DOI https://doi.org/10.30525/978-9934-26-608-9-17

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON THE HUMAN RIGHT TO PRIVACY AND SECURITY

Kravchuk S. M.

INTRODUCTION

In today's environment of rapid digital technology development, the impact of artificial intelligence (hereinafter referred to as AI) on society and individuals in particular is a constant phenomenon that changes over time and affects the fundamental rights of citizens, especially their rights to privacy and security. The opportunities for public and private institutions to collect, analyze, and use personal data are expanding, while at the same time creating risks to the realization of the human right to privacy. The use of artificial intelligence as a tool for cyberattacks and manipulation to spread disinformation, or the deliberate creation of risks to information and physical security, are not isolated phenomena. There is a lack of adaptation of legal mechanisms for the protection of privacy and security when using AI in video surveillance systems. In the absence of proper legal regulation, the use of artificial intelligence in video surveillance and facial recognition poses a threat of excessive interference in the private lives of citizens. There is a need for scientific research into aspects of the application of machine intelligence to ensure a balance between security, fundamental human rights, and innovation.

The relentless development of artificial intelligence is causing significant changes in the field of human rights, especially in the context of the right to privacy and security. The widespread use of various artificial intelligence systems for the collection, analysis, and storage of personal data in video surveillance and facial recognition processes is causing human concerns about the loss of control over personal information. This issue has been researched and addressed in a number of works by researchers such as: Blihar M. M. (legal mechanisms for the protection of personal data)[1]; Gilyaka O. S. (the right to privacy and the protection of personal data in the context of digitalization)[2]; Gutsalyuk M. V. (cyber threats caused by hybrid warfare and

[1] Бліхар М. М. Організаційно-правовий механізм захисту персональних даних. *Науковий вісник Ужгородського університету*: серія: Право. Ужгород, 2023. Т. 2. Вип. 77. С. 31-36. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/283773/277973 (дата звернення: 25.06.2025).

[2] Гиляка О. С. Право на приватність та захист персональних даних в умовах цифровізації. Вісник Національної Академії правових наук України. Харків: *Право*, 2023. Т. 30, № 1. URL: https://visnyk.kh.ua/web/uploads/journals_pdf/%D0%92%D1%96%D1%81%D0%BD%D0%B8%D0%BA%20%D0%9D%D0%90%D0%9F%D1%80%D0%9D%D0%A3_%D0%A2%D0%BE%D0%BC%2030(1)_2023.pdf#page=15 (дата звернення: 25.06.2025).

countering them)[3]; Diorditsa I. V. (cybersecurity policy of Ukraine)[4]; Kravchuk V. O. (foreign experience in personal data protection on social networks)[5]; Marushchak A. I. (human information rights, information security)[6]; Mrak V. B. (face recognition methods in video surveillance systems and means of recognizing moving objects)[7]; Semenyuk O. O. and Samoray O. K. (features of the GDPR legal regime in Ukraine)[8].

The purpose of the study is to analyze the impact of AI on privacy in the context of mass collection of personal data; violations of security rights through cyberattacks using AI through manipulation; creation of a legal basis for the safe operation of video surveillance and facial recognition systems; description of the main features of personal data protection in the digital environment; identifying gaps in current legal regulation and presenting proposals for improving legislation at both the national and international levels in the aforementioned problem areas.

1. The impact of AI on the right to privacy through mass data collection

Digital transformation has ushered in a new stage in the evolution of civilization, encompassing socio-economic, humanitarian, and informational modernization. As part of this transformation, large-scale data digitization is taking place, and significant amounts of personal information are stored in a format that allows for their free transfer, dissemination, and exchange at various levels, including transnational. Such changes give rise to risks related to the protection of personal data.

Artificial intelligence is a set of theoretical concepts and practical approaches in the field of information technology aimed at creating systems

[3] Гуцалюк М. В. Кіберзагрози під час гібридної війни та протидія організованій кіберзлочинності. Інформація і право, 2025. № 1 (25). С. 123-131. URL: http://il.ippi.org.ua/article/view/324708 (дата звернення: 25.06.2025). DOI: https://doi.org/10.37750/2616-6798.2025.1(52).324708

[4] Діордіца І. В. Кібербезпекова політика України: стан та пріоритетні напрями забезпечення : монографія. Херсон : Видавничим дім «Гельветика», 2017. 548 с. URL: http://library.kpi.kharkov.ua/files/new_postupleniya/kipouk.pdf (дата звернення: 25.06.2025).

[5] Кравчук В. О. Зарубіжний досвід захисту персональних даних у соціальних мережах. Науковий вісник Ужгородського університету: серія: Право. Ужгород, 2023. Т. 2. Вип. 78. С. 49-53. URL: https://dspace.uzhnu.edu.ua/jspui/handle/lib/56098 (дата звернення: 25.06.2025).

[6] Марущак А. І. Визначення поняття «інформаційні права людини». *Інформація і право.* Вип. 2. С. 21-26.

[7] Мрак В. Б. Методи розпізнавання обличчя у систем відеоспостереження з використанням машинного навчання. Інфокомунікаційні технології та електронна інженерія. 2023. Т. 3, № 2. С. 33-42. DOI: 10.23939/ictee2023.02.033

[8] Семенюк О. О., Саморай О. К. Особливості правового режиму GDPR в Україні. Проблеми та перспективи реалізації та впровадження міждисциплінарних наукових досягнень: збірник наукових праць з матеріалами VIII Міжнародної наукової конференції, м. Конотоп, 20 грудня 2024 р. Міжнародний центр наукових досліджень. 2024. С. 217 – 220.

capable of independent intellectual functioning, similar to the decision-making processes in the human brain. Thanks to its capabilities, technical systems are able to learn, process large amounts of information, and recognize patterns in it.

Personal data protection is an extremely relevant topic and is only becoming more important over time. It involves ensuring confidentiality, secure distribution, information exchange, and protection from unauthorized access or use. In this context, digital transformation poses a number of challenges related to ensuring data reliability, proper storage, and use.

Currently, large amounts of personal information, including confidential information, are collected from various sources and undergo certain stages of processing, which poses a threat to the security of the right to privacy[2].

Machine learning is a set of technologies that enables computer systems to think and make decisions based on mathematical algorithms formed from available data, specific instructions, and rules. This approach allows systems to gradually learn and improve through information analysis without instructions from programmers and constant reprogramming.

