DOI https://doi.org/10.30525/978-9934-26-400-9-6

OSINT AS AN INVESTIGATIVE TOOL: PROBLEMS OF COLLECTION AND STANDARDIZATION

Latysh K. V., Demidova Ye. Ye., Kapustina M. V.

INTRODUCTION

With the expansion of technological capabilities and the emergence of social media, traditional evidence is significantly updated and supplemented by digital evidence. Modern information technologies are actively applied in all spheres of life: economy, law enforcement and judicial activities, management, medicine, etc. A significant amount of information is being digitized on a daily basis through the creation of relevant electronic registers and the construction of a digital state. The war has posed significant challenges not only to citizens and the state, but also to the existing global order and security system, demonstrating its limitations in preventing and resolving armed conflicts. It has also revealed the shortcomings of existing investigative and judicial procedures, prompting public (or, as they are called abroad, non-governmental) organizations to take the initiative in the search for justice. However, the interaction and regulation of these organizations remains comprehensive.

These inevitable processes require a change in traditional approaches to the tools, means, methods and techniques of collecting, examining, evaluating and using evidence for the purpose of detecting, investigating, prosecuting and preventing criminal offenses. At the same time, it is necessary to take into account the growing dependence of investigations on digital evidence in modern investigations, especially in times of conflict and war, also due to the inaccessibility and danger of access to the scene of the crime. The practice of combating crime convincingly shows that without modern, appropriate information support for criminal investigations, it is almost impossible to combat criminal manifestations. At the same time, this also raises a number of legal problems due to the legislative unpreparedness of criminal procedure for such digital challenges, the lack of proper legal regulation of interaction with digital evidence, and other challenges related to the dynamic nature of digital data, the importance of preserving its integrity, and the consequences of technological progress on legal standards and practices.

The purpose of this chapter is therefore to consider certain aspects of such problems and to suggest possible options for the procedural behavior of participants in criminal proceedings with respect to the documentation of

OSINT data. It also focuses on the need to comply with the legal and ethical framework governing the receipt and use of digital evidence from open sources. International cooperation plays a critical role, and, in this regard, there is a need to standardize the solution to these problems, especially in the context of global conflicts and human rights violations.

1. Investigative standards: the path to improvement

In order to develop science-based practical recommendations for the collection, preservation, use, and examination of digital (evidence) information in the context of hostilities, it is important to consider several key investigative standards.

These include the following:

1) The Berkeley Protocol for Investigations Using Open Digital Data[1];

2) Leiden Guidelines on the Use of Digitally Derived Evidence[2];

3) International Protocol on Documentation and Investigation of Sexual Violence in Conflict,

4) Standards for the Investigation of War Crimes: General Part[3],

5) Guidelines on Basic Investigative Standards for Documentation of International Crimes in Ukraine[4].

Analyzing the content of such standards, we should agree with the point of view of M. Shepitko, who notes the prospects of developing such standards of investigation, but points out the following shortcomings

1) lack of common parameters for these standards, which led to different understandings of their content;

2) the substitution of standards with a separate investigative methodology, even in some cases a simplified "copy" of the structure of a

[1] Практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права з прав людини та гуманітарного права. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf

[2] Leiden Guidelines on the Use of Digitally Derived Evidence. URL: https://leiden-guidelines.netlify.app/guidelines/

[3] Методичні рекомендації «Стандарти розслідування воєнних злочинів. Загальна частина», затверджено Генеральним прокурором від 28.04.2023р., схвалено Протоколом засідання методичної ради від 16.03.2023р. № 3. URL: https://justgroup.com.ua/wp-content/uploads/2023/05/standart-rozsliduvannya_zagalna-chastyna.pdf?fbclid=IwAR12V2TQQChDAbJR3or3oiVf0QObng6mDpMF4b5DXwG2obBbNygHu5Ft2Kg

[4] Керівництво з базових стандартів розслідування для документування міжнародних злочинів в Україні. URL: https://globalrightscompliance.com/wp-content/uploads/2023/05/КЕРІВНИЦТВО-З-БАЗОВИХ-СТАНДАРТІВ-РОЗСЛІДУВАННЯ-ДЛЯ-ДОКУМЕНТУВАННЯ-МІЖНАРОДНИХ-ЗЛОЧИНІВ-В-УКРАЇНІ.pdf

separate investigative methodology, or coverage only of the criminal law and international characteristics of war crimes;

3) the absence of the actual formulation of such standards, as only principles, practical forensic advice, certain aspects of evidence and sample documents are formulated;

4) The specific steps to be taken by the investigator are not disclosed and the tactics of investigative (search) actions are not recommended[5].

In light of the above, it seems necessary to comply with international standards, such as those set forth in the Rome Statute of the International Criminal Court, on the collection, documentation and preservation of evidence. Of course, the Rome Statute is not binding on Ukraine, as it has not yet ratified it, but only signed it. This demonstrates Ukraine's agreement with the principles of the Statute, but ratification is necessary for Ukraine to become a full member of the International Criminal Court and for the Statute to enter into force in the country. Nevertheless, it seems necessary to take into account successful international practices and adapt them to Ukrainian realities, since the ratification of the Rome Statute implies amendments to the national legislation of the member state in order to bring it into conformity with the obligations established by the Statute. In the case of Ukraine, this means adapting its legislation to the standards of the International Criminal Court, especially in the areas of war crimes, crimes against humanity and genocide.

