EASTERN EUROPEAN JOURNAL OF TRANSNATIONAL RELATIONS

Using Anti-OSINT to Create a Positive Image of Internet Users to Prevent Criminal Acts

Marcin Konieczny
Institute of Law and Administration
Pomeranian University in Slupsk, Poland
marcin.konieczny@upsl.edu.pl
ORCID 0000-0002-1798-1509

Abstract. The role of using anti-OSINT to promote a positive image of Internet users and fight cybercrime is becoming increasingly important in the era of digital transformation. Therefore, the purpose of this study was to analyse the specific features of using OSINT as a legal means of obtaining and using Internet user data. To fulfil this purpose, various methods were employed, namely: dialectical, comparative legal, systematisation, descriptive, and systemic analysis. The analysis found that OSINT can be quite vulnerable to disinformation, as electronic identifiers can be easily modified, which increases the risk of falsifying the personal data found. It was found that there are methods of obtaining data, such as information about the operating system, fonts, screen settings, and plug-ins, which allow for more reliable user identification. This is becoming key to improving the effectiveness of intrusion detection systems and identifying potential intruders in the network. The study emphasised the need to take steps to change the culture, including reducing the attractiveness of abuse among users. This makes such negative behaviour less attractive and less supportive. One possible measure that can be taken is to limit the ability to create multiple accounts for a single user, which can help prevent "long-term" negative effects. To ensure the ethical use of OSINT and prevent negative consequences, it is vital to develop and follow clear rules that follow privacy and data protection laws. This will help create a prominent level of trust and security in the online environment.

Keywords: information from open sources, cyberspace, privacy, data analysis.

JEL Classification: D83, L86, K42, K24.

Citation: Konieczny, M. (2025). Using Anti-OSINT to Create a Positive Image of Internet Users to Prevent Criminal Acts. *Eastern European Journal of Transnational Relations*, *9*(2), 25-35. https://doi.org/10.15290/eejtr.2025.09.02.02.

Publisher's Note:

Copyright: © 2025 Author. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY 4.0.) license (https://creativecommons.org/licenses/by/4.0/).

1. INTRODUCTION

The development and implementation of advanced IT technologies, specifically the development of Internet marketing and cross-site tracking systems, have led to the emergence of practices that violate the privacy of individuals. Companies operating on the Internet collect large amounts of personal information, such as browsing history, and actions taken by users on web resources. This may include identifying a user by the unique technical characteristics of their device, which creates a so-called "fingerprint" that is used to create a user profile.

The relevance of using anti-OSINT to create a positive image of Internet users and prevent criminal acts is that in the digital world, the protection of personal information and privacy of users is becoming increasingly important. Criminal elements are actively using online sources to commit cybercrime, such as fraud, identity theft, and identity-related crime.

This type of intelligence is receiving increasingly more attention in Polish academic circles. For instance, Kędzierska (2022) emphasises that there are two principal ways of understanding intelligence gathering: in a narrow sense, it is a single act of information gathering, while in a broad sense, intelligence covers a series of organised activities (intelligence cycle).

According to Ciekanowski et al. (2023), the optimum structure of international security guarantees in cyberspace is an urgent challenge that should be a priority for all countries seeking to protect their citizens from cyberthreats. Current challenges in the field of cybersecurity include the need for international cooperation, the development of cooperation methods, and the formulation of new legal norms.

Wolski (2022) establishes that the role of OSINT, both qualitatively and quantitatively, will continue to grow as a result of the development of online media and changes in people's lifestyles. This is a global trend that encompasses not only the technological revolution, but also changes in the cultural, social, and economic dimensions of society. The global trend of the growing role of OSINT is reflected not only in the technological sphere, but also in the cultural, social, and economic contexts. For instance, the use of OSINT helps to identify and analyse trends in people's consumer approach to online media, their interests, and behavioural changes. This can be of great importance for business, politics, and social sciences, allowing for informed decision-making based on up-to-date information from the online environment.

According to Goryca (2023), the key purpose of analysing information from open sources is to obtain data on potential threats to life and property that are essential for the state or organisation. This analysis is aimed at identifying potential hazards and risks to plan and implement preventive measures to ensure the safety and security of these facilities in the long term. Analysing information from open sources is critical to ensure the security and protection of life and property of strategic importance to the state or organisation. This analysis helps to identify potential hazards and risks with sufficient predictability, which allows for the development and implementation of preventive measures to prevent possible threats in the long term. This approach is key to ensuring the stability and security of the entire society.