The legal mechanism for the protection of personal data in Ukraine is based on the Constitution of Ukraine, international obligations, in particular the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108)[9], and the Law of Ukraine "On the Protection of Personal Data" (hereinafter referred to as the Law)[10]. The Constitution enshrines the fundamental rights and freedoms of citizens, including the right to non-interference in personal and family life (Article 32), which is the basis for the protection of personal data. The Law is the main regulatory act governing relations related to the protection of personal data and determining the procedure for its processing. It was adopted in 2010 and has undergone changes, but in general it can be assessed as requiring further improvement, especially in the context of the implementation of GDPR standards. Work is currently underway on a new draft law "On the Protection of Personal Data" (for example, draft law No. 8153)[11], which should bring Ukrainian legislation closer to European

[9] Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних. Страсбург, 28 січня 1981 року. URL: https://zakon.rada.gov.ua/laws/show/9 (дата звернення: 25.06.2025).

[10] Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI: станом на 27 жовтня 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 25.06.2025).

[11] Гаврилюк А. GDPR по-українськи: ключові аспекти ЗП №8153 «Про захист персональних даних». *Юридична газета online*. № 4 (792). 2024. URL: https://yur-gazeta.com/publications/practice/zahist-intelektualnoyi-vlasnosti-avtorske-pravo/gdpr-poukrayinski-klyuchovi-aspekti-zp-8153-pro-zahist-personalnih-danih.html (дата звернення: 25.06.2025).

standards. Certain aspects of personal data protection are regulated by other acts (for example, the Criminal Code of Ukraine provides for liability for violation of the secrecy of correspondence or illegal collection, storage, use, or dissemination of confidential information).

A data subject is a natural person whose personal data is being processed. They have a wide range of rights: to know the sources of collection, location, and purpose of processing of their data; to receive information about the conditions for providing access to personal data, in particular information about third parties to whom the data is transferred; to access their personal data; to submit a reasoned request to change or destroy their personal data if it is processed unlawfully or is inaccurate; to object to the processing of their data in certain cases; to withdraw consent to the processing of personal data; to transfer data (the right to receive their data in a structured, commonly used, and machine-readable format and to transfer it to another controller); to protect their rights against unlawful processing of personal data.

Personal data controller – determines the purpose and scope of personal data processing. Responsible for ensuring data protection. Personal data processor – a person who receives data from the controller for processing. Third party – any person other than the data subject, controller, or processor. Data controllers and processors are required to take organizational and technical measures to protect personal data from unauthorized access, destruction, distortion, etc. This includes developing internal regulations, appointing responsible persons, and ensuring an adequate level of database protection.

The Constitution of Ukraine (Articles 21, 31-32) enshrines the fundamental principles of equality before the law and personal freedom, inalienability, and the inviolability of fundamental rights. Interference in personal and family life is prohibited, except in cases provided for by the Constitution of Ukraine. The collection, receipt, use, and dissemination of confidential information about a person without their consent is prohibited, except in cases specified by law and only in the interests of national security, economic well-being, or the protection of human rights[12]. Everyone has the guaranteed right to protection from interference in their private life, as well as to the inviolability of correspondence, telephone conversations, correspondence, including e-mails, and other information relating to personal data.

Ukraine uses Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such

[12] Конституція України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2% D1%80#Text (дата звернення: 25.06.2025).

data, and repealing Directive 95/46/EC (General Data Protection Regulation)[13]. This international legal act in the field of personal information protection on the Internet was officially recognized by Ukraine through ratification by the Verkhovna Rada. The relevance of this document today is confirmed by the fact that Internet users constantly fill out various application forms for registration on websites, recklessly leaving their personal data. That is why the issue of preventing unauthorized access to such data and possible negative consequences for personal data subjects is one of the state's priorities in the field of protecting human rights and freedoms. More and more developers agree that rapid technological progress and globalization create new challenges for the effective protection of personal information. The scale of personal data collection and sharing has also increased. Modern technological means allow both commercial structures and state institutions to use personal data on an unprecedented scale to ensure their activities. In addition, individuals are increasingly providing access to their own data for public viewing on a global level. The economy and social life have changed due to technology and should continue to encourage the free flow of personal data within the EU and its transfer to third countries and international organizations, provided that a high level of protection is ensured[14].

It is necessary to recognize the urgent need to rethink the concept of human rights in the context of digitalization and the rapid development of modern technologies, because in today's reality, any attempts to discuss new technologies in a positive light, considering them completely safe and having no impact on human rights, are completely inappropriate. Identifying such technologies with full compliance with human rights standards and perceiving them exclusively as means of total control that threaten democratic principles is simplistic and manipulative[2].

In everyday life, Internet users continue to unknowingly leave a significant amount of personal data, without even suspecting that it could be used by third parties. Disputes over the protection of personal data and access to information are usually settled through legal appeals. An alternative mechanism is to appeal to the Ukrainian Parliament Commissioner for Human Rights, whose representatives conduct inspections and draw up reports on violations of the right to personal data protection and the right to

[13] Регламент Європейського Парламенту і Ради (ЄС) 216/679 від 27.04.2016 р. про захист фізичних осіб при обробці персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). URL: https://ips.ligazakon.net/document/MU16144 (дата звернення: 25.06.2025).

[14] Бліхар М. М. Організаційно-правовий механізм захисту персональних даних. Науковий вісник Ужгородського університету: серія: Право. Ужгород, 2023. Т. 2. Вип. 77. С. 31-36. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/283773/277973 (дата звернення: 25.06.2025).

access information, on the basis of which the court may impose administrative penalties.

Personal data includes a wide range of information, including basic information (name, surname, date of birth, etc.) and more confidential data such as certain medical records, biometric parameters, and financial information. An important feature to remember is even indirect data, such as IP address or geolocation, which can later be used to identify a person.

Sources of personal data are usually classified into three main categories. The first is data provided by the user themselves, in particular when registering for online services or filling out questionnaires. The second covers information collected as a result of surveillance through video surveillance or activity trackers. The third group is data generated by systems through the analysis of user behavior, preferences, and interactions in the digital space in general[15].

The processing of personal data is lawful if at least one of the following conditions is met:

– the data subject has consented to the processing of personal data for one or more specific purposes;

– processing of personal data is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

– processing of personal data is necessary for compliance with a legal obligation to which the controller is subject;

– processing of personal data is necessary to protect the vital interests of the data subject, his or her personal data, or another natural person;

– processing of personal data is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controllers;

– processing of personal data is important for the purposes of protecting the legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child[2].

