THE ISSUE OF SOCIAL NETWORKS PAGE CYBER PROFILING

Ruslan Tazetdinov
Doctor of Philosophy, docent

Sh.A. Xoliqov
Doctor of Philosophy, docent

Azamat Ikanov
Doctor of Philosophy, senior researcher

Abstract. *This article was carried out within the framework of the targeted scientific and practical research project ALM-202310202738 "Development of innovative profiling technology for use in public safety activities," in which the process of analyzing personal characteristics based on user activity in social networks and forming their psychological and social portrait - the issue of cyberprofiling - is deeply covered. The theoretical foundations of cyberprofiling, applied methods, technological approaches, possibilities of practical application, and legal and ethical aspects are analyzed. The article extensively covers the dangers arising on social networks, the protection of personal data and their application in scientific research, and provides scientific insights into the future prospects of this area.*
Keywords: *social networks, cyberprofiling, digital traces, information security, personal data, psycholinguistics, artificial intelligence, criminology*

IJTIMOIY TARMOQLARDA KIBERPROFAYLING MASALALARI

Annotatsiya: *Mazkur maqola ALM-202310202738-sonli “Jamoat xavfsizligini ta'minlash faoliyatida foydalanish uchun innovatsion profayling texnologiyasini ishlab chiqish” ilmiy-amaliy tadqiqot loyihasi doirasida amalga oshirilgan bo'lib, unda ijtimoiy tarmoqlardagi foydalanuvchi faoliyati asosida shaxsiy xususiyatlarni tahlil qilish, uning psixologik va ijtimoiy portretini shakllantirish jarayoni – kiberprofayling masalasi chuqur yoritilgan. Kiberprofaylingning nazariy asoslari, qo'llaniladigan metodlari, texnologik yondashuvlari, amaliy qo'llanish imkoniyatlari hamda huquqiy-axloqiy jihatlari tahlil qilinadi. Ijtimoiy tarmoqlarda paydo bo'layotgan xavflar, shaxsiy ma'lumotlarning himoyasi va ularning ilmiy tadqiqotlarda qo'llanishi masalalari keng yoritilib, mazkur yo'nalishning kelajak istiqbollari haqida ilmiy mulohazalar bildirilgan.*
Kalit so'zlar: *Ijtimoiy tarmoqlar, kiberprofayling, raqamli izlar, axborot xavfsizligi, shaxsiy ma'lumotlar, psixolingvistika, sun'iy intellekt, kriminologiya.*

ВОПРОСЫ КИБЕРПРОФАЙЛИНГА В СОЦИАЛЬНЫХ СЕТЯХ

Аннотация: *Статья выполнена в рамках целевого научно-практического исследования «Разработка инновационных технологий профилирования для использования в деятельности по обеспечению общественной безопасности». В ней подробно рассматривается процесс анализа личностных характеристик на основе активности пользователей в социальных сетях и формирования их психологического и социального портрета – киберпрофайлинга. Анализируются теоретические основы киберпрофайлинга, применяемые методы, технологические подходы, возможности практического применения, а также правовые и этические аспекты. В статье подробно рассматриваются опасности, возникающие в социальных сетях, вопросы защиты персональных данных и их применение в научных исследованиях, а также дается научное обоснование перспектив развития данного направления.*

Ключевые слова: *социальные сети, киберпрофайлинг, цифровые следы, информационная безопасность, персональные данные, психолингвистика, искусственный интеллект, криминология.*

In the context of the information society of the 21st century, the Internet and social networks cover all aspects of human life. On platforms such as Facebook, Instagram, Telegram, TikTok, X (Twitter), LinkedIn, billions of users regularly share information reflecting their lives. This information is becoming not only a means of communication, but also a large source of information that allows one to analyze the human personality and evaluate it according to various criteria. Cyberprofiling is a scientific and practical direction that uses such opportunities, aimed at identifying a person's personal characteristics, views, social status, and possible behavior through their activity on social networks [1].