Lakomy's (2023) research focuses on the use of personal data protection rules in the context of investigating potentially dangerous individuals, including members and supporters of violent extremist groups. Furthermore, the researcher considers possible threats to the security of the researcher and the scientific infrastructure used in OSINT projects. Analysing possible threats to the security of the user and scientific infrastructure is vital to ensure the efficiency and safety of research. Consideration of these aspects helps to increase the level of data security and reduce risks for research participants and researchers.

Lewulis (2022) addresses a crucial issue of modern criminal law related to the use of digital evidence in court proceedings. This is especially true in the Internet era, where a considerable part of the evidence of an informational nature is available online. The in-depth legal analysis provided in this study helps to understand how this digital evidence fits into existing judicial procedures, striking a balance between the protection of human rights and effective justice.

While legal scholars have shown considerable interest in this subject, there remains a significant gap in scientific exploration of certain facets. Specifically, the efficacy of anti-OSINT strategies, the societal and psychological impacts of employing anti-OSINT for safeguarding user data confidentiality, and the ethical utilization of acquired data within privacy frameworks require deeper investigation. Thus, it can be argued that the use of anti-OSINT to create a positive image of Internet users to prevent criminal acts is becoming increasingly relevant both in practice and among academic groups.

The purpose of this study was to identify promising ways to use anti-OSINT to prevent criminal acts aimed at identifying and preventing the misuse of users' personal data.

2. MATERIALS AND METHODS

The study employed a dialectical method that offered a better insight into the essence of OSINT. The dialectical method allowed for a deeper understanding of the substance of employing OSINT. This implies consideration of not only technological aspects, but also socio-cultural, economic, and legal factors. For instance, consideration of societal needs for protection against cybercrime, technological capabilities in the field of cybersecurity, and the effectiveness of legal regulation are key aspects that determine the role and significance of anti-OSINT.

The systematisation method was used for a comprehensive investigation. This method has become a key tool for organising and structuring the data obtained in the context of using anti-OSINT to create a positive image of Internet users. The systematisation method was used to organise and group the data obtained on various aspects of this problem, such as technical aspects of anti-OSINT use, ethical issues, social consequences, etc. This method helped to consider the system as a whole, specifically, to factor in the interconnections and interactions between its constituent elements.

The application of the comparative legal method helped to analyse the practices of the European Union in regulating artificial intelligence, specifically in the context of OSINT. The methods of descriptive and system analysis were used to establish the factors influencing the development of OSINT.

The use of the formal legal method helped to investigate the existing regulations in the field of cybersecurity, especially in relation to the use of anti-OSINT, the rights of Internet users, and the prevention of crime in the digital environment. Using this method, the study analysed the existing regulations in the field of cybersecurity, which helped to determine the legal framework and mechanisms for regulating these issues, identifying problematic issues and formulating prospects for further legal research in the context of using anti-OSINT for a positive image of Internet users and combating cybercrime.

The study also employed methods such as concretisation and generalisation. The method of concretisation was used to identify problems associated with the application of anti-OSINT to create a positive image of Internet users. This method helped to identify the key aspects and factors that complicate the effective implementation of this strategy. The method of generalisation helped to systematise the data and draw general conclusions about possible solutions to the identified problems. The use of various methods helped not only to identify problems in this field, but also to highlight ways for further improvement in this area. A detailed analysis and concretisation of the problems was carried out by investigating the practice of using anti-OSINT in various fields, including legal, social, and technical aspects, which offered an insight into the main challenges and potential obstacles to the successful implementation of the strategy of creating a positive image of Internet users through anti-OSINT.

To fully understand and substantiate the problematic, the study used the norms of various legal sources, namely: Directive (EU) 2016/680 (European Parliament and Council of the European Union, 2016a), the General Data Protection Regulation (European Parliament and Council of the European Union, 2016b; GDPR, 2018), the White Paper (European Commission, 2020), etc.

3. RESULTS

Open-source research is an essential component of intelligence activities. One of the technical intelligence methods that includes monitoring information from open sources, analysing this information and preparing reports for decision makers is Open-Source Intelligence (OSINT). This is specialised information that is gathered and structured to answer concrete questions (OSINT Telegraph, n.d.).

OSINT activities include collecting and analysing official documents, statutes, monitoring new scientific developments, data from databases, commercial and government websites, and online diaries from other sources. Generally, OSINT-based intelligence tools include a range of resources (Table 1).

