УДК 343.1
DOI https://doi.org/10.32782/2524-0374/2023-3/131

IMPLEMENTATION OF THE DIGITAL OPEN SOURCES IN THE CRIMINAL INVESTIGATION PROCESSES

ВИКОРИСТАННЯ ВІДКРИТИХ ЕЛЕКТРОННИХ ДЖЕРЕЛ ПІД ЧАС РОЗСЛІДУВАННЯ У КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ

Ivanova S.S., 4th year student
Educational and Scientific Institute of Law of the Taras Shevchenko National University of Kyiv

The article explores the prospects of using digital open sources when applying modern investigative methods. The publication provides an overview of the benefits of using electronic open sources in criminal and human rights investigations, including their potential to reduce costs and the ability to quickly and efficiently retrieve large volumes of data.

The study also notes the possible shortcomings of using digital open sources, in particular, the reliability of the obtained materials. To ensure the accuracy and reliability of data collected from open electronic sources, the study highlights the need to provide investigative bodies with appropriate guidance.

The article also emphasizes the need to apply ethical principles in the process of using digital open sources in investigations. The author gives examples of national and international practices of using special means in the investigation process and modern trends in collecting and researching evidence obtained from open sources. In order to preserve individual rights and ensure that investigations are conducted in a fair and reasonable manner, there is a need for a clearly defined ethical legal framework to guide investigators in the use of digital open sources.

The benefits and importance of existing legal requirements that ensure impartial investigation of violations while respecting the rights of all parties are also discussed in this publication. The study highlights the importance of a sound regulatory framework governing the use of electronic evidence. The author advocates the need to create a procedure and standards for obtaining such evidence, in particular data for forensic examination. The author cites the experience of law enforcement agencies in Ukraine as an example of the basic development of rules for the use of digital data, in particular during a criminal investigation.

Key words: digital open sources, criminal investigation, digital evidence, open source intelligence, human rights, investigation of international crimes.

У статті досліджуються перспективи використання відкритих електронних джерел під час застосування сучасних методів розслідування. У публікації наведено загальний огляд переваг використання відкритих електронних джерел у кримінальних розслідуваннях і розслідуваннях у сфері прав людини, включаючи їх потенціал для зниження витрат, а також здатність швидко й ефективно отримувати значні обсяги даних.

Також у статті відзначаються можливі недоліки застосування відкритих електронних джерел, зокрема достовірність отриманих матеріалів. Щоб гарантувати точність і надійність даних, зібраних із відкритих електронних джерел, у дослідженні підкреслюється необхідність забезпечення органів розслідування відповідними рекомендаціями.

У статті також наголошується на необхідності застосування етичних принципів в процесі використання відкритих електронних джерел у розслідуваннях. Авторкою наводяться приклади національної та міжнародної практики використання спеціальних засобів у процесі розслідування та сучасні тенденції збирання та дослідження доказів, отриманих із відкритих джерел. Для того, щоб зберегти індивідуальні права та гарантувати, що розслідування проводяться справедливим і розумним способом, існує необхідність у чітко визначеній етичній правовій базі, яка б скеровувала слідчих у використанні відкритих електронних джерел.

Переваги та значення чинних правових вимог щодо забезпечення неупередженого розслідування порушень із одночасним дотриманням прав усіх сторін також обговорюються в цій публікації. Дослідження підкреслює важливість досконалої нормативної бази, що регулює використання електронних доказів. Авторка відстоює необхідність створення процедури та стандартів для отримання таких доказів, зокрема даних для судової експертизи. Авторка наводить досвід правоохоронних органів в Україні як приклад базової розробки правил використання цифрових даних, зокрема під час кримінального розслідування.

Ключові слова: електронні відкриті джерела, кримінальне розслідування, електронні докази, дослідження відкритих джерел, права людини, розслідування міжнародних злочинів.

In today's world, the internet has become an integral part of our daily lives. We rely on it for communication, entertainment, education, and even for conducting business transactions. However, with the increasing use of the internet, new challenges have arisen, such as cybercrime, fraud, and other illicit activities that threaten individuals, businesses, and governments worldwide. To combat these threats, investigators have had to adapt their methods and tools to the digital era, which has given rise to digital open source investigation.

A great deal of the population has direct access to the Internet, including the ownership of social media pages that often can verify the identity of its holder uncovering even the most intricate details about the person's life. From a long-term perspective, the strategy we chose to deal with this mass load of information can define the sphere of influence and its limits in light of respect for human privacy and the possible prevalence of society's need for protection.