In Ukraine, the Law "On the Protection of Personal Data," which regulates the rights of data subjects, defines the obligations of controllers and data processors, and establishes requirements for the protection of information in the digital environment. According to Article 11 of the law, the grounds for the processing of personal data are defined[10]. It should be

[15] Прокопенко О. Є. Розробка навчальної системи для збору персональних даних з використанням штучного інтелекту та соціальної інженерії. Кваліфікаційна робота. Тернопіль, 2024 URL: https://elartu.tntu.edu.ua/bitstream/lib/48324/1/Masters_Thesis_SBm-62_Prokopenko_O_E_2024.pdf (дата звернення: 25.06.2025).

noted that the list does not include grounds for processing personal data for national security or public order purposes. In addition, there is no mention of the presumption of consent to processing in public places, even though these grounds are often used to justify the processing of biometric data.

An example of a possible risk to privacy and personal data protection from AI is the situation that arose in May 2022, when the UK Information Commissioner's Office fined Clearview AI Inc. for violating the General Data Protection Regulation (GDPR)[16] regarding the collection and use of facial data. Clearview AI is an American company that calls itself "the world's largest facial recognition network." It allows users, including the police, to upload images of people to their app. These images are then checked against the Clearview AI database. The app then provides a list of similar or matching images with a link to the website from which they were taken. The company was found to have violated the General Data Protection Regulation on the following grounds:

– failure to use users' personal data in a fair and honest manner, given that individuals were not informed or did not reasonably expect their data to be used in this way;

– lack of a legal basis for collecting users' personal data;

– failure to stop the endless collection of data;

– failure to comply with the highest standards of protection of information required for special category data (biometric data);

– requesting additional personal information, including photographs, at the request of members of the public, whether they are in their database. This could act as a deterrent to individuals wishing to object to the collection and use of data[17].

Another apt example that clearly demonstrates how AI can be used to modify private data is the actions of ShareWithCare. A study was conducted using a fake training video titled "A Message from Ella/Without Permission." The aim of this project was to clearly show the possible consequences of carelessly publishing data about children on the Internet. Anyone who thoughtlessly posts photos or videos of children online increases the risk of inadvertently making them victims of personal data exchanges, hackers, facial recognition, pedophiles, and other potential threats to children's safety and privacy. The study yielded the following results:

– sharing photos and videos of children online is widespread: 86% of parents thoughtlessly share material featuring their own children;

[16] Загальний регламент про захист даних (GDPR). URL: https://gdpr-text.com/uk/ (дата звернення: 25.06.2025).

[17] ICO Fines «World's Largest Facial Network.» (2022, May 25). Your Front Page for Information Governance News. URL: https://actnowtraining.blog/2022/05/25/ico-fines-worlds-largest-facial-network/ (дата звернення: 25.06.2025).

– the younger the child, the more often their relatives post photos and videos of them: 70% of parents post photos of their children under the age of 5 at least once a week using messengers; 59% post photos of children aged 6 to 9; 46% post photos of children aged 10 to 14;

– only a third of parents realize that one photo is enough for their child to become a victim of identity theft;

– 85% of respondents trust that recipients of shared photos will not distribute them to third parties;

– 65% of people are unaware of the consequences of innocent posts.

For the “Links from Ella” project, a character named Ella, aged 9, was created using the latest AI technologies. The Deepfake (artificially created) video shows adult Ella talking to her surprised parents and confronting them with the results of sharing her childhood photos online[18]. This material serves as a warning and reminder about the dangers of carelessly sharing personal data online and how, with the development of digital technologies, particularly artificial intelligence, there is a growing need for privacy protection and appropriate legal regulation.

Proper protection of personal data is key in today's world and is guaranteed by both national laws and international regulations. Society needs to ensure a timely, multi-level security system for everyone in this area. The European Union's General Data Protection Regulation (GDPR) plays an important role in protecting consumer rights and privacy in the digital world. The fundamental principles of the GDPR are the principle of lawfulness (processing is carried out only with the consent of the data subject or on grounds provided for by law), fairness (data must be processed honestly), purpose limitation and adequacy (data is collected for specific, defined and legitimate purposes, and is adequate, relevant, and not excessive in relation to those purposes), accuracy, confidentiality (data must be protected against unlawful access and disclosure), and storage limitation (no longer than necessary for the purposes for which it was collected).

2. Analysis of legal mechanisms for personal data protection in the digital age

Legal mechanisms for protecting personal data in the digital age cover a wide range of issues, including the existence of and compliance with regulatory requirements, ensuring organizational and technical data security, and protecting the rights of various data subjects and human rights in particular.

[18] Kirchhof N. ShareWithCare: Photos of children require special protection online. 2023 URL: https://www.telekom.com/en/media/media-information/archive/sharewithcare-children-s-images-deserve-protection-on-the-net-1048376 (дата звернення: 25.06.2025).

Legal regulation is an integral part of ensuring the protection of personal data on the Internet. Such mechanisms may include regulatory acts, certain standards, principles, and recommendations that define the requirements for the collection, processing, storage, and use of personal information. In addition, legal systems also guarantee accountability for violations of established rules in the field of personal data protection and outline mechanisms for protecting the rights and interests of individuals[19].

Legal mechanisms cannot do without international cooperation, which plays an important role in ensuring effective interaction between different states in the field of personal data protection. Within the European Union, for example, there is the European Data Protection Board, which coordinates the activities of national supervisory authorities and promotes the harmonization of personal data protection issues. That is why legal mechanisms are considered a necessary link in the protection of personal data in the digital environment, as they ensure the regulation of a number of rules and requirements for the collection, processing, and storage of personal information, and also determine liability for violations and guarantee the observance of the rights and interests of data subjects.

One of the most important legal instruments for protecting personal data on the Internet is regulatory and legal acts. They govern the collection, storage, and use of personal information, define the rights and obligations of data collectors and users, and establish legal liability for violations of relevant regulations. Such legislative acts exist at both the international and national levels. Another important legal mechanism for protecting personal data is court decisions. In cases of violation of the right to personal data protection, courts can decide on compensation for damages and impose fines on offenders. Such decisions set legal precedents and help strengthen personal data protection systems in the digital environment.

In addition to legislative acts and court decisions, self-regulatory mechanisms also play an important role in ensuring the protection of personal data. They are based on the voluntary adoption of certain rules and standards of conduct aimed at data collectors and users. Mechanisms of this nature can contribute to improving the level of personal data protection.

The next tool for protecting personal data is self-regulation mechanisms, which are responsible for the voluntary establishment of rules and standards by the organizations themselves that process personal information, voluntarily establishing rules and standards that will regulate the collection, storage, and processing of data. Many social networks, for example, have

[19] Пащенко, О. А., Хоменко, В. Л. Роль правових механізмів при захисті особистих даних в інтернеті. *ББК*, *67*(304.3). Львів, 2023. С. 165-169. URL: https://law.lnu.edu.ua/wp-content/uploads/2015/09/Zbirnyk_7_Lviv_IPconference.pdf#page=165 (дата звернення: 25.06.2025).

their own privacy policies that implement various digital platforms, informing users in detail about the types of material collected and how it is processed. The advantage of self-regulation is its flexibility and ability to respond quickly to changes in the technological environment. At the same time, unlike state regulation, these mechanisms do not provide for legal liability and mechanisms for its enforcement against violators.