Table 1

OSINT intelligence tools

Name of the application, service, or search engine	Functions
OneLook, Keyword Tool, Answer the Public	help to establish the search target
Hash At It, Social Search	detect mentions of the query in all leading social media and other platforms, not limited to them
Watson News Explorer, News Now, All You Can Read	perform quick news analysis aimed at identifying trends in search topics
Selection Search, Infinite Scroll for Google	applications that improve conventional search
Google Dorks, Google Hacking	special technique used by the media, investigative agencies, security engineers, and any users, the essence of which is to create queries in various search engines to identify concealed information and vulnerabilities that can be found on publicly accessible servers

Note. Source: compiled by the author of this study based on OSINT toolkit. (n.d.); Frankivsk District Court of Lviv (2023).

In this context, the process of searching for and processing information involves several stages. The first stage is to formulate the task – one needs to clearly define the task and analyse the analytical problem. The second stage is planning, which involves developing a plan for gathering information about the problem. At this stage, it is decided what exactly will be checked and analysed. It is important to clearly define goals and objectives. To perform search tasks, methods and tools are used to help identify and obtain the necessary information. The next stage involves analysing and evaluating key sources and their content. Analysis is a key factor in interpreting large amounts of data. The collection of information should be aimed at achieving certain goals. The analytical functions of OSINT include content analysis of information materials, reviewing the results of a thematic selection in the form of quotes (results of information collection on the Internet, statistical analysis of information sources covering events (OSINT Telegraph, n.d.).

Thus, the use of OSINT intelligence can answer many of the questions that decision-makers have and also focus the efforts of intelligence agencies on more complex and "narrow" tasks. OSINT technology is one of the key technologies for "in-depth collection" of multi-format information of various levels, as well as the development of new knowledge based on it. The dissemination and use of verified information from open sources facilitates the exchange of such information, as no covert methods or secret sources are used to obtain it.

The existing protocols governing the handling of such data typically focus on law enforcement entities. For instance, the European Union has the authority to process personal information and construct profiles of individuals "suspected of or planning to commit a criminal offense" (European Parliament and Council of the European Union, 2016a). However, these guidelines do not extend to the realm of scientific research, leaving scientific projects related to identifiable online user behavior without a solid legal foundation. This raises the question of what steps should be taken to navigate this ethical quandary.

Under the current standards commonly used for processing personal data in scientific endeavors, three distinct approaches can be identified. Firstly, research initiatives should steer clear of any actions that might be construed as profiling individuals online. This principle is evident, for example, in the decision not to disclose the identities behind usernames or email addresses of users sharing materials linked to terrorism. Analyzing IP addresses or metadata from shared images could also pose challenges by revealing user locations. Adopting this strategy helps sidestep potential issues associated with handling personal data of individuals involved in terrorist activities.

One potential strategy is to pseudonymize or anonymize any incidental discoveries involving personal data. Pseudonymization involves excluding specific personal identifiers, like usernames, from the project database to prevent revealing an individual's identity. However, this method could impact study outcomes, especially if the person under analysis is crucial in terrorist online interactions. This underscores the importance of exploring alternatives, such as anonymization or pseudonymization.

Anonymization entails removing "personal identifiers, both direct and indirect, that could lead to identifying an individual" (General Data Protection Regulation, GDPR). This approach is generally preferred as pseudonymized data may still be subject to data protection laws due to re-identification risks. Nonetheless, OSINT is susceptible to misinformation, and electronic identifiers can be easily altered, increasing the risk of falsifying discovered personal data.

Moreover, as outlined in the White Paper on Artificial Intelligence, safeguarding research participants from potential harm is crucial. Sharing such information with authorities could jeopardize innocent internet users unrelated to terrorism, especially considering instances where terrorist organizations have stolen personal data online. For example, followers of the Islamic State hacked random Twitter accounts to disseminate propaganda, highlighting the need for robust protection measures.

The authentication of this data could potentially lead to the profiling of individuals through "online identifiers," raising legal concerns about such practices. Conversely, certain accidental discoveries might aid in uncovering the real identities of terrorist group members. Therefore, the appropriate course of action in this ethical dilemma hinges on specific factors like the nature of the identified personal data and its link to terrorist acts. This complexity underscores the need for deeper ethical deliberation and research on the matter.