The concept of cyberprofiling is mainly inextricably linked with traditional profiling theory. Profiling was initially formed in the fields of criminal psychology and criminalistics as a method of creating a personal portrait of a criminal by analyzing their behavior. However, in the digital age, since people conduct most of their activities in virtual space, profiling methods have also transformed into a new form - cyberprofiling. The essence of this process is based on the collection and analysis of human digital traces. Digital tracks include user entries, comments, attitudes on various topics, photos and videos, and even when they are active. The data collected in this way allows for the reconstruction of the social and psychological image of the individual [2].

"Cyber Behavioral Analysis" (Cyber Behavioral Analysis), located in the center, is a method based on the study of the criminal's actions, habits, goals, and motives in the digital environment. Through this analysis, conclusions are drawn about the criminal's personal portrait, possible intentions, and future actions.

The system relies on two main approaches:

1. Deductive Profiling. In this approach, a personal portrait of the criminal is created based on available evidence, facts, and digital traces. It includes the following elements:

– Open Source Intelligence: Gathering information about a criminal through the Internet, social networks, and open data.

– Victimology: Obtaining information about the perpetrator based on the victim's personality, habits, and activities.

– Modus Operandi (Style of Action): The perpetrator's constantly recurring methods, techniques for carrying out cyberattacks.

– Motive: Identifying the cause of a crime, such as financial gain, political intent, personal animosity, or gaining experience.

– Digital Forensics and Digital Criminalistics: Study of computer, mobile device and network traces, scientific analysis of digital evidence [3].

These directions reveal the personality and behavior of a cybercriminal based on evidence.

2. Inductive Profiling. This approach is based on the general typology of criminals. It focuses on the study of specific cybercriminal groups, their behavior, and their typical patterns. For example:

categories such as hackers, fraudsters, cyber spies, “cryptocurrency criminals” [4].

The main advantage of inductive profiling is that it summarizes the criminal's portrait, based on previous experience and statistical observations, even if no clear personal traces of the criminal have been found (Fig. 1).

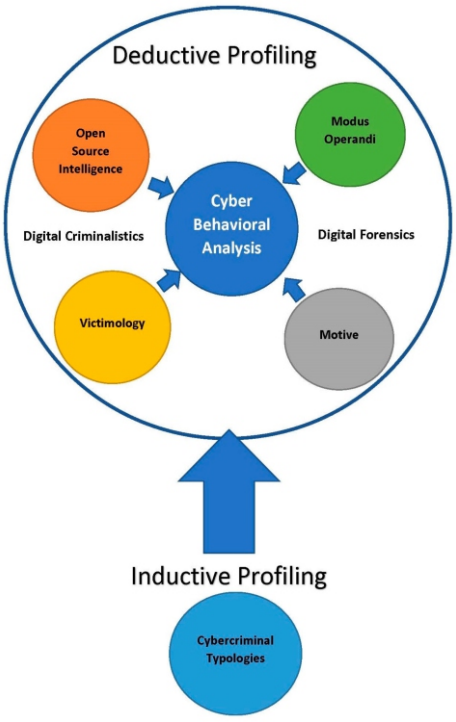

Fig-1. Areas of application of cyberprofiling

The methodology of cyberprofiling is a complex and multi-stage process. First of all, the data collection stage is carried out, in which open sources (open source intelligence – OSINT) are used. At the next stage, the data are analyzed semantically, linguistically, and psychologically.

For example, phrases in user texts, their emotional coloring, the metaphors used, or the style of language serve as an important source in determining the mental state, sphere of interest, and social views of a person. Also, by analyzing visual materials, it is possible to draw conclusions about a person's material situation, aesthetic views, and lifestyle [5].

Another important area of cyberprofiling is the analysis of social network connections. Each user has their own virtual network of contacts” which provides information about their personal values, social status, and even ideological views. Through graph analysis of social networks, it is possible to determine which groups a user belongs to, with whom they are actively connected, and their reputation on the network. (Figure 2).

Fig – 2. Graphical analysis of user social interactions

In recent years, machine learning and artificial intelligence technologies have been widely used in cyberprofiling. Algorithms such as Natural Language Processing (NLP), Sentiment Analysis, and Computer Vision allow for the automatic analysis of large volumes of text and images. These technologies help predict users' moods, political views, behavioral trends, and potentially dangerous behaviors. For example, cyberprofiling tools are being effectively used to detect individuals involved in terrorist organizations through social networks at an early stage or to monitor online fraud activities [6].

