sunflowers' aim is to create a platform to securely transmit, store and make available to legitimate authority information on international crimes, the victims of these crimes, and also to provide victims with help for reparations obtaining and psychological care. From this example, it is evident that not only governmental and non-governmental organizations could collect information, but also individuals and different other structures.

It is not the only Ukrainian case. For example, gross human rights violation evidence constituting crimes under international law allegedly committed by Belarusian authorities and others in the run-up to the 2020 presidential election and its aftermath, when different NGOs collected, consolidated, verified, and preserved evidence, with a view to supporting accountability bodies. For that reason, it was created the International Accountability Platform for Belarus (IAPB) and supported by a wide range of States, notably Austria, Belgium, Canada, Czech Republic, Denmark, Estonia, Finland, Germany, Iceland, Latvia, Lithuania, the Netherlands, Norway, Poland, Romania, Slovakia, Switzerland, Lichtenstein, the United Kingdom and the United States of America as well as the European Union[11].

In addition, "open source information is widely used by UN human rights fact-finding missions, commissions of inquiry and other official human rights investigations"[12].

The relentless digitization of all life processes has bypassed neither spheres of pre-trial investigation and trial nor their expert support. More and more crimes are committed with the help of the Internet to disguise the fact that they have been illegal. Therefore, the prompt acquisition and use of knowledge in the field of digital forensics has become a real challenge for law enforcement and judicial systems.

Digital forensics tools have been firstly used in practice by journalists, human rights defenders, and international non-governmental organizations, when compared to law enforcement agencies, due to the absence of mandatory, normatively established requirements for their collecting information for activity, and the limitation of information obtaining resources, which constantly require tools modernization and search methodology updating.

The digital evidence search, collection, extraction and research is a rather complex multidisciplinary task, as it requires both thorough forensic, criminal procedural, and technical (digital) knowledge. Therefore, in such cases, it is necessary to apply to the Institute of Special Knowledge for:

1) involvement of a specialist from the relevant field in conducting investigative (search) actions to provide advice on:

– appropriate places to search for information,

– the possibilities of overcoming the means and technologies of digital investigative activity and searching for hidden (conspirant), deleted information,

[11] International Accountability Platform. URL: https://iapbelarus.org/about/

[12] Yvonne McDermott et al., 'Open Source Information's Blind Spot: Human and Machine Bias in International Criminal Investigations' 19(1) JICJ 85-105.

– the information proper extraction and subsequent recording on digital media in order to preserve its integrity, authenticity and protect against possible modifications or destructions, including remote (for example, if the information is stored in the cloud);

2) appointing and conducting forensic examinations in the information technologies field.

Regarding the fact that a large number of war crimes, in which victims and participants are foreign citizens, are committed on the territory of Ukraine, judicial experts and specialists not only of the national, but also of the international level should be involved. For example, in the case of the downed Malaysian Boeing MH-17, as part of the joint investigation team, besides international investigators, foreign forensic experts and specialists were working, too.

A significant number of international non-governmental and national public organizations have already been involved in helping investigate war crimes on the territory of Ukraine, including the occupied territories (for example, Global Rights Compliance). They collect the information which, in the future, with compliance to relevant procedural requirements, may become evidence in criminal proceedings, as well as record traces of shelling, search for victims and witnesses.

As for the second case, when international and national non-governmental organizations are involved into the process of evidence gathering, there arises a big question that can be considered in two dimensions.

If the mentioned non-governmental organizations collect information about the event taking place independently by themselves, separately from the investigative team, after they have inspected the event scene, then no special issues arise here. The facts' collecting time is important, so that it takes place precisely after the inspection of the scene by the investigative-operational group, because the integrity of the criminal offence trace picture has surely to have been confirmed before they are carried out.

It is quite a different matter when such non-governmental organizations' members are directly involved in the investigative (search) actions, since such involvement requires strict adherence to the criminal procedural form. Therefore, such persons can be involved in research only in the status of specialists or other participants of criminal proceedings.