In addition, when it comes to investigative standards for crimes such as war crimes, it is important to consider data protection legislation, such as the EU's General Data Protection Regulation (GDPR), especially when processing personal data. Therefore, at a minimum, the development and regulation of data protection and privacy practices should be included in applicable legislation and investigative standards under development.

The use of internationally recognized digital evidence collection techniques (e.g., the Berkeley Protocol) also requires consideration of digital evidence collection principles and standards for information storage and protection. It is important to ensure the integrity, confidentiality, and availability of information through the use of encryption, backup, and other information security methods.

[5] Шепітько М. Розслідування воєнних злочинів в Україні: напрями та перспективи. Criminalistics and forensic expertology: science, studies, practice 19 (compiler Gabriele Juodkaite-Granskiene; scientific-editorial committee: Henryk Malewski (chairman) and others. Forensic Science Centre of Lithuania, Criminalists' association of Lithuania. Vilnius, Brno, 2023. С. 55, 57.

Documentation and reporting protocols include the creation of accurate and detailed records of all stages of information processing, from collection to presentation as evidence.

It is also important to take into account international humanitarian law, i.e. to ensure that all processes for collecting and using information comply with international humanitarian law.

It is necessary to ensure cooperation with international organizations and international law enforcement and human rights organizations in order to share information and best practices.

As mentioned above, these standards, i.e. scientifically based practical recommendations for the collection, storage, use and research of information from open sources (open-data source) in the context of hostilities, can be adapted and supplemented to take into account the specifics of hostilities and existing national legislation, and determine further directions for the development of strategic relations and cooperation between cybersecurity actors, pre-trial investigation bodies, courts and individuals. As of 2023, there is a lack of proper legal regulation of the collection and storage of such information in the CPC of Ukraine, which is why there is an urgent need for investigators and operatives to turn to other procedural sources that are non-procedural (advisory, auxiliary) in nature[6].

The specificity of information from open sources is related to the fact that it is the result of analytical processing of a large volume of open, publicly available information flows, which are: a) mass media: printed newspapers, magazines, radio and television; b) the World Wide Web online publications, blogs, discussion groups (forums), citizen media (e.g. mobile phone videos, user-generated content), YouTube, RuTube and other video hosting sites, wiki directories and other social media sites (Facebook, Twitter, Instagram, Telegram, etc.)[7].

Open-source information is "publicly available information that any member of the public can observe, purchase, or request without special legal status or unauthorized access"[8]. This data allows law enforcement to gather critical information without violating privacy, which is a key aspect of

[6] Зоренко Д. До питання процедури фіксації результатів OSINT в контексті розслідування воєнних злочинів. Сучасні реалії протидії воєнним злочинам: набутий досвід та погляд в майбутнє: матеріали панельної дискусії VII Харківського Міжнародного юридичного форуму 25 вересня 2023 року. Київ : Алерта, 2023. 146 с. С. 39.

[7] Одерій О.В., Кожевніков О.А. Отримання криміналістично значущої інформації шляхом аналізу відкритих інтернет-джерел. *Правовий часопис Донбасу*. 2020. № 4 (73). (С. 146) С. 144-155

[8] HRC UC Berkeley and UN OHCHR 2020, 6. URL: https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf

ensuring respect for human rights and the rule of law during investigations. For example, the use of OSINT tools has played a critical role in the investigation of high-profile cases such as the MH-17 incident and the investigation of war crimes in Ukraine. A notable instance was the investigation of civilian mass graves in Bucha, Kyiv region. Satellite technology was instrumental in determining the timeline of events, particularly the period during which the bodies appeared. This timeline coincided with the reported occupation of the area by Russian forces, a claim denied by Russia, which instead attributed the actions to Ukrainian authorities.

It is necessary to establish the entire process of researching digital (evidentiary) information: from its collection and storage to its examination and evaluation. The Prosecutor vs. Gbagbo case can be cited as an illustrative example, where a large number of facts and messages published in public and social media were accepted as credible by the authorities, despite the fact that the investigators had not taken any measures to verify them[9]. The Chamber mentioned that "such evidence can in no way be presented as the fruit of a full and proper investigation", although it can be of great use in understanding some real situations[10]. Therefore, it is important to define the role of the investigator in this process, which can be divided into the following investigative situations:

1) when the investigator independently collects this digital information from open sources,

2) when information from open sources is provided by a participant in criminal proceedings,

3) when information from open sources is provided by an unauthorized person who is not a party to the criminal case and therefore has no procedural status in the case and no procedural rights.