By analysing this information, one can identify a user as a new one and assign them a certain rating even before verifying their identifiers. After examining the data and considering legitimate and suspicious user actions, the system determines the user's score and decides on further steps. For instance, if a user's rating exceeds a certain value according to certain criteria, they are allowed to continue interacting with the system. In the case of a lower rating, additional information about the user may be required, and in the worst case, if the system detects suspicious data, the account may be restricted or blocked.

Apart from collecting information to ensure the security of web resources, websites also use user data for marketing purposes. For example, prices for goods may differ depending on the operating system on the user's device (iOS, Android). In addition, depending on the location, the hotel listings on the websites may change to suit one's preferences and accommodation needs.

Modern information systems use various methods of identification based on storing IP addresses of visitors' computers and cookies on their computers. However, there are disadvantages to both of these methods. For instance, dynamic IP addresses allocated to users from the Internet service provider's pool can reduce the reliability of identification, as can the use of proxy servers and anonymisers. In case of cookies, their linking to a particular

browser can make identification more difficult when using multiple browsers, and there is a risk of data being replaced or deleted.

However, there are methods for obtaining data that indicate the user's working environment, such as operating system data, fonts, screen settings, plug-ins, etc. Systematic evaluation and analysis of this data allows achieving a prominent level of online identification efficiency. The use of such methods increases the reliability of user identification, which is essential for optimising intrusion detection systems and identifying potential intruders in the network.

The study's overarching finding indicates that platforms can shift their culture to decrease the appeal of abusive actions among users, thus making such conduct less appealing and dissuading it. One potential strategy is to restrict users from creating multiple accounts, thus mitigating potential long-term negative effects. Currently, when a user gets blocked from one account, they can promptly create another, allowing them to persist in their inappropriate conduct.

Therefore, in protecting privacy in the legal environment, it is vital to factor in not only the conventional aspects, but also new challenges arising from the development of modern technologies. The legal aspects of using user tracking tools, such as trackers, are particularly important, as they directly affect cybersecurity, information, and personal data protection. Therefore, the use of anti-OSINT as a means of creating a positive image of Internet users is an essential element in the fight against criminal activity in the online environment. This technology is aimed at detecting and preventing the misuse of users' personal data for illegal purposes, such as fraud, cyberbullying, identity theft, and other forms of cybercrime.

To ensure that OSINT does not have negative consequences and to promote its ethical use, clear rules that follow privacy and data protection laws must be developed and enforced. This approach will help ensure a prominent level of trust and security in the online environment.

Companies that provide OSINT tools and platforms should also actively support the ethical use of these technologies by developing policies and tools to prevent potential misuse and ensure data privacy. For instance, social media can implement privacy controls that allow users to control access to their personal information and limit its use for OSINT purposes.

It is also important to cooperate with regulators and law enforcement authorities to develop guidelines and best practices for the use of OSINT. This will help reduce the risks associated with this technology and ensure an adequate level of protection of confidential information. Other security measures include limiting the amount of personal information shared online, implementing strong password policies, and regularly updating software and systems.

Additionally, it is vital to cooperate with law enforcement agencies and software developers to quickly respond to potential threats and detect criminal activity in the online environment. It is also necessary to conduct ongoing training and awareness campaigns for users on Internet safety and the importance of ethical use of information technology.

When discussing contemporary OSINT, which operates on the basis of the Internet, it is impossible not to mention cybercrime. Cyberspace, being an integral part of modern development, has become not only an environment for the exchange of information, but also an arena for numerous crimes that violate the legal order. The most serious threats include: phishing (data theft through fake messages), cyberterrorism (politically motivated attacks on critical infrastructure and state systems), and the spread of malware, such as viruses, worms, and Trojan horses, which are used to steal data or take control of devices.

The list of these crimes also includes hacking (unauthorized access to systems), cyberstalking (harassment of victims online), and other forms of abuse, such as grooming and spoofing. Statistics show a dynamic increase in cybercrime, which affects both individuals and businesses - the latter, especially small businesses, are often the target of attacks leading to serious financial losses and even bankruptcy. In the face of criminals constantly improving their

methods and the increasing digitization of life, it is crucial to strengthen IT security and user awareness of cyber threats (Konieczny, 2023).

