UDC 316.776:004.58
DOI https://doi.org/10.32782/2524-0374/2025-1/164

OSINT AS A NEW CHALLENGE TO DE-ANONYMIZATION OF A PERSON ON THE WORLDWIDE WEB

OSINT ЯК НОВИЙ ВИКЛИК ДЕАНОНІМІЗАЦІЇ ОСОБИ У ВСЕСВІТНІЙ МЕРЕЖІ

Bokshorn A.V., PhD, Associate Professor,
Assistant Professor at the Department of Administrative Law Disciplines,
Odesa State University of Internal Affairs

Chernetska V.V., Master Student (educational program "Criminal Analysis",
specialty 124 "Systems Analysis),
Odesa State University of Internal Affairs

In today's digital world, the issue of privacy protection is becoming increasingly important, particularly in the context of the constant development of technologies and access to open information. Operations based on open sources of information (OSINT) play a key role in the processes of analysis and data collection, which can lead to unauthorized deanonymization of a person in the online space. Given the wide range of open data available to any person through social networks, forums, blogs and other platforms, the use of OSINT tools has become a powerful mechanism for discovering personal information even without specialized technical skills. The authors consider possible risks to user anonymity, in particular in the context of social media, public records and geolocation services. Particular attention is paid to deanonymization practices through the analysis of behavioral patterns, interaction with other users, as well as using metadata. The paper also discusses measures to protect personal data and methods for minimizing the risks associated with the use of such technologies.We are talking about: not disclosing personal data to third parties and not reacting to various dubious messages about winning the lottery, promotions, etc.; the need to use only licensed software on all devices that can guarantee data security and do not forget to update it as necessary; refusing to use public Wi-Fi; the need to create reliable passwords and the need to periodically update them; minimizing posting your own photos on social networks; ensuring the privacy of your profile on social networks; avoiding the use of programs that may violate privacy (such programs include, for example, GetContact), etc. This article aims to raise awareness of the importance of maintaining privacy in the context of digital transformation and to promote the development of sound approaches to the use of OSINT from an ethical and legal point of view.

Key words: OSINT, open source intelligence, deanonymization of a person on the Internet, OSINT methods, OSINT tools, protection of human and civil rights through the prism of the individual's right to privacy, deanonymization, confidentiality, personal data, digital security

У сучасному цифровому світі проблема захисту приватності стає дедалі важливішою, зокрема в умовах постійного розвитку технологій та доступу до відкритої інформації. Операції, засновані на відкритих джерелах інформації (OSINT), відіграють ключову роль у процесах аналізу та збору даних, що може призвести до несанкціонованої деанонімізації особи в інтернет-просторі. Враховуючи наявність широкого спектра відкритих даних, доступних для будь-якої особи через соціальні мережі, форуми, блоги та інші платформи, використання інструментів OSINT стало потужним механізмом для виявлення особистої інформації навіть без спеціалізованих технічних навичок. Авторами розглянуто можливі ризики для анонімності користувачів, зокрема у контексті соціальних медіа, публічних записів і геолокаційних сервісів. Особлива увага приділяється практикам деанонімізації через аналіз патернів поведінки, взаємодії з іншими користувачами, а також за допомогою метаданих. У роботі також обговорюються заходи захисту особистих даних та методи мінімізації ризиків, пов'язаних з використанням таких технологій. Мова йде про: нерозголошення особистих дані стороннім особам та відсутність реакції на різноманітні сумнівні повідомлення про виграш у лотерею, акції тощо; необхідність використання на всіх пристроях тільки ліцензійного програмного забезпечення, яке здатне гарантувати безпеку даних та не забувайте оновлювати його по мірі необхідності; відмову про використання загальнодоступний Wi-Fi; необхідність створення надійних паролей та необхідність періодичного оновлення їх; мінімізацію розміщення власних фото у соціальних мережах; забезпечення приватності профілю у соціальних мережах; уникнення користування програмами, які можуть порушити приватність (до таких програм можна віднести, наприклад, GetContact) тощо. Ця стаття має на меті підвищити обізнаність про важливість збереження приватності в умовах цифрової трансформації та сприяти розвитку обґрунтованих підходів до використання OSINT з етичної та правової точок зору.