Then there is the issue of registration of such data, especially in the last third situation, when digital data is provided by a person who has no relation to the criminal case and, therefore, cannot provide evidence. In this case, the investigator may request such information in accordance with Article 93 of

[9] Freeman, Lindsay, and Raquel Vazquez Llorente. 2021. “Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age.” *Journal of International Criminal Justice* 19 (1): 163–88. https://doi.org/10.1093/jicj/mqab023

[10] *Prosecutor v. Laurent Gbagbo.* ICC. Pre-Trial Chamber I. “Decision adjourning the hearing on the confirmation of charges pursuant to article 61(7)(c)(i) of the Rome Statute.” ICC-02/11-01/11 (2013); Latysh K. The role of digital forensics in the investigation of international crimes. Забезпечення стійкості у складних умовах: збірник матеріалів доповідей учасників міжнародної міждисциплінарної науково-практичної конференції. (Харків – Брістоль, 8 червня 2023 р.). Харків, 2023. 288 с. С. 54-56.

the Criminal Procedural Code of Ukraine (hereinafter – the CPC of Ukraine) or interrogate as a witness (Article 224 of the CPC of Ukraine) with further attachment of additional evidence. There is also a practice of initiating criminal proceedings by international non-governmental organizations and national NGOs in cases where their open-source investigation has identified persons involved in the commission of a war crime, which is usually documented in the form of a report. This is a new format of documents that the investigator must work with and verify the accuracy of the data contained therein. There are a number of steps that the investigator can take independently to verify the information provided or to engage a specialist to conduct such verification, followed by an appropriate forensic investigation.

2. Forensic examination of OSINT data

These are formal issues, but they receive considerable attention in Ukrainian courts because there is no algorithm for storing OSINT data that has been tested and accepted by the Ukrainian judicial system, and each practitioner continues to do so at his or her own discretion, and judges will consider such data only if there is a relevant forensic examination report. Therefore, it is necessary to take into account the reliability and accuracy of information from open sources, as it can be subjective or falsified. Therefore, its analysis and interpretation require a professional approach, critical thinking and the involvement of persons with specialized knowledge.

Photographic and video images of people are often used as important sources of information in OSINT. Of particular forensic interest, for example, is the technology of automatic identification of a person's identity based on elements of their appearance as reflected in a photograph or video, which has wide commercial and scientific applications. This technology is interesting because it can be performed without contact with the subject of the search. On the World Wide Web, there are online services for searching people by facial features among the multitude of photographs available on the personal pages of popular social networks (Search4faces, VK.watch, etc.)[11]. However, the data obtained during such a search, as well as other open sources, usually only provide information on the potential match of the external characteristics of a given person. In order to determine whether a particular person is depicted on the relevant photos (videos), a portrait examination is required.

[11] Одерій О.В., Кожевніков О.А. Отримання криміналістично значущої інформації шляхом аналізу відкритих інтернет-джерел. *Правовий часопис Донбасу*. 2020. № 4 (73). (С. 146) С. 144-155.

The subject of portrait examination is the regularities of the physiological structure of a person's appearance, its changes during life and after death, the use of a person's appearance for detection and investigation of criminal offenses[12]. Portrait examination allows to identify the person depicted in a photograph or video, to determine whether the person depicted in different photographs or videos is the same person, including in the case of pictures taken at different times, taking into account possible changes in the appearance of this person, etc.

In the context of active military operations on the territory of Ukraine, facial recognition has become particularly relevant, given the large number of photographs and videos that regularly appear on social media from various hotspots. These materials often contain valuable information that can be used in investigations, and sketch identification allows for the identification of individuals involved in unlawful acts, including military personnel, militants, civilians, and other participants responsible for war crimes and violations of international humanitarian law. In addition, facial recognition can assist in the search for missing persons by identifying them in photographs or videos that may indicate their last known whereabouts. Thus, in situations where crimes are documented and posted on social media, facial recognition becomes a key tool in identifying not only the perpetrators of these crimes, but also their victims. For example, a well-known case of such examination was a study to identify the deceased Hero of Ukraine Oleksandr Matsievskyi in the case of the shooting of a Ukrainian serviceman by Russians, when forensic experts were provided with a video of the event that appeared on the Internet[13].

It should be noted that the possibility of performing identification research may be affected by the following factors, among others: 1) change in appearance due to surgical intervention (plastic surgery); 2) change in appearance due to cosmetic procedures (biorevitalization; mesotherapy; facial modeling with fillers; botulinum toxin injections, etc.); 3) cosmetic design (makeup); 4) change in appearance due to disease or injury (e.g.,

[12] Можливості портретної експертизи: Офіційний сайт Тернопільського науково-дослідного експертно-криміналістичного центру МВС України:. URL: https://ndekc.te.ua/news/mozhlivost-portretno-ekspertizi

[13] При визначенні особи загиблого Мацієвського для ілюстрації експерти КНДІСЕ використали штучний інтелект. Офіційний сайт UNN. URL: https://unn.ua/news/pri-viznachenni-osobi-zagiblogo-matsiyevskogo-dlya-ilyustratsiyi-eksperti-kndise-vikoristali-shtuchniy-intelekt.

psoriasis spots, improperly fused nasal bones after a fracture, etc.)[14]. In addition, the quality of the photographs (videos) and the lighting conditions during the shooting, especially in cases of low resolution or poor lighting, may also have a negative impact on the study. This applies both to materials provided for direct examination (e.g., video from the Internet depicting a person to be identified) and to samples for comparative examination. The likelihood of manipulation, including the use of modern technology and artificial intelligence, must also be considered. In this regard, it is advisable to order a comprehensive forensic portrait and forensic photographic examination in order to establish the facts of editorial changes in the form of editing in digital photographs[15].