4. DISCUSSION

The Polish scientific literature defines the concept of "open-source intelligence", which describes the process of gathering intelligence based on publicly available sources, such as media analysis and journalism (Goryca, 2023). According to Riebe et al. (2023), this method is not secret or illegal, as it is based on open sources. As noted above in the research findings, OSINT is a technical intelligence method that involves monitoring information from open sources, analysing this information and preparing reports for decision makers, i.e., specialised information that is gathered and structured to answer concrete questions. This definition is the most appropriate.

Khadim et al. (2023) emphasize that the selection of detection methods and available open sources significantly relies on the research goals. While acknowledging this viewpoint, it's crucial to recognize that these choices are also influenced by the technical intricacies of the Internet layer being studied. For instance, within the external network, OSINT primarily serves to map online information ecosystems supporting violent extremist groups or gauge their propaganda efforts. Specifically, Kamal (2023) highlights that many OSINT initiatives in this domain start with "Google hacking", leveraging advanced search engine parameters and commands. However, for precise outcomes, "Google hacking" must be complemented by specific keywords related to terrorist plans. Raharjo (2023) further underscores the need to utilize Salafi-jihadist terminology and terms associated with the Islamic State's key publications, leaders, structure, or ideology to pinpoint their online addresses accurately. Furthermore, there are various ways to automate search queries that web crawlers typically use, such as using Selenium and Python scripts, and then manually reviewing the search results.

The available methodologies and tools offer three distinct strategies for analyzing surface network domains. The initial strategy concentrates on exploring the technical aspects of websites, enabling the retrieval of data regarding the registrar (via who.is) or the actual IP address of the site. Moreover, this approach facilitates the identification of other sites hosted on the same server using reverse IP lookup technology. Although this data collection process can be laborious, it can be streamlined and expedited through specialized web crawlers and intelligence software. Notably, tools like SpiderFoot, as highlighted by Papayamma et al. (2023), aid in uncovering external links within a domain, providing insights into the structure and interconnections of the terrorist information ecosystem.

The second strategy, as proposed by David et al. (2023), emphasizes extensive data extraction and processing from surface web domains. A variety of Python scripts serve this purpose effectively. For instance, Metagoofil automates the detection, collection, and analysis of metadata from text files accessible via a specified URL. Another notable tool, Recon NG, offers a broad array of functionalities, including the identification of email addresses, concealed files, and subdomains. It's worth mentioning that many of these data extraction tools have dual applications, commonly utilized for both OSINT investigations and penetration testing purposes.

The third category of tools, as outlined by Hadi et al. (2023), focuses on analyzing individual files discovered on Internet addresses associated with terrorism. This is achieved using either standalone programs or simple browser add-ons. For instance, Exif Viewer enables the extraction of metadata from image files, potentially revealing GPS coordinates indicating the image's capture location. While this method presents opportunities for counter-terrorism efforts, it is not extensively employed in investigations. Nonetheless, these techniques aid in gathering data about the geographical distribution of interconnected terrorist domains and accounts, assessing the magnitude of propaganda disseminated through specific URLs, and uncovering technical attributes of propaganda materials.

Expanding on this, Putter & Henrico (2022) and Narasimhan et al. (2023) highlight that beyond the surface web, OSINT has also been integral in examining terrorist activities on social media platforms like Facebook and Twitter. These platforms serve as conducive environments for open-source intelligence analysis due to the

abundance of potential investigative subjects they offer. It's worth acknowledging that social media platforms have been extensively utilized by followers and affiliates of violent extremist groups.

There are two distinct categories of platforms concerning OSINT capabilities. The first group, emphasizing privacy, offers limited integrated search functionalities accessible solely to registered users. Facebook is an example of a platform following this approach. This restricted access could be a contributing factor to the decline in research concerning terrorist activities on such social networks in recent times. On the other hand, the second category relies on specialized web crawlers. However, their efficacy is often hindered by the scanning protection mechanisms deployed by numerous clandestine services, limiting their effectiveness.

Considering all the above aspects, despite its considerable potential, information obtained from open sources is not a universal solution in conducting online research of terrorist propaganda. It has its limitations and cannot be considered a "silver bullet". Usman et al. (2023) have identified a range of issues that need to be solved before launching open-source research projects. These problems include the difficulties associated with the massive amount of data on the Internet, which is usually unorganised by nature. Classifying and managing them poses serious challenges. In addition, the researchers using this method may be vulnerable to misinformation. Verification of information from open sources requires complex and time-consuming processes, and in some cases even becomes impossible.