From a practical point of view, the area of application of cyberprofiling is very wide. Law enforcement agencies use it to prevent crime and identify criminals, while national security agencies use it to expose extremist and terrorist activities. In the field of cybersecurity, cyberprofiling is useful for the early detection of phishing, malware distribution, and other types of cybercrime. At the same time, commercial companies are also widely using this method.

For example, in the field of marketing, cyberprofiling serves as an important tool for studying customer interests and consumer behavior, and in HR departments – for evaluating candidates and analyzing their personal qualities.

However, the widespread use of cyber-profiling technologies also creates a number of problems. One of the biggest problems is ensuring the privacy of private life and the confidentiality of information. Everyone wants their private life to be protected, but excessive openness and the desire to show off on social networks can lead to many dangerous consequences. There is also a possibility that the misuse of cyberprofiling results can lead to human rights violations. Therefore, when carrying out this process, it is necessary to strictly comply with international norms, conventions on human rights, and the requirements of national legislation [7].

Conducted scientific analysis shows that cyberspace profiling allows one to draw large-scale and deep conclusions about a person through digital traces on social networks. This makes it possible to use it as an effective tool not only in scientific research, but also in practice. At the same time, there is a need to improve the legal, ethical, and technological aspects of this technology, which determines the future development of cyberprofiling.

The issue of social networks page cyber profiling is highly relevant for Uzbekistan, where the active digitalization of society and the rapid expansion of internet users – especially among the youth – have transformed social media into a central platform for communication, self-expression, and public discourse. In this environment, cyber profiling offers both opportunities and challenges to maintaining social and national loyalty.

From a security perspective, cyber profiling of social networks can serve as an effective tool to identify risks related to extremist propaganda, cyber fraud, or disinformation campaigns targeted at Uzbek citizens. It helps specialists trace patterns of online behavior, detect suspicious networks, and prevent the manipulation of public opinion that might threaten the stability and loyalty of society to the state. In this sense, the technology supports Uzbekistan's strategic priorities of ensuring information security and protecting youth from harmful online influences.

However, the loyalty dimension also raises important ethical considerations. Excessive or uncontrolled use of cyber profiling may be perceived as surveillance, potentially eroding trust between citizens and the government. For Uzbekistan, which is committed to reforms, openness, and strengthening democratic values, it is crucial to strike a balance: while using cyber profiling to safeguard national security and protect public order, it is also important to respect individual rights, data protection, and freedom of expression.

Therefore, in the context of Uzbekistan's loyalty, the issue of social networks page cyber profiling must be approached as part of a broader digital governance strategy. It should combine advanced technologies, clear legal regulations, and public trust-building measures. This ensures that profiling serves not as a restrictive instrument but as a protective and supportive mechanism, helping to strengthen national unity, preserve cultural values, and nurture responsible digital citizenship among the youth

Cyberprofiling of social media pages is becoming an innovative and effective tool for studying human activity in the modern information society. It yields practical results in such areas as law enforcement, cybersecurity, marketing, and personnel policy. At the same time, cyberprofiling is closely related to the protection of human rights and information privacy, and the ethical aspects of this process need to be studied more deeply in the future. Combining cyber-profiling technologies with artificial intelligence, strengthening data protection mechanisms, and developing international standards will contribute to the more effective development of this area.

References

1. Kosinski, M., Stillwell, D., Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. PNAS.
2. Turban, E., Sharda, R., Delen, D. (2017). Decision Support and Business Intelligence Systems. Pearson.
3. Tene, O., Polonetsky, J. (2012). Big Data for All: Privacy and User Control in the Age of Analytics. Northwestern Journal of Technology and Intellectual Property.
4. Zafar, H., Ko, M. (2020). Cyber Profiling: Understanding User Behavior on Social Media. Journal of Information Systems Security.
5. O‘zbekiston Respublikasi “Shaxsiy ma'lumotlar to'g'risida”gi qonuni, 2019.
6. Castelluccia, C., De Montjoye, Y.-A., & Shokri, R. (2014). Privacy in the Age of Big Data. IEEE Security & Privacy.
7. Solove, D. (2021). Understanding Privacy. Harvard University Press.