To analyze the effectiveness of various legal instruments, it is advisable to consider, using relevant cases as examples, situations of personal data protection violations on the Internet and understand what legal response mechanisms were involved in each of them. For example, one can consider court decisions concerning violations in the field of personal information protection on social platforms, conclusions on the cancellation of various policies for the collection and use of personal data, as well as cases where self-regulatory mechanisms have proven effective in preventing such violations. The analysis will help to understand the importance of each legal mechanism and its capabilities in different contexts. In conclusion, it should be noted that personal data is a particularly valuable information resource that requires adequate protection on the Internet. In order to implement such protection, various legal mechanisms are used, including regulatory acts, court decisions, and self-regulatory instruments.

Research into the effectiveness of legal mechanisms based on relevant cases shows that each of them can be quite effective when applied correctly and in a proper manner. For example, the Cambridge Analytica incident demonstrated the need for immediate improvement of legislation to ensure adequate protection of users' personal data. At the same time, according to the court's conclusion in the Google v. CNIL case, there appears to be a high level of effectiveness in the protection of personal information by judicial authorities, which have obliged the relevant organizations to comply with established protection standards[20].

In the future, in order to ensure effective protection of personal data on the Internet, it is necessary to continue scientific research and develop new legal mechanisms that will respond to the new challenges of the digital age. It is advisable to carefully consider the potential of implementing blockchain technologies for the storage and transfer of personal data in order to ensure their security and confidentiality.

[20] Пащенко, О. А., Хоменко, В. Л. Роль правових механізмів при захисті особистих даних в інтернеті. *ББК*, *67*(304.3). Львів, 2023. С. 165-169. URL: https://law.lnu.edu.ua/wp-content/uploads/2015/09/Zbirnyk_7_Lviv_IPconference.pdf#page=165 (дата звернення: 25.06.2025).

3. The role of AI in video surveillance and face recognition systems

One of the controversial technologies known for its advanced features and capabilities can rightly be considered face recognition technology. With the help of artificial intelligence, the features of the appearance of a certain person are analyzed according to the available images, which leads to the identification of a person[21].

When discussing the protection of digital rights, special attention should be paid to the use of face recognition technologies and the processing of visual data of citizens obtained as a result of the operation of video surveillance systems. Since such data belongs to the category of personal and sensitive data, their processing must be accompanied by a high level of security and be legally enshrined. The use of AI in this area is increasingly influencing the interference with privacy. A digital footprint can be stored online due to the inability to delete certain information. In this regard, the right to be forgotten is formal. It is extremely difficult to guarantee this right to a person [22].

The peculiarity of Face Recognition Technology is defined by two processes: "entry into a certain database of persons and finding matches"[22]. The main task of identification is to obtain an image with excellent quality. Such identification is carried out at a distance, without involving a person in the process.

The primary goal of Face Recognition Technology was to help the military identify enemies at a distance[23]. Over time, the scope of this technology has expanded. Now, the main tasks are to ensure public order, establish national security, and prevent crime. The European Union and the United States use Face Recognition Technologies for varying degrees of network monitoring, mass data analysis, collection and cataloging for intelligence and security purposes[24]. Awareness of the use of video

[21] Максимович Т. М. Технології розпізнавання облич і право на приватність та захист персональних даних. Магістерська робота. Київ, 2021. С. 8., с. 15. URL: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/b15e28f6-c716-451e-9da1-4f98635d500d/content (дата звернення: 25.06.2025).

[22] Гиляка О. С. Новітні технології та права людини: аналіз деяких критичних проблем цифрової ери. Вісник Національної академії правових наук України, 2023. № 30 (2). С. 15-30. URL: https://visnyk.kh.ua/web/uploads/pdf/%D0%92%D1%96%D1%81%D0%BD%D0%B8%D0%BA%20%D0%9D%D0%90%D0%9F%D1%80%D0%9D%D0%A3_%D1%82%D0%BE%D0%BC%2030_2_2023_%D0%A3%D0%9A%D0%A0-15-30.pdf (дата звернення: 25.06.2025).

[23] Nakar S., Greenbaum D. Now you see me. Now you still do: facial recognition technology and the growing lack of privacy. Journal of Science & Technology Law – Boston University. 2017. P. 95. URL: https://www.bu.edu/jostl/files/2017/04/Gree3nbaum-Online.pdf (дата звернення: 25.06.2025).

[24] Wright Elias. The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector. Fordham Intell. Prop. Media & Ent. L.J. 2019. P. 617. URL: https://ir.lawnet.fordham.edu/iplj/vol29/iss2/6/ (дата звернення: 25.06.2025).

surveillance systems and cameras with a face identification module does not relieve the relevant persons from liability for human rights violations. When using facial recognition technology, there are risks of obtaining results that will be subsequently used beyond the originally defined purposes. It is worth remembering that the recording of faces by a surveillance camera does not always mean that the person understands the purpose of this surveillance. Thus, an ordinary person who is potentially under surveillance may not understand what data is recorded, for what purpose the camera is installed, who initiated it or who owns the surveillance system. In the case of the presence of certain representatives of public authorities in public places, citizens may be identified as subjects responsible for maintaining order and security. In this case, individuals may be clearly aware that under certain circumstances their personal data will be collected and processed by the relevant authority. Cameras in public places do not guarantee the identity of the observer or the identification of the real purpose of the surveillance. In this regard, the work of data controllers is based on the formulation of a clear purpose of using Face Recognition Technology and collecting personal data to prevent unreasonable accumulation of databases[25]. In the process of collecting personal data through the use of face recognition technologies, the sufficiency requirement is closely related to the quality of the images obtained. After all, one high-quality image can replace the presence of several low-quality images, ensuring accuracy and a positive identification result. Thus, the application of the latest technological capabilities is due to the effective use of Face Recognition Technology and allows us to obtain high quality images.

Automated video surveillance systems are networks of video sensors designed to monitor people and their behavioral characteristics in order to detect potentially dangerous actions. This approach is used in systems based on the analysis of biometric data, human behavioral characteristics, and the identification of anomalies and abnormal behavior to determine the state of danger. An example of such indicators is the detection of certain objects that indicate danger, such as cold or hot weapons.