The novelty of electronic evidence has widely spread across the globe proving the necessity of its engagement even in the most isolated independent jurisdictions. Facing the recent unfortunate events, humanity realized the need for a proper and accurate collection of each and every perpetration following strict guidelines which at the same time can grant resilience to some extent. The complexity of the issue brought up is multilevel, beginning with the tools of the evidence collection and resulting in the issue of admissibility that concerns not only a national judiciary but mostly the international institutions in charge of investigation and adjudication.

The research on that topic has been conducted by numerous scientists such as S. Albul, O. Bandurka, M. Budakov, I. Kondratiev, O. Korystin, Y. Maksimenko, A. Marushchak, G. Novytskyi, D. Banisar, K. Osakwe, A. Robert and others.

This article's objective is to highlight the significance of establishing regulations in criminal justice for digital investigative procedures while also recognizing the possible difficulties that may develop. The purpose is to encourage analytical conversations and develop a complete system that ensures credible rights protection in its fullness, correctness, and clarity by analyzing abroad practice and developing a pertinent legal framework. Ultimately, the article promotes the need for a judicial system that is more equitable and easily accessible while upholding the essential ideas of the rule of law. Further, it is demonstrated as necessary and advantageous for the legal theory and practice to conduct a thorough analysis of inter-

national experience before developing a legal framework. The study also emphasizes how crucial it is to strike a balance between the necessity for efficient investigation methods and the defense of individual rights.

As has been aptly mentioned in the scientific literature, at present, there is no single stable terminology that would define the evidence obtained from digital data carriers, nor the procedure for working with them, in particular in Ukraine. Therefore, in practice, questions often arise regarding the correct presentation of such evidence and its presentation in court [1].

One of the main advantages of digital open source investigation is its accessibility. This makes it easier to investigate international crimes or to work on cases that involve multiple jurisdictions. Moreover, digital open source investigation is typically less expensive than traditional investigation methods, as it does not require travel, surveillance, or other costly techniques.

Another advantage of digital open source investigation is its speed. In many cases, investigators can obtain information in real-time, allowing them to respond quickly to developing situations. This can be critical in situations where time is of the essence, such as in cases of child abduction or terrorism.

However, digital open source investigation also poses new challenges for investigators. For example, the vast amount of information available on the internet can be overwhelming, making it difficult to sift through and identify relevant information. Moreover, digital open sources investigation must be conducted in compliance with ethical and legal guidelines to avoid infringing on individuals' privacy rights.

The usage of internet open source data for human rights investigations has surged during the last few years. There has been a lot of experimentation, with the open source investigative space being seen as something of a Wild West – a new, disembodied digital frontier where anything goes, especially in social media research [2].

In essence, digital open source investigation is an important tool in the modern investigator's arsenal. It offers a range of advantages over traditional investigation methods, including accessibility, speed, and the ability to overcome certain challenges. However, it also poses new challenges that must be addressed, such as managing the vast amount of information available and ensuring compliance with ethical and legal guidelines. As technology continues to evolve, digital open source investigation will likely become an even more important aspect of investigation work in the future.

The increasing reliance on digital sources of information in modern times has given rise to new challenges for investigators. In order to ensure the reliability of conclusions and establish facts with confidence, it is necessary to apply uniform approaches and methods when using open sources in official investigations. This is particularly critical in international criminal and human rights investigations, where the use of digital open sources can provide valuable evidence that might not otherwise be accessible. However, the lack of a universal legal order creates obstacles in the accurate recording and examination of evidence in their clear, accurate, and full nature. These challenges highlight the necessity of developing standardized approaches and methods for digital open source investigation that can help to ensure the reliability of evidence and improve the accuracy of conclusions drawn from it.

The ratification of the Convention on Cybercrime [3], which was primarily designed for member states of the European Union, later was recognized by other nations due to the growing public danger that cybercrime poses and was a significant and effective step for Ukraine. This legal document granted protection from various aspects of cybercrime on the global level, obliging the Party of the Convention to adopt necessary legislation.

Information search and analysis using open sources for their further use by law enforcement agencies and the court can be operated based on different methods. As Mr. Zharkov notes, the US intelligence community is the originator of the term "intelligence from open sources" (Open Source Intelligence – OSINT), defines OSINT as one of the types of military intelligence, which is designed to search, collect and analyze information from publicly available sources [4]. Open Source Intelligence refers to the collection, analysis, and dissemination of information from publicly available sources, including news articles, social media, government reports, and academic research. It can be used to support law enforcement and national security efforts, such as tracking terrorist activity or identifying cyber threats.