Photographic examination also examines photographic and video materials, but unlike portrait examination, it is used in cases when it is necessary to determine the data recorded in the photographic images in a latent (implicit) form. For example, to determine the size of objects captured in the photograph, the relative position of cars in relation to the edges of the road, the point of taking the photograph, or to reconstruct the material environment of the scene from the photographs. Photographic expertise is often used to detect signs of editing in photographs, to identify objects in photographs, to determine the natural dimensions of objects depicted in photographs, to determine the content of information marks depicted in photographs (for example, the state license plate of a vehicle)[16].

Such comparative studies are conducted using image quality assessment methods (local focus quality methods, noise characterization methods, discrete cosine transform (DCT) analysis methods, image entropy analysis methods). In addition, artificial intelligence technologies are also being introduced into photographic investigations. For example, in addition to the above-mentioned image enhancement technologies, a Unet-type artificial neural network model with the EfficientNetB4 feature classifier is used,

[14] Гусєва В. О. Проблеми ідентифікації особи за ознаками зовнішності під час розслідування кримінальних правопорушень. *Теорія та практика судової експертизи і криміналістики*. 2021. Випуск 2 (24). С. 116 (С. 109-122)

[15] Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : наказ Міністерства юстиції України від 08 жовтня 1998 року № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98

[16] Чорний С., Брендель О., Гратіашвілі Д. Автентифікація зображень на основі їх семантичної сегментації у нейронних мережах глибокого навчання з їх попереднім обробленням за методами фільтрації. Теорія та практика судової експертизи і криміналістики. 2022. Випуск 1 (26). С. 128.

which has proven to be effective in detecting signs of photo manipulation[17]. In today's information space, where unverified or deliberately distorted information often appears, photographic examination serves as a means of verifying and verifying the veracity of images, which is of great importance for the accurate and objective establishment of facts, which is critical for preserving historical truth and conducting effective investigations.

Video and audio recording expertise, which includes not only video and audio recording but also the means of recording and reproducing audio and video information, is no less important in assisting in the evaluation of information derived from OSINT.

During the investigation the following types of researches are carried out: identification studies of human voice and speech (establishing individual and group identity of persons by comparing their voices and speech on sample signals and the studied signals); diagnostic studies of human voice and speech (establishing certain signs of a person's voice and speech; study of sound and video recording devices, diagnostic studies to establish technical conditions and technology for obtaining a recording; identification and diagnostic[18]. In the context of information warfare and propaganda, accurate analysis of video and audio materials helps to identify a person by speech characteristics, to find out whether the speech was spontaneous (unprepared) or prepared, to determine which of the participants in the conversation belongs to a certain remark, to determine the sources and nature of sounds accompanying the main recording, as well as the duration of certain sound phenomena[19] and other important issues. Thus, examination of video and audio recordings allows not only to establish new facts, but also to identify and refute false information, which contributes to maintaining the information security of the society.

The peculiarity of the existing methods of expert examination of computer hardware, software products, and telecommunication networks is that they require constant updating and improvement due to the constant changes in data representation formats, operating and file systems, data

[17] Чорний С., Брендель О., Гратіашвілі Д. Автентифікація зображень на основі їх семантичної сегментації у нейронних мережах глибокого навчання з їх попереднім обробленням за методами фільтрації. Теорія та практика судової експертизи і криміналістики. 2022. Випуск 1 (26). С. 128.

[18] Експертизи відео-, звукозапису. Офіційний сайт Тернопільського науково-дослідного експертно-криміналістичного центру МВС України. URL: https://ndekc.te.ua/news/mozhlivost-ekspertizi-vdeo-zvukozapisu

[19] Особливості призначення судових експертиз : практ. порадникь/ М-во внутр. справ України; Експертна служба; Харківський наук.-дослід. експерт.-криміналіст. Центр. Вид. 2-ге, переробл. Харків, 2021. С. 64-66 (92 с.)

transfer protocols, and technical means of information transmission. It is clear that the development and improvement of such methods is possible only with the use of modern equipment, software and specialized knowledge of specialists in the field of telecommunications systems and IT technologies[20]. It is important to note that any interaction with a technical medium such as a mobile phone can lead to changes in its memory and loss of its integrity status. This includes seemingly minor actions, such as turning the device on and then immediately turning it off, which can still affect the data integrity and subsequently the device's status as an object of evidence[21].

3. Investigative Information Systems and Technologies

Another set of OSINT data can come from open-source information systems, which are the most modern means of information support. Information systems in forensic science are generally understood as an organizationally ordered set of arrays of information about certain objects and information technologies, including modern computer hardware, software, and communication networks that provide the processes of inputting, processing, and outputting information to the user[22]. Information systems, as V. Zhuravel has rightly pointed out, serve as a basis for support of decision-making of the investigator conducting criminal proceedings, activation of his intellectual activity in planning, proposing versions, selection of optimal systems of investigative (detective) and covert investigative (detective) actions for their verification[23].