Video surveillance analytics solutions based on artificial intelligence offer great opportunities for processing large amounts of data. They can be integrated into a video surveillance management platform and then deployed on a virtually unlimited number of cameras to provide round-the-clock coverage. Over time, technology improves and algorithms become more accurate in recognizing standard behavior patterns and detecting new dangers. This confirms the effectiveness of security systems and justifies the analytics performed by artificial intelligence. For example, AI helps to

[25] Ünver H. Akın. Artificial Intelligence, Authoritarianism and the Future of Political Systems. Centre for Economics and Foreign Policy Studies, 2018. P. 4. URL: http://www.jstor.org/stable/resrep26084 (дата звернення: 25.06.2025).

facilitate the detection of dangerous activities (fights, falls, or other criminal acts); facilitates timely scanning of crowd behavior for early detection of potential threats; it accurately identifies important objects that may pose a threat to a person or society as a whole; detects non-standard and prohibited behavior, such as attempts to enter a controlled, protected area; is able to instantly perform a thorough analysis of long-term trends in order to predict incidents before they occur; artificial intelligence can correlate data from other systems of the facility; is able to recognize license plates; conducts audio analysis and analysis of data from other systems, such as AI sensors, to form a comprehensive and detailed security solution. Based on the above, it can be concluded that face recognition technology is not always able to accurately match images from surveillance cameras with existing images in the database. The main reasons for errors in identification and efficiency are poor image quality and lack of information in the database. Usually, this is where the information or a combination of information is stored, but the practical result is not always achieved. Face recognition technologies do not determine the percentage of accuracy. However, the constant improvement of technologies helps to increase the accuracy of artificial intelligence analytical processes.

Different types of technologies are used to create a machine vision application to achieve the goal of real-time face recognition using neural network systems. Each of them depends on the right choice of tools and methods, and requires high performance, accuracy, and efficiency to successfully complete tasks. This includes Computer Vision, which is the basis for all face recognition systems. It is known for automatic detection in images or video streams. Special libraries are used to implement this technology. For example, OpenCV (guarantees fast image analysis), or Dlib, which recommends ready-made detection solutions. The next technology is Deep Learning, which provides analysis of complex structures. A key feature is convolutional neural networks (CNNs), which extract unique features to create embeddings, or mathematical vectors. Examples include FaceNet, ArcFace, and DeepFace models, which are well-known and impressive for their high accuracy even in difficult conditions. YOLO (You Only Look Once) is considered the most famous representative of "real-time algorithms", which aims to accurately detect faces in video streams with incredible speed and accuracy. MTCNN (Multi-task Cascaded Convolutional Networks) efficiently finds key points for better analysis. "Video Stream Processing works in a real-time system. It also works effectively with large amounts of video information. Tools such as FFmpeg are used to ensure efficient decoding and processing of video streams of various formats, which makes it easy to adapt the system to work with video at different frame rates or resolutions. For instant face recognition needs, you can use ready-made

"APIs" such as Microsoft Azure Face API, Google Cloud Vision API, or Amazon Rekognition. These systems guarantee accurate face recognition without the need to train models independently, but their use is usually limited by cost or dependence on third-party services. IoT (Internet of Things) tools used by organizations to integrate with other systems allow them to combine video surveillance, access control, and behavioral analysis into one single infrastructure. The operation of such an infrastructure is easily ensured by centralized management[26].

4. Legal regulation of the use of AI in video surveillance and face recognition systems

The issue of legal and regulatory protection in the use of computer vision technologies is of particular relevance in the context of their rapid implementation in many areas, ranging from security and medicine to transportation and marketing. The use of this type of technology involves the collection, processing and storage of significant amounts of information, including personal data, which may subsequently lead to threats to human rights.

One of the main problems in terms of violation of the legal framework is non-compliance with the laws on privacy and personal data protection. As noted earlier, computer vision is responsible for face recognition and involves the processing of biometric data. In the event of unauthorized data collection or processing, organizations may face significant legal consequences, including the payment of significant fines and a lowered reputation. For example, if a facial recognition system is placed in a public place without informing citizens or without their consent, this may be considered a violation of the right to privacy.

Equally important is the issue of copyright infringement of machine learning algorithms and models. Computer vision technologies are often developed using open data sets or existing models that may be subject to intellectual property rights.

It is worth remembering that computer vision systems do not always work flawlessly and also make mistakes, falsely recognizing individuals or objects.

Most often, the use of Facial Recognition Technology violates the human right to respect for private and family life[23]. If this technology is used without the consent of a specific personal data owner, a conflict arises between the private interests of the person in respect of whom the technology is used and the interests of the business entities that initiate this respective use of the

[26] Степаненко О. І. Нейромережна система розпізнавання людей в реальному часі у системах безпеки : кваліфікаційна робота магістра спеціальності 121 «Інженерія програмного забезпечення». Науковий керівник А. І. Безверхий. Запоріжжя: ЗНУ, 2024. 87 с. URL: https://dspace.znu.edu.ua/jspui/handle/12345/24554 (дата звернення: 25.06.2025).

technology. Ensuring a balance between these interests is important. After all, human rights constitute a fundamental value in the legal understanding of democratic states and require proper protection. However, on the other hand, there are also business interests that may partially intertwine with public interests (entrepreneurs exercise their right to freedom of business activity, providing the state with benefits in the form of jobs, taxes and other mandatory contributions). It would be reasonable to protect both rights, but given the specifics of face recognition technology, this is practically impossible. In such a situation, the object to which this technology is applied will usually be at a disadvantage in relation to the entity that will use this technology.

When using this technology, entities must ensure transparent data collection, as well as have an appropriate and justified legal basis for collecting and processing them. According to Article 6 of the General Data Protection Regulation (GDPR)[16], there are six legitimate conditions for the processing of personal data to be considered lawful if at least one of them is met: 1) consent (the data subject has given explicit consent to the processing of his or her personal data for a specific purpose); 2) the existence of a contract; 3) the presence of a legal obligation (processing is carried out to comply with a legal obligation imposed on the controller, who must determine the purposes and means of processing personal data); 4) the need to protect the vital interests of any individual; 5) the existence of a public interest or the exercise of official powers vested in the controller; 6) the existence of legitimate interests (provided that they do not prevail over the fundamental rights and freedoms of the data subject)[27].

The use of artificial intelligence technologies in public administration covers a wide range of areas, contributing to the implementation of the principle of transparency, minimization of corruption risks, speed, and transparency of organizing high-quality interaction between government agencies and citizens.

In addition to the introduction of a wide range of public services, artificial intelligence is being actively integrated in complex and narrowly focused professional areas. In law enforcement in Ukraine, AI is used to automate information analysis, detect offenses, and even predict criminal activity based on large amounts of data. Facial recognition technologies, as well as text and image processing systems, have significant potential here, as they can significantly improve the process of identifying offenders.