In light of the topic discussed, there is a particular necessity to mention the Berkeley Protocol on Digital Open Source Investigations [5] which was composed in 2022 as a result of Berkeley Law's Human Rights Center (HRC) and the U.N. Human Rights Office's three-year fruitful cooperation. As it is referred by Berkley Law Center the document outlined marks the first global guidelines for using publicly available information online – including photos, videos, and other content posted to social media sites – as evidence in international criminal and human rights investigations.

Paying attention to the relevance of procedure aspects, rights of privacy, and guided investigative process, the authors seek to construct a balanced system compromising difficulties that arose from the standards of international courts and tribunals. Abiding by the general rule of the standard of proof in criminal jurisdiction we must acknowledge the distinction accompanying the international practice. While the bar for admissibility of evidence in international criminal courts and tribunals is generally lower than that of some national courts, the methods of evidence collection will still affect the weight judges give to the evidence.

The proper investigation process composed by the Berkeley Protocol includes six main phases namely online inquiry, preliminary assessment, collection, preservation, verification, and investigative analysis.

Analyzing the first stage, we can witness established types as follows: searching, which is the process of finding information and information sources by using basic or sophisticated search strategies; monitoring, which is the process of finding fresh information by repeatedly and persistently reviewing a set of reliable sources. The aspect of particular importance hereinafter is the absolute necessity of remaining vigilant of bias while conducting the investigation as a whole as well as its only element.

Whilst conducting a preliminary assessment the responsible body should estimate the criteria of relevance, reliability, the chance of item removal, the safety of the item, and subsequent duties concerning the following custody of the digital item. Moving on to the collection and preservation of the evidence, the information taken should be stored in its fullness, accuracy, and clearness as detailed as possible. For instance, regardless of the collection format, all available data on the material must be preserved, such as the source code of the web page, embedded media files, hush value, data of the collection and preservation processes, etc. The structure must be kept, safeguarding authenticity, availability, identity, persistence (integrity and viability of a digital item in technical terms), renderability, and understandability.

Apart from the selection of the data gathered, the veracity and validity of the information are verified through the analysis of the source, content, and technical data. Finally, the investigative analysis takes place in the eventual stage, contributing to the process of evaluating and interpreting factual data to provide substantial results applicable to case development or decision-making.

The protocol's investigation process ensures that infringements are thoroughly and impartially investigated, while also respecting the rights of all parties involved. Its elements are not only a simple guidance on the investigation process but an authentic handbook of practical issues that

should be embedded into national practice. A detailed regulation will be an instrument of avoidance of the matters of the misusage of powers or a mistake on the lack of practical knowledge. The abovementioned is a concept that serves the supreme purpose of conducting a fair trial, through the mitigation of the probability to fail to establish a legal order due to the inadmissibility of evidence.

As a result, the introduction of the Berkeley Protocol affects the concept of digital sources utilized for the purpose of investigation, making such data universally acceptable. Understandable access to consecutive information creates a vast of opportunities for the public to explore and contribute to the work of responsible bodies. The benefits of the evidence obtained from journalistic research, individual claims can create the most accurate event profile. Furthermore, since such access is not limited by a certain jurisdiction, a real course of events can be traced up to the live translation that grants a factual representation of any atrocities.

The adoption of legislation governing the use of electronic evidence is a necessary reaction to the new problems in criminal law and forensics brought on by the world's shift to the digital era. Furthermore, the development of processes and procedures for gathering electronic evidence is especially impacted by forensic evidence, which plays a significant role in establishing objective law [6].

The experience of Ukraine and its people can prove an absolute fundamental need of internalizing the guidelines on digital evidence utilization. Moreover, society has already been acquainted with services that thoroughly accumulate the information given to apply it further, especially in the judicial examination.

One such project is aimed at documenting and preserving evidence of human rights violations and atrocities through the use of technology. An EyeWitness was developed by the International Bar Association, and as a groundbreaking initiative has been widely recognized for its contributions to the field of international criminal justice [7].