Today, many information systems and technologies are used in the investigation of war crimes. Among them, in our opinion, an important place in connection with Russia's armed aggression against Ukraine is occupied by those aimed at searching for and identifying individuals. These systems include:

---

[20] Коршенко В. Судова телекомунікаційна експертиза як джерело доказів під час розслідування кіберзлочинів. *Jurnalul juridic naţional: teorie şi practică.* 2017. № 2 (24). С. 192–194.

[21] Білоус В., Латиш К. Судові експертизи радіоелектронних засобів як форма використання спеціальних знань під час розслідування корупційних кримінальних правопорушень. *Наукові праці Міжрегіональної Академії управління персоналом. Серія: Юридичні науки.* 2022. Випуск 1 (61). С. 5-11. DOI: https://doi.org/10.32689/2522-4603.2022.1.1.

[22] Birykov, V. 2009. *Theoretical foundations of information and reference support for the investigation of crimes*.Luhansk: LVV LDUVS named after E.O. Didorenko.

[23] Zhuravel, V., Shepitko, V. 2017. Automated information systems as means of improving the investigation of murders. *Journal of the National Academy of Legal Sciences of Ukraine*, 1(88), 163-172.

1) Unified Register of Missing Persons under Special Circumstances, which is an electronic database for storing, protecting, processing, using and disseminating information on missing persons under special circumstances, their unidentified remains, the existence or non-existence of a court decision declaring them missing, missing or dead, as well as other data used to ensure the registration of missing persons for the purpose of their search. A person who has disappeared under special circumstances is a person who has disappeared in connection with an armed conflict, military actions, temporary occupation of a part of the territory of Ukraine, natural or man-made emergencies. The Unified Register of Missing Persons under Special Circumstances is created to collect and centralize information and data on such persons, as well as to record information necessary for their effective search. The structure of the Register consists of interconnected sections containing: information on persons missing under special circumstances; information on unidentified bodies (remains) of deceased persons and related objects, documents[24];

2) Electronic Register of Human Genomic Information, which is an information and communication system that ensures the collection, registration, accumulation, storage, updating, search, use and dissemination (distribution, transmission) of human genomic information. The electronic register of human genomic information makes it possible to: identify a person who has committed a criminal offense; search for a missing person; identify an unidentified human corpse, its remains and parts; identify a person who is unable to provide information about himself/herself due to health, age or other circumstances[25];

3) automated recording of human genetic characteristics, which is a collection of DNA profiles of persons suspected or accused of committing crimes, detainees, convicts, and biological traces seized during the examination of the crime scene and other investigative (search) actions, including in cases of missing persons[26];

4) the Arkan system is a set of organizational and administrative measures, software, hardware and telecommunication tools ensuring the

[24] Закон України Про правовий статус осіб, зниклих безвісти за особливих обставин. https://zakon.rada.gov.ua/laws/show/2505-19#Text.; Положення Про Єдиний реєстр осіб, зниклих безвісти за особливих обставин. Затв. Наказом МВС України 22.08.2022 № 535. https://zakon.rada.gov.ua/laws/show/z0998-22#Text.

[25] Закон України Про державну реєстрацію геномної інформації людини. https://zakon.rada.gov.ua/laws/show/2391-20#Text.

[26] Інструкція з організації функціонування криміналістичних обліків експертної служби МВС України: затв. Наказом МВС України від 10.09.2009 № 390. https://zakon.rada.gov.ua/laws/show/z0963-09#Text.

processing of information (input, acceptance, receipt, transmission, registration, storage) on the control of persons, vehicles and goods crossing the state border of Ukraine. This system was created in order to a) to provide timely, reliable and functionally complete information and analytical support for the activities of the System's bodies in the implementation of measures to prevent and stop the entry into or exit from Ukraine of persons who are not authorized to enter Ukraine or who are temporarily restricted in their right to enter Ukraine in accordance with the law, or who are temporarily restricted in their right to leave Ukraine; b) searches at state border checkpoints for persons hiding from the bodies of inquiry, investigation and court, evading criminal sanctions; c) suppression of illegal activities of natural and legal persons who illegally transport migrants to Ukraine or transit them through the territory of Ukraine; d) strengthening of control over compliance with the rules of entry, exit, stay in Ukraine of foreigners and stateless persons, as well as performance of other tasks in the sphere of law enforcement in accordance with the law[27];

5) analytical supplement "War criminals of the Russian Federation". This analytical appendix has been developed by processing and systematization of the information about the enemies of Ukraine published by the Defense Intelligence Service of Ukraine on its web-resource. The analytical supplement "War Criminals of the Russian Federation" provides an accessible and visual demonstration of the enemy's management of the geography of human resources and types of troops used in the war. This application sorts the information by such individual characteristics as age, rank, geography, etc. In addition, it contains information on the personnel of the invaders[28].