Ключові слова: OSINT, розвідка з відкритих джерел, деанонімізація особи в інтернеті, методи OSINT, інструменти OSINT, захист прав людини та громадянина через призму права особи на приватність, деанонімізація, конфіденційність, персональні дані, цифрова безпека

Problem Statement. OSINT tools provide the ability to collect a variety of information about people from publicly available sources, including, but not limited to, names, email addresses, home addresses, and location over a period of time. The use of modern electronic devices, including smartphones, fitness trackers, and the sharing of personal information through social networks and other online platforms, makes searching for information on the Internet a trivial task, especially for professionals. At the same time, it is important to understand that it is extremely important to ensure proper verification of the information obtained. Since the use of unverified data can lead to the formulation of incorrect conclusions and the adoption of incorrect decisions. This is especially important today, in the context of modern information warfare, where reflexive control can be actively used to manipulate the perception and actions of the enemy, it is necessary to approach the analysis of information obtained from open sources with great caution. In this context, the Russian-Ukrainian conflict has demonstrated that developing critical thinking skills and using advanced analytical tools can significantly improve the quality of open data analysis and, consequently, the quality of decisions made on its basis. However, the use of open source intelligence tools is relevant not only when it comes to war crimes. In fact, they demonstrate good performance in investigating various types of criminal offenses, the number of which has indeed increased since the beginning of the war. It is necessary to understand that it is extremely important to ensure proper verification of the information received. Since the use of unverified data can lead to the formulation of incorrect conclusions and the adoption of incorrect decisions. This is especially important today, in the context of modern information wars, where reflexive control is used to manipulate the perception and actions of the enemy, it is necessary to approach the analysis of information obtained from open sources with great caution. In this context, the Russian-Ukrainian conflict has demonstrated that the development of critical thinking skills and the use of advanced analytical tools can significantly improve the quality of analysis of open

data and, accordingly, the quality of decisions made on their basis [5]. Also, in the context of the study, we must not forget that there is a need to ensure proper protection of an individual's personal data. Issues of confidentiality and security are becoming increasingly relevant, and the increase in the use of OSINT for the purpose of deanonymization requires the development of new approaches and technologies for the protection of personal information.

Presentation of the main material. Open Source Intelligence (OSINT) is a concept, methodology and special technology for obtaining and using military, political, economic and other information from open sources in compliance with the norms of current legislation. Technologies are used for decision-making in the field of national defense and security, in investigations, etc. The methodology includes a number of methods: information collection, registration, accounting and analysis, analytical and synthetic processing of primary information, it also includes storage and dissemination of information, information security and presentation of research results.

After analytical and synthetic processing, primary information from open sources can become truly valuable knowledge that will help solve the tasks that may be set before law enforcement agencies, etc. A specific category of technical and human resources, sources of information and methods of their collection - all this distinguishes OSINT from other types of intelligence. Among the advantages of OSINT (in comparison with other types of intelligence) it is worth noting:

Availability. To use OSINT information sources, it is not necessary to conduct special measures or create complex technical intelligence systems. You just need to have a clear strategy - where and what to look for.

The volume of information sources. OSINT allows you to achieve the goal by processing a large volume of information resources, which is growing quite intensively even today. This advantage can also be considered a disadvantage. After all, the large volume of material that needs to be processed leads to the fact that you can not understand it, get confused, this makes it difficult to formulate an assessment of the usefulness of data for solving the task.

Versatility. With the help of OSINT today, it is possible to satisfy the vast majority of information needs of individuals interested in obtaining intelligence information. It should be noted that currently, information from open sources and publicly available information can be obtained from: the Internet (here we are talking about various forums, blogs, social networking sites, video sharing sites such as YouTube.com, Wikipedia, Whois records of registered domain names, Darknet web resources, etc.), diplomatic missions, information from religious organizations, national-level intelligence organizations, academic direction (we are talking about the results of scientific research, formatted into scientific articles, dissertations, etc.). In this context, one cannot ignore the “gray literature”, which includes economic reports, marketing research, etc.

Efficiency. The high degree of renewal of information resources allows you to quickly respond to changes in the situation, the state of intelligence objects in real time.