The EyeWitness project utilizes a custom-built camera application that can be easily installed on smartphones or other mobile devices. This application enables users to record videos and take photographs of human rights violations, such as torture, forced disappearances, and extrajudicial killings. The collected data is then securely stored and analyzed by a team of forensic experts, who can use it to provide crucial evidence in trials against perpetrators of these crimes. Verifying the media uploaded, not only actual photo/video materials are being analyzed during the trial, but additionally embedded metadata that helps to demonstrate the authenticity of the footage.

Overall, the EyeWitness initiative marks a significant advancement in the field of human rights advocacy and documentation, offering an effective tool for those looking to hold human rights offenders accountable and pursue justice for victims. At the moment, more than 45 thousand media files have been recorded and have already made an impact during the investigation performed by the United Nations, the practice of the International Criminal Court, different European war crimes units, domestic courts, and international police forces.

The EyeWitness to Atrocities app has played a crucial role in documenting the human rights violations in Ukraine following the russian invasion. Between 24 February and 27 September 2022, the app's users uploaded a staggering number of visual and audio records that captured the appalling situation on the ground [8]. The footage revealed the extent of the damage inflicted on residential areas, educational institutions, cultural heritage sites, and commercial properties. The recordings also exposed incidents that had not received extensive media coverage at the time, indicating the value of EyeWitness accounts and citizen journalism in such conflicts. The evidence collected through the app highlights the importance of technology in documenting and preserving evidence of human rights abuses in conflict zones.

Due to the scale of the damage brought by the russian invasion, the Ukrainian government has also developed a system of reporting war crimes. Currently, anybody who has witnessed or suffered the consequences of war crimes can upload the evidence through the website or application which will be used to prosecute the responsible ones both on the national and international level [9].

Covering the topic of independent research initiatives, we would like to refer to the Bellingcat Investigation Team, which created a map of civilian harm in Ukraine [10]. and is a powerful tool for visualizing the widespread impact of the ongoing War in Ukraine on civilians.

By compiling and analyzing data from a variety of sources, including open source information and EyeWitness testimony, the map provides a detailed and comprehensive view of the harm suffered by individuals and communities throughout the country. The map allows users to explore specific incidents of harm, including civilian deaths and injuries, damage to infrastructure and homes, and other forms of violence and abuse. By highlighting the human toll of the conflict, the map serves as a critical resource for a better understanding of the dynamics of the conflict and advocates for greater protection for civilians.

It is worth mentioning that publicly available tools are present to maintain an independent investigation by the individual or to contribute their own efforts to a more extensive project. An example of the beforementioned would be an Online Investigation Toolkit [11] created by Bellingcat, which gives a detailed guide on the online available information used for various investigations, or a methodology on the topic.

We have already mentioned the aspect of widespread Internet access that grants an opportunity to experiment on the matter of digital investigation. Notable, practices used in private spheres are not always credible enough to be exposed before the officials of the State (or interstate) investigation, however, some of the approaches are genuinely worthwhile.

The knowledge of collaboration, deep internet research, and proper evaluation of the evidence with a regard to the safety measures of web anonymity make a great researcher while partly being accessible through the resources such as "Exposing the Invisible: The Kit" [12]. Using a variety of digital tools and tactics, the project has developed many strategies to assist people and groups in examining and exposing complicated social and political issues. Developing networks and collaborations, performing research and analysis, confirming information sources, and leveraging visual storytelling and data visualization are just a few of the tactics. The initiative places a strong emphasis on the value of morally and responsibly conducting investigations as well as the necessity of continuous learning and adaptation in the rapidly evolving digital environment.

In recent years, the use of open source intelligence has become increasingly important in many fields, including law enforcement, journalism, and academia. The availability of the vast amount of digital data, combined with the development of sophisticated analysis tools, has made it possible to uncover information that would have been difficult or impossible to access just a few years ago. Using open digital sources, the BBC team in the investigation on the Cameroonian soldiers in 2015 [13] was able to gather a profound piece of information from a video that was circulating on social media. They also used specialized tools for data analysis, such as verification of the visual content, including unique identifiers (people, buildings, flora, fauna). The element of particular interest is a video comparison analysis and spatial analysis, which help to examine different objects and landscape features at an appropriate resolution and check against satellite, geodata, or maps, comparing features of objects, persons, and locations [5].

Through the analysis of this data, the team was able to identify patterns and connections between the individuals

involved in the crime. This BBC investigation highlights the growing importance of open digital source investigation in uncovering latent crimes and other illicit activities. By leveraging the power of digital data and advanced analysis tools, investigators can shine a light on hidden networks and hold those responsible accountable for their actions.