A separate group of information support tools for the investigation of war crimes aimed at searching for and identifying individuals consists of information systems and technologies based on the principle of searching for information from open sources and registers. Such information systems and technologies include:

[27] Положення про інтегровану міжвідомчу інформаційно-телекомунікаційну систему щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон: затв. Наказом Адміністрації Державної прикордонної служби України, Державної митної служби України, Державної податкової адміністрації України, Міністерства внутрішніх справ України, Міністерства закордонних справ України, Міністерства праці та соціальної політики України, Служби безпеки України, Служби зовнішньої розвідки України від 3 квітня 2008 р. N 284/287/214/150/64/175/266/75 https://zakon.rada.gov.ua/laws/show/z0396-08#Text

[28] Офіційний веб-портал – Головного управління розвідки Міністерства оборони України. https://gur.gov.ua/content/war-criminals-rf.html

1) Face recognition technology developed by the American company Clearview AI. Clearview AI's face recognition algorithm works as a search engine that contains more than 40 billion images of faces from open web resources, including media, photo websites, social networks, and many other open sources. One of the benefits of this technology is that it provides highly accurate facial recognition across all demographic groups. For example, the Clearview AI face recognition algorithm is designed to account for aging, changes in posture and position, changes in facial hair, and many visual conditions[29]. The use of facial recognition technology developed by the American company Clearview AI allows to identify: deceased persons; persons who, for objective or subjective reasons, are unable to provide information about themselves; captured Ukrainian citizens; Russian military personnel, representatives of the Russian armed forces and members of illegal armed groups; persons involved in collaboration; Ukrainian children deported to the territory of the Russian Federation and the temporarily occupied territories of the Russian Federation; persons involved in the illegal removal of children from the territory of the Russian Federation;

2) the electronic application "Who are you", created to simplify the procedure of checking suspicious persons at checkpoints, on the streets during curfew, at the entrance to shelters and in other situations. The application allows instant verification of the following types of checks: whether the passport is valid or considered lost; whether the person is on the state wanted list; whether the person is on the list of military terrorists or illegal armed groups; whether the person is in the Myrotvorets database; whether the person is subject to sanctions of the National Security and Defense Council[30];

3) the information system "Book of Executioners of the Ukrainian People". This information system contains verified information about Russian military personnel who have committed and are still committing crimes on the territory of Ukraine. Information about war criminals is collected in real time, which means that the information base of this system is constantly updated. All criminals presented on the site are confirmed and verified by one of the law enforcement or intelligence agencies of Ukraine. There are no random people on the resource and no fake names that criminals use to hide on social media. In addition, using the feedback form, any Ukrainian who has become a victim of Russian aggression can identify

[29] Clearview AI Principles https://www.clearview.ai/principle

[30] «ТиХто» – додаток, який допомагає шукати окупантів. https://vechirniy.kyiv.ua/news/64785/

the perpetrator and provide additional information that will be used to record the facts of Russian crimes in Ukraine[31];

4) the online registry "Russian War Criminals", which contains personal data of Russian army personnel, identified persons of captured Russians, as well as Russians killed during the war in Ukraine. The registry also contains evidence of their stay in Ukraine (each soldier's profile contains a link to the evidence base), while information on others is still being collected and processed. The registry contains the following information about Russian servicemen: surname, first name, patronymic, military rank, date of birth, affiliation to a military unit, and status (participant in the war in Ukraine, liquidated, captured, suspect)[32].

Thus, the considered information systems and technologies have a significant potential for the investigation of war crimes and are effective information tools for the search and identification of persons in war.

CONCLUSIONS

Advances in digital technologies and the emergence of social media have significantly updated the scope of traditional evidence, necessitating a revision of approaches to the collection, examination, evaluation, and use of evidence.

The chapter emphasizes the increasing reliance on digital evidence in modern investigations, particularly in conflict and war scenarios. It highlights the legal challenges posed by the unpreparedness of legislation to address digital challenges, the lack of adequate legal regulation of digital evidence, and the dynamic nature of digital data. International cooperation and standardization in addressing these challenges is very important, especially in global conflicts and human rights violations. Cooperation with international organizations and law enforcement agencies would be very useful to share information and best practices. The need to adhere to international standards, such as those set out in the Rome Statute of the International Criminal Court, and to adapt them to local contexts is discussed.

The chapter also highlights the importance of data protection laws, such as the GDPR, in the process of collecting and using digital evidence. It highlights the importance of ensuring the integrity, confidentiality, and availability of information through secure methods such as encryption and backup. It highlights the role of international humanitarian law in guiding

[31] Книга катів українського народу. База російських військових, які чинили злочини в Україні. URL: https://russian-torturers.com.

[32] Російські воєнні злочинці. Онлайн-реєстр. URL: https://rwc.shtab.net

the collection and use of information. The need for proper legal regulation of the collection and retention of digital information in the context of hostilities is highlighted, as is the importance of open-source information and its implications for law enforcement and human rights.

It examines the role of OSINT tools in the investigation of high-profile cases such as the MH-17 incident and war crimes in Ukraine. It emphasizes the need for a systematic approach to investigating digital information, from collection to exploitation.

The chapter discusses the need to define the investigator's role in collecting and reviewing digital information. Finally, it emphasizes the importance of addressing formal issues in the preservation and legal admissibility of OSINT data, given its reliability and accuracy.

These conclusions highlight the evolving landscape of digital evidence in the context of modern investigations, particularly during conflict, and the need for legal, technological, and collaborative strategies to effectively manage this evidence.