[27] Гуменюк В. І. Правове регулювання технологій розпізнавання обличчя в ЄС, США та Україні: приватно– та публічно-правовий аспекти: кваліфікаційна робота магістра спеціальності 081 «Право». Київ: НаУКМА, 2024. 95 с. Р. 19-23. URL: https://ekmair.ukma.edu.ua/handle/123456789/30834 (дата звернення: 25.06.2025).

The integration of artificial intelligence into law enforcement in Ukraine offers numerous opportunities, such as increasing the efficiency of processing a large amount of information, which greatly facilitates the investigation of criminal offenses and the detection of abuses.

However, along with the benefits of adopting the latest AI technologies, there are also significant risks. Insufficient confidentiality of personal data can lead to human rights violations, and therefore the issue of introducing artificial intelligence technology requires proper legal regulation, as well as the creation of effective mechanisms to protect personal data from unauthorized processing, including loss, illegal or accidental destruction, and from unauthorized access to them by unauthorized persons[28].

We will try to go beyond the usual approaches and propose some innovative and possibly provocative ideas, taking into account current trends and future challenges.

We offer the following novel proposals for improving the legal regulation of the use of AI in video surveillance systems.

1. Introduction of the "Right to anonymous existence in public space". The substantive essence lies in the need to legislate the right of a person to be unrecognized by artificial intelligence systems in public places where there is no justified public need for such identification. This means that, by default, video surveillance systems with face recognition should operate in an anonymization mode, recognizing only movement and objects, not specific individuals. The mechanism for implementing this right is to allow the use of facial recognition only if there is a court decision regarding a specific person or group of persons (something similar to wiretapping) and for a specifically defined crime or threat of committing a crime with a limited validity period based on a court decision until the person's criminal record is expunged. For other purposes (e.g., analyzing the flow of people to optimize urban transport), use technologies that guarantee complete anonymization of data at the stage of its collection.

The novelty lies in shifting the focus from "justified need to use" to "justified need to derogate from anonymity," making anonymity the default state in public space.

2. Application of the concept of "Dynamic Privacy Zones". The idea is to introduce zones defined by law, where the level of permissible use of artificial intelligence for video surveillance and face recognition varies depending on the time of day, event and social context.

[28] Троцький, О. О. Правове регулювання та потенційні ризики застосування штучного інтелекту в правоохоронній діяльності. Штучний інтелект у правовій практиці: межі та можливості. *Збірник тез Всеукраїнського круглого столу.* Львів, 2024. С. 181-187. URL: https://files.znu.edu.ua/files/Bibliobooks/Inshi79/0059014.pdf#page=180 (дата звернення: 25.06.2025).

"High privacy zones": appropriate residential areas, schools, medical facilities – where facial recognition is allowed only in emergency cases (with consent and in the presence of an emergency).

"Medium privacy zones": parks, squares, transportation hubs – where aggregate flow analysis is allowed (without identification), but facial recognition is possible only with clear warning and consent or on the basis of a court order.

"Low privacy zones": borders, airports, areas of high terrorist threat – where more invasive technologies can be used, but with clear justification and transparency for citizens.

The novelty lies in the fact that instead of universal rules, we propose a flexible system that takes into account the context of use and social expectations of

privacy. The implementation mechanism may include automatic warnings (e.g., via mobile apps) (for example, via mobile applications) about entering an area with a certain level of AI surveillance.

3. “Privacy Algorithm Audit” with independent “White hackers. The substantive essence is to introduce a mandatory, regular and public audit of artificial intelligence algorithms used in video surveillance and algorithms used in video surveillance and face recognition systems, carried out by independent experts (even “white hackers”).

The mechanism is mandatory disclosure (under NDA) of the architecture of algorithms for audit for potential vulnerabilities, errors, bias, and the possibility of identifying individuals without their consent or authorization.

Auditors should check not only the declared functions, but also hidden capabilities, including backdoors or unintentional identification.

The results of the audit (generalized, without disclosing sensitive information) should be publicly available.

The novelty lies in shifting the focus from regulatory “what can and what can and cannot be done” to “how it works“, adding a layer of transparency and control at the technical level that is difficult to circumvent. The use of “white hackers” adds a pragmatic focused on identifying real threats.

4. “The Right to Imitate. The substantive essence is the legislative consolidation of the human right to use technology to change one's appearance (e.g., camouflage masks, special makeup, face-distorting projectors) in order to avoid face recognition in public space, unless it poses a direct threat to security.

The mechanism of implementation is to establish clear boundaries when such actions are legal (for example, not to conceal a person during a crime or in high-risk areas where identification is mandatory by law). This may be a kind of “challenge” for AI developers, but it is also a form of active protection of the right to privacy that belongs to humans.

The novelty lies in shifting the responsibility for privacy protection partially to citizens themselves, providing them with tools for active "demarche" against comprehensive surveillance, and encourages technology companies to develop more advanced but ethical systems.

5. "White hackers.The substantive essence is to introduce a mandatory,

The implementation mechanism will allow developers to test technologies without the risk of violating current legislation, while regulators and those who will be reversing legal regulation will be able to better understand the potential risks and opportunities of new intelligent systems, formulating more adequate and flexible legal norms on this basis. Implementation of this mechanism will allow for a faster response to technological changes.

The novelty lies in the fact that instead of retrospective regulation, which always lags behind technology, a proactive approach is proposed, where regulators are actively involved in the process of development and evaluation, shaping the legal framework proactively.

These proposals are aimed at creating a more balanced, flexible, and future-oriented legal framework that can more effectively address the challenges posed by artificial intelligence to human privacy in the modern world. They require considerable political will and expert discussion for their implementation, especially legal discussion.

CONCLUSIONS

Thus, AI as a phenomenon has become a key element in the development of the modern digital environment. Its unlimited potential covers various areas of activity as an intelligent personal assistant and an advisor on optimization and automation of business processes. However, the introduction of artificial intelligence raises new challenges and threats, in particular, in the field of personal data protection.

With the continuous development of digital technologies, the possibilities through which human rights are realized have changed significantly. On the one hand, this has contributed to the empowerment of individuals, ensuring the low level of fundamental rights and supporting the economic growth of states around the world. On the other hand, these technologies cause massive human rights violations on a global scale. Therefore, in the context of digitalization, it is extremely important to reconsider approaches to human rights protection, as it is wrong to consider the latest technologies absolutely safe and pose no threat. There is an increasing number of technological threats that call into question the guarantee of human rights and freedoms. For example, restrictions on access to online platforms, systematic violations of privacy, mass surveillance, disregard for the human right to be forgotten, the spread of disinformation and the use of hate speech. These phenomena

deface the new reality, calling into question the adequacy of traditional legal and institutional response mechanisms to the ever-increasing pace of technological change. As a result, political, social, and legal institutions are repeatedly unable to ensure an adequate level of human rights protection in the wake of the rapid digital transformation, which creates an urgent need to modernize legal regulation in this area.