Realizing the particular importance of the guideline's implementation in the legal governance of the latest investigative practices we are obliged to be aware of numerous challenges that could present frequent obstacles in the establishment of equitable and accessible justice.

In order to counterbalance possible hurdles legislator as well as the legal community have to remember to integrate a clear system of leverage that retain the proper level of impartiality and independence of every individual involved in the collection and examination of proof. Furthermore, the ethical standards must be evaluated while constructing a certain norm or a rule to prevent a chance of obstructing the rights of individuals which eventually leads to the court's recognition of the evidence as inadmissible.

One of the main arguments for the introduction of special regulatory acts would be its universal accessibility. An enlarged number of opportunities that become viable would allocate genuine freedom concerning such aspects as international cooperation in criminal matters, a profound reserve of data, precise reconstruction of the course of events in time and space, recognition of the national criminal procedures, and accordingly the evidence database on the international level (e.g., international criminal tribunal).

With the systematic examination of overseas practice, we would be able to construct a relevant and beneficial legal framework. Especially, in times of ubiquitous uncertainty, jurisprudence has to perform a function of stable ground saturated with the fundamental principles of the rule of law reassuring each social element of its sustainability and cohesion. Therefore, further exploration of the topic is highly encouraged to promote analytical discussions to devise the most accurate and comprehensive system guaranteeing credible rights protection in its fullness, accuracy, and clearness.

BIBLIOGRAPHY

1. Вінаков А. В., Манжай І. А. Окремі питання фіксації електронних доказів. *Актуальні питання протидії кіберзлочинності та торгівлі людьми* : зб. матеріалів Всеукр. наук.-практ. конф. Харків : ХНУВС, 2017. С. 86–87.
2. Koenig A., Irving E., McDermott Y., Murray D. New Technologies and the Investigation of International Crimes: An Introduction. *Journal of International Criminal Justice*. 2021. № 19(1). P. 1–7.
3. Convention on Cybercrime / Council of Europe. URL: https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf (дата звернення: 22.03.2023).
4. Жарков Я. М. *Наукові* підходи до визначення суті розвідки з відкритих джерел. *Вісник Київського національного університету ім. Т.Шевченка. Сер. Військово-спеціальні науки.* 2013. Вип. 30. С. 38–41.
5. Berkeley Protocol on Digital Open Source Investigations / Human Rights Center, University of California, Berkeley and Office of the United Nations High Commissioner for Human Rights. URL: https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf (дата звернення: 22.03.2023).
6. Moussa A. F. Electronic evidence and its authenticity in forensic evidence. *Egyptian Journal of Forensic Sciences.* 2021. № 11. URL: https://doi.org/10.1186/s41935-021-00234-6 (дата звернення: 22.03.2023).
7. About us. *EyeWitness to Atrocities:* website. URL: https://www.eyewitness.global/about-us (дата звернення: 22.03.2023).
8. EyeWitness submitted evidence of human rights violations committed in Chernihiv to UN Commission of Inquiry. *EyeWitness to Atrocities*: website. URL: https://www.eyewitness.global/eyewitness-submitted-evidence-of-human-rights-violations-committed-in-Chernihiv-to-UN (дата звернення: 22.03.2023).
9. Якщо ви стали потерпілим або свідком воєнних злочинів Росії – фіксуйте та надсилайте докази! *Офіс Генерального прокурора* : веб-сайт. URL: https://warcrimes.gov.ua/en/ (дата звернення: 22.03.2023).
10. Civilian harm in Ukraine. *Bellingcat*: website. URL: https://ukraine.bellingcat.com/?fbclid=IwAR3d_0-w_WuZn0mR74qJTA3yMwHzi-kHL-0EKq-IUFnTIsbNguXNWvV1BPVU (дата звернення: 22.03.2023).
11. Bellingcat's Online Investigation Toolkit. *Bellingcat*: website. URL: https://docs.google.com/spreadsheets/d/18rtqh8EG2q1xBo2cLNyhIDuK9jrPGwYr9DI2UncoqJQ/edit#gid=930747607 (дата звернення: 22.03.2023).
12. Exposing the Invisible. *The Kit*: website. URL: https://kit.exposingtheinvisible.org/en/ (дата звернення: 22.03.2023).
13. Cameroon soldiers jailed for killing women and children. *BBC news*: website. URL: https://www.bbc.com/news/world-africa-54238170 (дата звернення: 22.03.2023).