Additionally, Obaidat et al. (2025, July) highlight that certain segments of the dark web, like Freenet or ZeroNet, leverage peer-to-peer technology. This unique setup means that domains hosted on these networks don't rely on traditional hosting servers like those on the Clearnet. Instead, each user visiting these sites contributes to their distribution, presenting a heightened ethical concern for researchers. Simply accessing terrorist websites within these networks can inadvertently support them, potentially expanding their digital reach through the researcher's actions. This ethical dilemma, intertwined with international law, poses a serious risk of criminal liability for scholars, a topic that hasn't received thorough exploration within academia. The absence of definitive solutions adds complexity to researchers' efforts in exploring these environments.

To address these challenges, two approaches are worth considering. First, any research focusing on P2P networks should incorporate mechanisms to automatically block the sharing of visited locations, although the technical feasibility of this remains uncertain. Current solutions primarily rely on manual intervention to halt hosting, leaving room for inadvertent legal violations. Secondly, researchers venturing into these realms should engage with law enforcement and anti-terrorism authorities before commencing their projects. Collaborating with these entities is crucial to navigating the legal intricacies and ensuring compliance with international regulations.

Finally, it is worth mentioning that the methods used in anti-OSINT are the main tool for protecting personal data in the fight against cybercrime. They cover a wide range of activities, starting with a detailed analysis of content published on the internet and the identification of key cybersecurity objects and their interconnections, ending with the targeted collection and processing of information. This also includes the creation of complex networks of objects, which aims to ensure reliable protection of personal data in the online environment. American intelligence services use terms "intelligence collection disciplines" and "intelligence sources" to describe the main methods and sources used to collect intelligence (Table 2).

Table 2

Types of Intelligence Collection in FBI and CIA/Intelligence Community (IC)

FBI	CIA/Intelligence Community (IC)
– Human Intelligence (HUMINT) – Signals Intelligence (SIGINT) • telemetry intelligence (TELINT) • electronic intelligence (ELINT) – Imagery Intelligence (IMINT) – Measurement and Signatures Intelligence (MASINT) – Open-Source Intelligence (OSINT)	– Signals Intelligence (SIGINT) • communications intelligence (COMINT) • electronic intelligence (ELINT) • foreign instrumentation signals intelligence (FISINT) – Imagery Intelligence (IMINT) – Measurement and signature intelligence (MASINT) – Human intelligence (HUMINT) – Open-Source intelligence (OSINT) – Geospatial intelligence (GEOINT)

Note. Source: compiled by the author of this study based on "Intelligence Studies" (n.d.).

American intelligence services provide a valuable model for analysis thanks to their sophisticated data collection methods, which enable international comparisons. The main difference between a novice and an OSINT expert lies in the depth of analysis. A novice limits themselves to superficial data, while a specialist examines details: activity, publication dates, elements in the background of photos, and uses pseudonyms to find additional information. The goal of OSINT is to systematically collect data in order to create a comprehensive profile of an object, revealing hidden connections and enabling behavior prediction. There are two methods: passive – not revealing one's identity, using publicly available sources; and active – direct interaction with IT infrastructure, port scanning, and vulnerability detection (Congressional Research Service, 2007).

The line between legal OSINT and illegal activities is drawn in four key dimensions: the source of the data, the method of obtaining it, the purpose of the analysis, and respect for privacy. An activity is legal when it is based on the passive collection of information that has been knowingly made public by users, in a manner that respects platform regulations and serves legitimate purposes such as research or security. However, this line is crossed when security measures are actively breached (e.g., through phishing or hacking), data leaks are exploited, or information is processed for the purpose of harassment, blackmail, and unfounded profiling. Ultimately, therefore, it is not the availability of data itself that determines its legality, but whether the method of obtaining it and the context of its use violate the law and the autonomy of the individual.

5. CONCLUSIONS

The use of anti-OSINT, used to protect personal information and prevent its misuse, can play a key role in raising users' awareness of digital security. It will also contribute to a positive image of users online, which can make the Internet safer and more welcoming for all participants, helping to reduce criminal activity in the online environment. Therefore, the use of anti-OSINT as a means of creating a positive image of Internet users is an essential element in the fight against criminal activity in the online environment. This technology is aimed at detecting and preventing the misuse of users' personal data for illegal purposes, such as fraud, cyberbullying, identity theft, and other forms of cybercrime. Thanks to anti-OSIINT, users can be confident in their security and privacy

in the online environment, which helps to increase trust in online resources and reduce the risk of cybercrime. Such a positive image is reflected in the perception of users in social media, business, and other areas of online interaction, contributing to a safer and more trusted environment for all members of the online community.