A modern rethinking of technological progress through the prism of fundamental human rights requires recognizing that the latest digital tools are not only a factor of socio-economic development, but also a source of fundamentally new legal challenges. In the context of the rapid digitalization of the main spheres of public life, the issue of striking a balance between the innovativeness of technology and the effective implementation of the protection of human rights and freedoms is becoming increasingly urgent. The legal system, whether at the national or international level, shows a limited ability to adapt to changes caused by scientific and technological progress, which greatly complicates the timely regulation of new social relations. That is why it is now important to introduce adaptive legal mechanisms that can ensure not only legal compatibility of innovations, but also basic guarantees of fundamental human rights in the digital age.

The priority task of the state policy in the field of legal regulation of artificial intelligence is to guarantee the protection of the rights and freedoms of all subjects of civil legal relations related to the development and use of AI technologies with strict adherence to ethical standards and constitutional human rights.

Given the rapid development of the digital environment and the growing scale of cybercrime, especially in the context of the hybrid war waged against Ukraine, the issue of effective counteraction to cyber threats is of utmost importance. International cooperation plays a crucial role in creating a unified legal space for information exchange, prompt response to precedents, and providing a reliable basis for investigating cybercrime.

For Ukraine, it is important not only to consolidate these international legal relations but also to modernize national legislation to meet the latest challenges. For example, regulating the procedure for handling electronic evidence, creating legal instruments for blocking or confiscating digital assets, and ensuring their preservation at the early stages of investigations. The comprehensive implementation of these measures will help strengthen the cyber resilience of the state, protect the rights of citizens in the digital environment and improve the secure environment for the sustainable development of the information society.

Lightning-fast technological advances that cover all aspects of social life, such as facial recognition systems, are attracting considerable attention precisely because of their potential for reliable security and efficient data

management. However, the illusion of innovation may conceal risks that, in the absence of proper legal and technical regulation, may lead to violations of the human right to privacy. A characteristic feature of such systems is the need to process a large amount of personal data, which often exceeds the permitted scope to achieve the goal.

It is worth noting that, as a rule, modern thesological tracking systems do not guarantee absolute accuracy in combining camera data with images available in the database. This can be due to both image quality and gaps in databases or processing errors, which will obviously lead to false results. As a result, doubts arise about the reliability of such systems, which require an increased level of accuracy and responsibility. However, the constant development of technology creates preconditions for improving algorithms, which, subject to active legal support, will make it possible to eliminate or reduce risks and increase the efficiency of their use.

Legal regulation should not only adapt to modern challenges, but also be able to actively formulate clear standards and requirements for the use of artificial intelligence in law enforcement. Particular attention should be paid to regulating the limits and permissibility of interference with citizens' privacy using intelligent technologies. These criteria should be taken into account at the stage of designing the relevant software and developing algorithms for its operation. In their absence, it will be difficult to define the legal framework and create risks to human rights. In view of this, it is crucial to establish clear legal guidelines that would prevent abuse and guarantee compliance with the principles of fairness, legality and transparency in the operation of such systems to protect fundamental human rights.

SUMMARY

The study analyzes the multifaceted challenges facing the human right to privacy in the context of the rapid development of artificial intelligence, which is marked by the massive collection and processing of personal data. The research methodology focuses on a combined approach: 1) analysis of the methods of AI's impact on privacy through mass data collection (including research on the techniques of data collection, processing, aggregation and analysis used by AI algorithms and their potential impact on personal identification, profiling and digital dossier formation), including hidden forms of data collection and their unconscious transfer by users; 2) assessment of the effectiveness of existing legal mechanisms for the protection of personal data in the digital era (national, in particular, the Constitution of Ukraine and Ukrainian legislation on personal data protection and international legal norms (such as the GDPR)); study of the legal regulation of the use of AI in video surveillance and face recognition systems (the section analyzes specific aspects of the use of AI in technologies that

directly affect public and personal privacy). The issues of proportionality, necessity, legitimate aim, transparency and control mechanisms, as well as potential risks of discrimination and mass surveillance arising from such systems are considered. The publication focuses on the principles of consent, purposeful use, storage restrictions, right to be forgotten, and adequacy of security measures, as well as on cross-border data transfer. Generalized approaches of scientific research: the principle of "privacy by design" (provides for the integration of the principle of privacy and data protection at all stages of development, implementation and operation of AI systems in order to anticipate and minimize risks at the initial stages); balance between innovation and human rights protection (search for balanced solutions); strengthening oversight and accountability mechanisms; transparency and explainability of algorithms (the right of users to understand the logic of AI and to challenge decisions based on them); international cooperation and harmonization of legislation (the global nature of AI technologies and data flows requires close international cooperation and further harmonization of legal standards to avoid legal gaps and ensure comprehensive protection of human rights in the digital space.

REFERENCES:

1. Бліхар М. М. Організаційно-правовий механізм захисту персональних даних. *Науковий вісник Ужгородського університету*: серія: Право. Ужгород, 2023. Т. 2. Вип. 77. С. 31-36. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/283773/277973 (дата звернення: 25.06.2025).

2. Гиляка О. С. Право на приватність та захист персональних даних в умовах цифровізації. Вісник Національної Академії правових наук України. Харків: *Право*, 2023. Т. 30, № 1. URL: https://visnyk.kh.ua/web/uploads/journals_pdf/%D0%92%D1%96%D1%81%D0%BD%D0%B8%D0%BA%20%D0%9D%D0%90%D0%9F%D1%80%D0%9D%D0%A3_%D0%A2%D0%BE%D0%BC%2030(1)_2023.pdf#page=15 (дата звернення: 25.06.2025).

3. Гуцалюк М. В. Кіберзагрози під час гібридної війни та протидія організованій кіберзлочинності. Інформація і право, 2025. № 1 (25). С. 123-131. URL: http://il.ippi.org.ua/article/view/324708 (дата звернення: 25.06.2025). DOI: https://doi.org/10.37750/2616-6798.2025.1(52).324708

4. Діордіца І. В. Кібербезпекова політика України: стан та пріоритетні напрями забезпечення : монографія. Херсон : Видавничим дім «Гельветика», 2017. 548 с. URL: http://library.kpi.kharkov.ua/files/new_postupleniya/kipouk.pdf (дата звернення: 25.06.2025).