However, the question arises as to what legal status these persons are involved in, because the established criminal procedural form is mandatory and the procedure for conducting all investigative (search) actions is clearly regulated. In the first of the cases above, such persons act as part of the international investigative groups created and are included into their composition. Such experience is quite new and difficult to implement in the context of evidence exchange of between different jurisdictions, because each country participating in the international investigative team has its own requirements for the collection and storage of evidence, established by national legislation, which can very often differ from each other and from the established international practice.

But there has already existed a certain successful practice of joint international collection of evidence, recognized by the courts as admissible, in particular, in the above-mentioned case of the downed Malaysian Boeing MH-17, and in one of the Syrian cases, where the evidence was collected by an international (German-French) investigative team.

As for the second case, when international and national non-governmental organizations are involved into the process of evidence gathering, there arise a big question that can be considered in two dimensions.

If the mentioned non-governmental organizations collect information about the event taken place independently by themselves, separately from the investigative team, after they have inspected the scene of the event, then no special issues arise here. The facts' collecting time is important, so that it takes place precisely after the inspection of the scene by the investigative-operational group, because the integrity of the criminal offense trace picture has surely to have been confirmed before they are carried out.

It is quite a different matter when such non-governmental organizations' members are directly involved into the investigative (search) actions, since such involvement requires strict adherence to the criminal procedural form. Therefore, such persons can be involved into research only in the status of specialists or other participants of criminal proceedings.

Digital intelligence has been gaining momentum in Ukraine, especially due to the state of war and hostilities on its territory, but this does not accelerate the pace of their regulatory and doctrinal development. As it has been already mentioned, a significant number of non-governmental international organizations collect information about war and other crimes, the relevance of which will have to be confirmed in court in future, precisely with the help of remote investigation methods and technologies. In contrast to the practice developed in this part of the international investigative groups, the question regarding the evaluation of the information collected by non-governmental organizations by the courts has not yet been sufficiently developed.

The effectiveness of open sources data collection has been confirmed historically, since such collection has been carried out since the Second World War. Also, the North Atlantic Alliance (NATO) uses digital forensics tools, as evidenced by, in particular, the program documents (NATO Open Source Intelligence (OSINT) Reader (2002)[13] and Capability (2022).

In addition, digital forensics tools effectiveness was confirmed in the aforementioned case of the Boeing MH-17 downed and the investigation of war crimes on the territory of Ukraine[14]. Artificial intelligence helps in the search for Russian soldiers, whose faces were recorded in photos and videos from public places. We should agree with the proposed classification of open source information (Yv. McDermott, 2022) into four major groups: “1) primary: photographs, videos, parliamentary records; 2) secondary: NGOs Reports, journalistic accounts/op-eds; 3)

[13] NATO Open Source Intelligence Reader (2002) URL: https://cyberwar.nl/d/NATO%20OSINT%20Reader%20FINAL%20Oct2002.pdf

[14] MH17. The Open Source Evidence. A bellingcat Investigation. URL: https://www.bellingcat.com/app/uploads/2015/10/MH17-The-Open-Source-Evidence-EN.pdf

aggregated data: statistics, composite images, video explainers; 4) unique pieces of data: satellite images, social media posts"[15].

Therefore, the process of collecting digital evidence is quite complicated due to legal uncertainty and technical complexity. The increase of illegal activity in the digital plane, robotics and the use of artificial intelligence pose new strategic tasks for law enforcement agencies and courts to master at least the basics of such knowledge. High-quality and professional planning of the investigation of criminal offenses and further consideration of such cases in courts is impossible without it. This is related both to the specificity of the terminology used and to tactical and technical issues.

This project has received funding through the MSCA4Ukraine project, which is funded by the European Union.

[15] Yvonne McDermott et al., 'Open Source Information's Blind Spot: Human and Machine Bias in International Criminal Investigations' 19(1) JICJ 85-105.