OSINT has now become a valuable tool in many industries, but as its popularity has grown, so has the concern about its possible misuse. To ensure that OSINT does not have adverse consequences and to promote its ethical use, clear rules that follow privacy and data protection laws must be developed and enforced. Such approach will help ensure a prominent level of trust and security in the online environment.

Companies that provide OSINT tools and platforms should also actively support the ethical use of these technologies by developing policies and tools to prevent potential misuse and ensure data privacy.

It is also important for companies to cooperate with regulators and law enforcement authorities to develop guidelines and best practices for the use of OSINT. This will help reduce the risks associated with this technology and ensure an adequate level of protection of confidential information. Other security measures include limiting the amount of personal information shared online, implementing strong password policies, and regularly updating software and systems.

Prospects for further research should include the effectiveness of anti-OSINT strategies, as well as the socio-psychological consequences of using anti-OSINT in ensuring the privacy of user data.

REFERENCES

Bangsawan, M. I., Santoso, B., Diarti, D. K., Mahendra, S., & Kubota, E. (2020). Personal data protection policy during Covid-19 pandemic. *Law and Justice*, 1, 21-31. https://doi.org/10.23917/laj.v8i1.1558.

Block, L. (2023). The long history of OSINT. *Journal of Intelligence History*, 1, 1-15. https://doi.org/10.1080/16161262.2023.2224091.

Ciekanowski, Z., Gruchelski, M., Nowicka, J., Żurawski, S., & Pauliuchuk, Y. (2023). Cyberspace as a source of new threats to the security of the European Union. *European Research Studies Journal*, 26(3), 782-797. https://doi.org/10.35808/ersj/3249.

Congressional Research Service. (2007, December 5). *Open source intelligence (OSINT): Issues for Congress* [Report]. University of North Texas Libraries, UNT Digital Library. https://digital.library.unt.edu/ark:/67531/metadc819267/m1/20.

David, A., Jeganathan, G. S., & Azam, S. (2023). *Internet users' top concerns ensuring data privacy, security and protection.* ICMRME-2023 Proceedings, 1, 1–17. https://www.researchgate.net/publication/372498509_Internet_Users_Top_Concerns_Ensuring_Data_Privacy_Security_and_Protection.

European Commission. (2020). *White paper on artificial intelligence: A European approach to excellence and trust.* https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

European Commission. (2020, February 19). White paper on artificial intelligence: A European approach to excellence and trust. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

European Parliament and Council of the European Union. (2016a, April 27). *Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.* Official Journal of the European Union, L 119, 89-131. https://eur-lex.europa.eu/eli/dir/2016/680/oj.

European Parliament and Council of the European Union. (2016b, April 27). *Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).* Official Journal of the European Union, L 119, 1-88. https://eur-lex.europa.eu/eli/reg/2016/679/oj.

Frankivsk District Court of Lviv. (2023). *Rishennia Frankivskoho raionnoho sudu m. Lvova No. 465/1964/23* [Decision of the Frankivsk District Court of Lviv No. 465/1964/23]. https://reyestr.court.gov.ua/Review/111542290.

GDPR (2018, May). General Data Protection Regulation (GDPR). https://gdpr-info.eu/.

Goryca, T. (2023). The use of open sources of information in the activities of the formations responsible for protection of the executive bodies of the state. https://wsb.edu.pl/files/pages/634/security_forum_1_2023_doi_10_26410_sf_1_23_6.pdf.

Hadi, H., Harris, S., & Cao, Y. (2023). Cybersecurity as a service for Internet of Everything (IoE). https://doi.org/10.13140/RG.2.2.28225.94563.

Intelligence studies: Types of intelligence collection. (n.d.). https://usnwc.libguides.com/c.php?g=494120&p=3381426.

Islamic State supporters hijack dormant Twitter accounts. (n.d.). https://dig.watch/updates/islamic-state-supporters-hijack-dormant-twitter-accounts.

Jacobs, A., & Kloo, I. (2023). Detecting global events with Bayesian changepoint detection on flight data. https://www.ieworldconference.org/content/WP2023/Papers/GDRKMCC23_53.pdf.

Kamal, M. (2023). Legal implications of AI-driven OSINT: Insider threats and data leaks in Egypt and the European Union. https://doi.org/10.13140/RG.2.2.22359.65446.