SUMMARY

This chapter addresses the complex and evolving issues surrounding the collection, storage, use and analysis of open-source digital information, particularly in the context of war. It emphasizes the need for science-based practical recommendations and the adoption of international standards, such as those set forth in the Rome Statute of the International Criminal Court. The challenges and considerations in ensuring the integrity, confidentiality, and availability of digital evidence, while respecting human rights and data protection laws such as the GDPR.

The chapter highlights the importance of appropriate methods and standards for handling digital evidence from open sources, particularly in the context of war crimes and other sensitive legal matters. It highlights the need for continuous updating and improvement of methodologies, taking into account rapid technological advances and changing data formats. It's important to ensure data integrity, define the role of forensic experts in verifying the authenticity of digital evidence, and the need to adapt international standards to local legal frameworks, thereby contributing to effective investigations and the preservation of historical truth.

References

1. Практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права з прав людини та гуманітарного права. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf (дата звернення 15.12.2023).

2. Leiden Guidelines on the Use of Digitally Derived Evidence. URL: https://leiden-guidelines.netlify.app/guidelines/ (дата звернення 10.12.2023).

3. Методичні рекомендації «Стандарти розслідування воєнних злочинів. Загальна частина», затверджено Генеральним прокурором від 28.04.2023р., схвалено Протоколом засідання методичної ради від 16.03.2023р. №3. URL: https://justgroup.com.ua/wp-content/uploads/2023/05/standart-rozsliduvannya_zagalna-chastyna.pdf?fbclid=IwAR12V2TQQChDAbJR3or3oiVf0QObng6mDpMF4b5DXwG2obBbNygHu5Ft2Kg (дата звернення 10.12.2023).

4. Керівництво з базових стандартів розслідування для документування міжнародних злочинів в Україні. URL: https://globalrightscompliance.com/wp-content/uploads/2023/05/КЕРІВНИЦТВО-З-БАЗОВИХ-СТАНДАРТІВ-РОЗСЛІДУВАННЯ-ДЛЯ-ДОКУМЕНТУВАННЯ-МІЖНАРОДНИХ-ЗЛОЧИНІВ-В-УКРАЇНІ.pdf (дата звернення 10.12.2023).

5. Шепітько М. Розслідування воєнних злочинів в Україні: напрями та перспективи. Criminalistics and forensic expertology: science, studies, practice 19. Forensic Science Centre of Lithuania, Criminalists' association of Lithuania. Vilnius, Brno, 2023. С. 55-61.

6. Зоренко Д. До питання процедури фіксації результатів OSINT в контексті розслідування воєнних злочинів. *Сучасні реалії протидії воєнним злочинам: набутий досвід та погляд в майбутнє:* матеріали панельної дискусії VII Харківського Міжнародного юридичного форуму 25 вересня 2023 року. Київ: Алерта, 2023. 146 с.

7. Одерій О.В., Кожевніков О.А. Отримання криміналістично значущої інформації шляхом аналізу відкритих інтернет-джерел. *Правовий часопис Донбасу*. 2020. № 4 (73). С. 144-155.

8. HRC UC Berkeley and UN OHCHR 2020, 6. URL: https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf (дата звернення 10.12.2023).

9. Freeman, Lindsay, and Raquel Vazquez Llorente. 2021. "Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age." *Journal of International Criminal Justice* 19 (1): 163–88. https://doi.org/10.1093/jicj/mqab023

10. *Prosecutor v. Laurent Gbagbo.* ICC. Pre-Trial Chamber I. "Decision adjourning the hearing on the confirmation of charges pursuant to article 61(7)(c)(i) of the Rome Statute." ICC-02/11-01/11.2013.

11. Latysh K. The role of digital forensics in the investigation of international crimes. *Забезпечення стійкості у складних умовах*: збірник матеріалів доповідей учасників міжнародної міждисциплінарної

науково-практичної конференції. (Харків – Брістоль, 8 червня 2023 р.). Харків, 2023. 288 с. С. 54-56. (дата звернення 10.12.2023).

12. Одерій О.В., Кожевніков О.А. Отримання криміналістично значущої інформації шляхом аналізу відкритих інтернет-джерел. *Правовий часопис Донбасу*. 2020. № 4 (73). (С. 146) С. 144-155.

13. Можливості портретної експертизи: Офіційний сайт Тернопільського науково-дослідного експертно-криміналістичного центру МВС України. URL: https://ndekc.te.ua/news/mozhlivost-portretno-ekspertizi (дата звернення 10.12.2023).

14. При визначенні особи загиблого Маціївського для ілюстрації експерти КНДІСЕ використали штучний інтелект. Офіційний сайт UNN. URL: https://unn.ua/news/pri-viznachenni-osobi-zagiblogo-matsiyevskogo-dlya-ilyustratsiyi-eksperti-kndise-vikoristali-shtuchniy-intelekt. (дата звернення 10.12.2023).

15. Гусєва В. О. Проблеми ідентифікації особи за ознаками зовнішності під час розслідування кримінальних правопорушень. *Теорія та практика судової експертизи і криміналістики*. 2021. Випуск 2 (24). С. 109-122.

16. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень: наказ Міністерства юстиції України від 08 жовтня 1998 року № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98 (дата звернення 10.12.2023).

17. Чорний С., Брендель О., Гратіашвілі Д. Автентифікація зображень на основі їх семантичної сегментації у нейронних мережах глибокого навчання з їх попереднім обробленням за методами фільтрації. *Теорія та практика судової експертизи і криміналістики*. 2022. Випуск 1 (26). С. 127-140.

18. Експертизи відео-, звукозапису. Офіційний сайт Тернопільського науково-дослідного експертно-криміналістичного центру МВС України. URL: https://ndekc.te.ua/news/mozhlivost-ekspertizi-vdeo-zvukozapisu (дата звернення 10.12.2023).

19. Особливості призначення судових експертиз: практ. порадникь/ М-во внутр. справ України; Експертна служба; Харківський наук.-дослід. експерт.-криміналіст. Центр. Вид. 2-ге, переробл. Харків, 2021. 92 с.

20. Коршенко В. Судова телекомунікаційна експертиза як джерело доказів під час розслідування кіберзлочинів. *Jurnalul juridic naţional: teorie şi practică.* 2017. № 2 (24). С. 192–194.

21. Білоус В., Латиш К. Судові експертизи радіоелектронних засобів як форма використання спеціальних знань під час

розслідування корупційних кримінальних правопорушень. *Наукові праці Міжрегіональної Академії управління персоналом.* 2022. Випуск 1 (61). С. 5-11. DOI: https://doi.org/10.32689/2522-4603.2022.1.1.

22. Бірюков В.В. Теоретичні основи інформаційно-довідкового забезпечення розслідування злочинів: монографія. Луганськ: РВВ ЛДУВС, 2009. 664 с.

23. Журавель В.А., Шепітько В.Ю. Автоматизовані інформаційні системи як засіб удосконалення розслідування вбивств. *Вісник Національної академії правових наук України*. 2017. № 1. С. 161-172.

24. Закон України Про правовий статус осіб, зниклих безвісти за особливих обставин. URL: https://zakon.rada.gov.ua/laws/show/2505-19#Text. (дата звернення 10.12.2023).

25. Положення Про Єдиний реєстр осіб, зниклих безвісти за особливих обставин. Затв. Наказом МВС України 22.08.2022 № 535. URL: https://zakon.rada.gov.ua/laws/show/z0998-22#Text. (дата звернення 10.12.2023).

26. Закон України Про державну реєстрацію геномної інформації людини. URL: https://zakon.rada.gov.ua/laws/show/2391-20#Text. (дата звернення 10.12.2023).

27. Інструкція з організації функціонування криміналістичних обліків експертної служби МВС України: затв. Наказом МВС України від 10.09.2009 № 390. URL: https://zakon.rada.gov.ua/laws/show/z0963-09#Text. (дата звернення 10.12.2023).

28. Положення про інтегровану міжвідомчу інформаційно-телекомунікаційну систему щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон: затв. Наказом Адміністрації Державної прикордонної служби України, Державної митної служби України, Державної податкової адміністрації України, Міністерства внутрішніх справ України, Міністерства закордонних справ України, Міністерства праці та соціальної політики України, Служби безпеки України, Служби зовнішньої розвідки України від 3 квітня 2008 р. № 284/287/214/150/64/175/266/7. URL: https://zakon.rada.gov.ua/laws/show/z0396-08#Text (дата звернення 10.12.2023).

29. Офіційний веб-портал – Головного управління розвідки Міністерства оборони України. URL: https://gur.gov.ua/content/war-criminals-rf.html (дата звернення 10.12.2023).

30. Clearview AI Principles. URL: https://www.clearview.ai/principle (дата звернення 10.12.2023).

31. «ТиХто» – додаток, який допомагає шукати окупантів. URL: https://vechirniy.kyiv.ua/news/64785/**(**дата звернення 10.12.2023).

32. Книга катів українського народу. База російських військових, які чинили злочини в Україні. URL: https://russian-torturers.com. (дата звернення 10.12.2023).
33. Російські воєнні злочинці. Онлайн-реєстр. URL: https://rwc.shtab.net (дата звернення 10.12.2023).

Information about the authors:
Latysh Kateryna Volodymyrivna,
PhD in Law, Associate Professor,
Assistant of the Department of Criminalistics,
Yaroslav Mudryi National Law University
77, Hryhoriia Skovorody str., 61024, Kharkiv, Ukraine
http://orcid.org/0000-0002-9110-116X

Demydova Yevheniia Yevheniivna,
PhD in Law, Associate Professor,
Associate Professor of the Department of Criminalistics,
Yaroslav Mudryi National Law University
77, Hryhoriia Skovorody str., 61024, Kharkiv, Ukraine
http://orcid.org/0000-0002-5049-7946

Kapustina Mariieta Vladyslavivna,
PhD in Law, Associate Professor,
Associate Professor of the Department of Criminalistics,
Yaroslav Mudryi National Law University
77, Hryhoriia Skovorody str., 61024, Kharkiv, Ukraine
http://orcid.org/0000-0003-1990-5259