Ease of use. Any secrets are usually surrounded by barriers of secrecy labels, principles of information isolation, as well as special access modes. This creates certain obstacles for interaction and transfer of information to interested structures. As for OSINT, it can be transferred to any interested authorities without any problems.

Cost. Expenditures on open source intelligence are small. For example, in the US intelligence budget they make up only about 1%, which is usually defined as a very meager share.

OSINT technologies and methods allow you to obtain as much necessary information as possible in a short time and spending a minimum of resources (there are a sufficient number of free OSINT tools), which is quite important in conditions of martial law. Note that about 40% of all information on the Internet is free [3]. Among the OSINT methods that are actively used today to collect information from publicly available sources, it is worth noting:

Social network analysis. This involves studying the profiles of individuals on popular social networks, including Facebook, Twitter, LinkedIn, Instagram, etc. From social networks, you can learn a person's personal data, their interests, preferences, and the circle of people they communicate with. People who post information about themselves on social networks or dating services understand that it becomes available to all users of the resource and that, by law, this information can be interpreted as "public."

The point is that this does not require any special confidentiality, but in social networks there is also information that the user hides and makes it available only to a certain group of users, we are talking about a circle of users who are in the circle of “friends”. In this case, the Internet resource must offer the user special protection measures. The bodies that ensure the search for intelligence information from open sources process personal data that is publicly available on the Internet. This means that the consent of the personal data subject to processing is not required for information processing. However, there is one point that must not be forgotten - the administrator or owner of the data must prove that the processed personal data is publicly available. This means that you must either provide evidence that the data was taken from publicly available sources, or obtain the consent of the data subject, and then save this document. In addition, it is necessary to have a document confirming the public availability of the sources of personal data. At the same time, the issue of confirmation by the website owner of written consent to the processing of personal data remains relevant.

News and media monitoring. These sources provide information about world events, the activities of various organizations, and the activities of individuals (when it comes to famous personalities and politicians);

Geodata analysis. This method provides information about traffic, a person’s location, trips they take, etc.;

Search in open databases, including telephone directories, company registers, etc.

Web scraping and web page analysis. Web scraping is a technology for automated data collection and analysis from web pages that is actively used to process large amounts of information from Internet resources. This process involves extracting structured data (e.g., text, images, metadata, links) from various websites. The collected data can be used to analyze trends, identify patterns, or create databases containing relevant information for further analysis. The main stages of web scraping are: sending requests to web pages, parsing HTML code to extract the necessary data, and storing them in a format convenient for analysis. For this, specialized software tools and libraries are used, such as BeautifulSoup, Scrapy, Selenium or libraries for the Python, Java or R programming languages. Web scraping allows for the analysis of large data sets in real time, which is extremely important for various fields: economics, marketing, social sciences, media, as well as for identifying information trends. Web scraping is also used to monitor competitors, collect price data, and analyze public opinion on social networks and news sites. In such cases, not only the accuracy and efficiency of data collection is important, but also the ethics of this process, in particular regarding respect for the terms of use of resources and legislation on the protection of personal data. Since some websites may block access to their data through such tools, various techniques for bypassing blocking are used, which requires additional knowledge and skills in the field of computer technology.

Analysis of video and audio means. This method allows you to obtain data by analyzing language, sound traces and other audiovisual data.

Using open information sources. This includes checking books, reports, articles that are freely available.

Searching archives and databases of various documents. This method allows you to study the retrospective of a phenomenon, etc [4].

In this context, the issue of the balance between freedom of information and the right of an individual to privacy becomes relevant. Legislative initiatives in various countries indicate a high level of public interest in this issue. Various companies and agencies must carry out their activities in strict accordance with the instructions issued by their governing organizations. They may differ in their content, but in any case, information obtained using OSINT tools must be obtained in a way that does not violate the norms of current legislation on confidentiality, must not be used for malicious purposes and must be used only when necessary.

Through the prism of these challenges, future research in the field of OSINT should focus on developing ethical principles for the use of open information, as well as on creating modern technologies that can eliminate the risk of malicious use of data that may compromise fundamental human rights and freedoms.