Kędzierska, G. (2022). Intelligence gathering in forensic science. https://cris.mruni.eu/server/api/core/bitstreams/5f7805f9-e06b-49cc-a8ef-9c65740fe87d/content.

Khadim, S. W., Hassen, O. A., & Ibrahim, H. (2023). A review on the mechanism mitigating and eliminating internet crimes using modern technologies. *Wasit Journal of Computer and Mathematics Science*, 3, 50-68. https://doi.org/10.31185/wjcm.48.

Konieczny, M. (2025). Anti-OSINT methods ensuring protection of personal data in the context of cybercrime. *RAIP*, 1(25), 127-144. https://doi.org/10.5604/01.3001.0055.1100.

Konieczny, M.K. (2023). Cyberprzestępczość - krótka historia, współczesne oblicza i trudna do przewidzenia przyszłość. *RAIP*, 1(23), 29-50. https://doi.org/10.5604/01.3001.0016.3776.

Lakomy, M. (2023). Open-source intelligence and research on online terrorist communication: Identifying ethical and security dilemmas. *Media, War & Conflict*, 1-18. https://doi.org/10.1177/17506352231166322.

Larsen, O., Ngo, H., & Le-Khac, N. (2023). A quantitative study of the law enforcement in using open source intelligence techniques through undergraduate practical training. *Forensic Science International: Digital Investigation*, 47, 1-11. https://doi.org/10.1016/j.fsidi.2023.301622.

Lewulis, P. (2022). Collecting digital evidence from online sources: Deficiencies in current Polish criminal law. *Criminal Law Forum*, 33, 39-62. https://doi.org/10.1007/s10609-021-09430-4.

Narasimhan, P. K., Bhosale, C., Hasban, M. P., Naqvi, N. Z., Ecevit, M. I., Schwarz, K., & Creutzburg, R. (2023). Open-source intelligence (OSINT) investigation in Facebook. https://doi.org/10.2352/EI.2023.35.3.MOBMU-357.

Obaidat, M. J., Al-Syouf, I. A., Awawdeh, Y. F., Masa'deh, A. E., & Al-Haija, Q. A. (2025, July). Darknet Threats and Detection Strategies: A Concise Overview. In *2025 16th International Conference on Information and Communication Systems (ICICS)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICICS65354.2025.11073091.

OSINT Telegraph. (n.d.). *Open source intelligence (OSINT): A comprehensive guide.* https://osinttelegraph.com/open-source-intelligence-osint-a-comprehensive-guide/.

OSINT toolkit. (n.d.). https://i-intelligence.eu/resources/osint-toolkit.

Papayamma, K., Varanasi, A., & Marrapu, A. K. (2023). Internet of Things integration and the significance of block chain security. *Innovations*, 74, 789-798.

Putter, D., & Henrico, S. (2022). Social media intelligence: The national security-privacy nexus. *South African Journal of Military Studies*, 1, 19-44. https://doi.org/10.5787/50-1-1345.

Raharjo, A. (2023). Prevention of cybercrime through the development of criminal responsibility principles for internet users. *Jurnal Dinamika Hukum*, 3, 1-13. https://www.researchgate.net/publication/372168145_Prevention_of_Cybercrime_through_the_Development_of_Criminal_Responsibility_Principles_for_Internet_Users.

Riebe, T., Biselli, T., Reuter, C., & Kaufold, M.-A. (2023). Privacy concerns and acceptance factors of OSINT for cybersecurity: A representative survey. *Proceedings on Privacy Enhancing Technologies*, 1, 1-17. https://petsymposium.org/popets/2023/popets-2023-0028.pdf.

Stratton Oakmont, Inc. v. Prodigy Services Co. (1995). Retrieved 30 April, 2024, from https://en.wikipedia.org/wiki/Stratton_Oakmont,_Inc._v._Prodigy_Services_Co.

Usman, B., Mojaye, E. M., & Msughter, A. E. (2023). Online surveillance and data privacy of internet users: A discourse. *Journal of Communication and Media Research*, 15, 118-128.

Wolski, J. (2022). "Open-source intelligence" (OSINT): The development, types, capabilities, and limitations of the Method of Obtaining and Analysing Information Extracted from Open Sources (pp. 78-81). https://cba.gov.pl/download/1/7358/CBAMaterialypokonferencyjneLEAF2022Analizakryminalnawprzyszlosci.pdf.