In Ukraine, the use of open sources of information (OSINT) is regulated by a number of regulatory legal acts. Among them are the Constitution of Ukraine, the Law of Ukraine "On the Protection of Personal Data", the Code of Ukraine on Administrative Offenses, the Criminal Code of Ukraine, and the Civil Code of Ukraine. According to the Fundamental Law, every person has the right to protection of his or her dignity, honor, private life, intimate and family secrets. This means that the collection, processing and use of personal data without the consent of their owner is illegal and may violate human rights. Therefore, organizations must guarantee the security of personal data, collect it only for a specific purpose, store it for a limited period of time and provide individuals with the opportunity to refuse the collection of their personal data. Failure to adhere to the above ethical considerations in OSINT research, such as showing respect for the privacy of other people, complying with relevant laws and regulations, and ensuring that the information obtained is used exclusively for lawful purposes, may result in a violation of such articles of the Constitution of Ukraine as Art. 31, 32, 34 [1], Criminal Code of Ukraine [2] also contains provisions that provide for liability for the disclosure and collection of information constituting a state or official secret. In addition, according to this legislative act, the unlawful collection and processing of personal data that violates the requirements of the law may be qualified as a violation of human rights. Inappropriate use of OSINT methods may lead to the perpetrators being held legally liable. Copyright cannot be ignored in this context. When collecting, analyzing or using data from open sources, which include Internet resources, social networks or public databases, it is imperative to comply with the copyrights on the said data. You cannot make copies and use the obtained information for your own interests and without the consent of their owners. It is important to collect only those data that are in the public domain for general use; it is necessary to follow the rules for collecting and processing personal data. And also remember that collecting and using information for the purpose of harming other persons may be classified as a crime and may have serious consequences.

Conclusions. The study of the use of OSINT technology as a tool for deanonymizing an individual in the online space opens up significant potential for collecting data about individuals, while at the same time raising deep questions about privacy and security. Despite the usefulness of OSINT in many areas, its ability to deanonymize poses a real risk to the personal confidentiality of individuals. The growing use of digital technologies and easy access to voluminous data on the Internet only increase the need for the protection of personal data. The prospects for the development of OSINT tools are impressive due to the constant progress in data processing and analysis technologies. It should be noted that the above information is useful for individuals who use open source intelligence tools. However, one cannot ignore the fact that individuals themselves must take care of the protection of personal information on the World Wide Web. The basis for the use of OSINT tools is a digital trace. To protect yourself, you should minimize it. This can be done in the following ways:

– do not disclose personal data to third parties and do not respond to various dubious messages about winning the lottery, promotions, etc.;

– use only licensed software on all devices that can guarantee data security and do not forget to update it as necessary;

– do not use public Wi-Fi;

– use VPN when using gadgets;

– create reliable passwords and update them periodically (it is advisable to do this at least once every few months);

– use two-factor authentication. It demonstrates good performance in terms of protection and allows you to protect personal data from attackers at a fairly high level;

– do not open links and do not go to sites that seem suspicious to you;

– download applications and programs only from official sites;

– minimize posting your own photos on social networks;

– ensure the privacy of your profile on social networks;

– do not use programs that may violate privacy (such programs include, for example, GetContact), etc.

BIBLIOGRAPHY:

1. Конституція України: Закон № 254к/96-ВР від 28.06.1996. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 25.12.2024)

2. Кримінальний кодекс України: Закон № 2341-III від 05.04.2001. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 28.12.2024)

3. Ланде Д. В. Правові питання конкурентної розвідки. Інформація і право. 2020. № 2(33). URL: http://ippi.org.ua/lande-dv-pravovi-pitannya-konkurentnoi- rozvidki-st-51-68 (дата звернення: 21.12.2024)

4. Опірський І.Р., Ангельська О.В., Главацбка А.Л. Дослідження технології використання OSINT як нової загрози з деанонімізації особи в інтернет просторі. Кібербезпека: освіта, наука, техніка. 2024. №1 (25). С.19-50.

5. Varzhanskyi,I. (2023). Reflexive Control as a Risk Factor for Using OSINT: Insights from the Russia–Ukraine Conflict. International Journal of Intelligence and CounterIntelligence, 1–31. https://doi.org/10.1080/08850607.2023.2228489