5. Кравчук В. О. Зарубіжний досвід захисту персональних даних у соціальних мережах. Науковий вісник Ужгородського університету:

серія: Право. Ужгород, 2023. Т. 2. Вип. 78. С. 49-53. URL: https://dspace.uzhnu.edu.ua/jspui/handle/lib/56098 (дата звернення: 25.06.2025).

6. Марущак А. І. Визначення поняття «інформаційні права людини». *Інформація і право.* Вип. 2. С. 21-26.

7. Мрак В. Б. Методи розпізнавання обличчя у систем відеоспостереження з використанням машинного навчання. Інфокомунікаційні технології та електронна інженерія. 2023. Т. 3, № 2. С. 33-42. DOI: 10.23939/ictee2023.02.033

8. Семенюк О. О., Саморай О. К. Особливості правового режиму GDPR в Україні. Проблеми та перспективи реалізації та впровадження міждисциплінарних наукових досягнень: збірник наукових праць з матеріалами VIII Міжнародної наукової конференції, м. Конотоп, 20 грудня 2024 р. Міжнародний центр наукових досліджень. 2024. С. 217–220.

9. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних. Страсбург, 28 січня 1981 року. URL: https://zakon.rada.gov.ua/laws/show/9 (дата звернення: 25.06.2025).

10. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI: станом на 27 жовтня 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 25.06.2025).

11. Гаврилюк А. GDPR по-українськи: ключові аспекти ЗП №8153 «Про захист персональних даних». *Юридична газета online.* № 4 (792). 2024. URL: https://yur-gazeta.com/publications/practice/zahist-intelektualnoyi-vlasnosti-avtorske-pravo/gdpr-poukrayinski-klyuchovi-aspekti-zp-8153-pro-zahist-personalnih-danih.html (дата звернення: 25.06.2025).

12. Конституція України. URL: https://zakon.rada.gov.ua/ laws/show/254%D0%BA/96-%D0%B2% D1%80#Text (дата звернення: 25.06.2025).

13. Регламент Європейського Парламенту і Ради (ЄС) 216/679 від 27.04.2016 р. про захист фізичних осіб при обробці персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). URL: https://ips.ligazakon.net/document/MU16144 (дата звернення: 25.06.2025).

14. Бліхар М. М. Організаційно-правовий механізм захисту персональних даних. Науковий вісник Ужгородського університету: серія: Право. Ужгород, 2023. Т. 2. Вип. 77. С. 31-36. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/283773/277973 (дата звернення: 25.06.2025).

15. Прокопенко О. Є. Розробка навчальної системи для збору персональних даних з використанням штучного інтелекту та соціальної

інженерії. Кваліфікаційна робота. Тернопіль, 2024 URL: https://elartu.tntu.edu.ua/bitstream/lib/48324/1/Masters_Thesis_SBm-62_Prokopenko_O_E_2024.pdf (дата звернення: 25.06.2025).

16. Загальний регламент про захист даних (GDPR). URL: https://gdpr-text.com/uk/ (дата звернення: 25.06.2025).

17. ICO Fines «World's Largest Facial Network.» (2022, May 25). Your Front Page for Information Governance News. URL: https://actnowtraining.blog/2022/05/25/ico-fines-worlds-largest-facial-network/ (дата звернення: 25.06.2025).

18. Kirchhof N. ShareWithCare: Photos of children require special protection online. 2023 URL: https://www.telekom.com/en/media/media-information/archive/sharewithcare-children-s-images-deserve-protection-on-the-net-1048376 (дата звернення: 25.06.2025).

19. Пащенко, О. А., Хоменко, В. Л. Роль правових механізмів при захисті особистих даних в інтернеті. *ББК*, *67*(304.3). Львів, 2023. С. 165-169. URL: https://law.lnu.edu.ua/wp-content/uploads/2015/09/Zbirnyk_7_Lviv_IPconference.pdf#page=165 (дата звернення: 25.06.2025).

20. Пащенко, О. А., Хоменко, В. Л. Роль правових механізмів при захисті особистих даних в інтернеті. *ББК*, *67*(304.3). Львів, 2023. С. 165-169. URL: https://law.lnu.edu.ua/wp-content/uploads/2015/09/Zbirnyk_7_Lviv_IPconference.pdf#page=165 (дата звернення: 25.06.2025).

21. Максимович Т. М. Технології розпізнавання облич і право на приватність та захист персональних даних. Магістерська робота. Київ, 2021. С. 8., с. 15. URL: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/b15e28f6-c716-451e-9da1-4f98635d500d/content (дата звернення: 25.06.2025).

22. Гиляка О. С. Новітні технології та права людини: аналіз деяких критичних проблем цифрової ери. Вісник Національної академії правових наук України, 2023. № 30 (2). С. 15-30. URL: https://visnyk.kh.ua/web/uploads/pdf/%D0%92%D1%96%D1%81%D0%BD%D0%B8%D0%BA%20%D0%9D%D0%90%D0%9F%D1%80%D0%9D%D0%A3_%D1%82%D0%BE%D0%BC%2030_2_2023_%D0%A3%D0%9A%D0%A0-15-30.pdf (дата звернення: 25.06.2025).

23. Nakar S., Greenbaum D. Now you see me. Now you still do: facial recognition technology and the growing lack of privacy. Journal of Science & Technology Law – Boston University. 2017. P. 95. URL: https://www.bu.edu/jostl/files/2017/04/Gree3nbaum-Online.pdf (дата звернення: 25.06.2025).

24. Wright Elias. The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial

Recognition in the Retail Sector. Fordham Intell. Prop. Media & Ent. L.J. 2019. P. 617. URL: https://ir.lawnet.fordham.edu/iplj/vol29/iss2/6/ (дата звернення: 25.06.2025).

25. Ünver H. Akın. Artificial Intelligence, Authoritarianism and the Future of Political Systems. Centre for Economics and Foreign Policy Studies, 2018. P. 4. URL: http://www.jstor.org/stable/resrep26084 (дата звернення: 25.06.2025).

26. Степаненко О. І. Нейромережна система розпізнавання людей в реальному часі у системах безпеки : кваліфікаційна робота магістра спеціальності 121 «Інженерія програмного забезпечення». Науковий керівник А. І. Безверхий. Запоріжжя: ЗНУ, 2024. 87 с. URL: https://dspace.znu.edu.ua/jspui/handle/12345/24554 (дата звернення: 25.06.2025).

27. Гуменюк В. І. Правове регулювання технологій розпізнавання обличчя в ЄС, США та Україні: приватно- та публічно-правовий аспекти: кваліфікаційна робота магістра спеціальності 081 «Право». Київ: НаУКМА, 2024. 95 с. Р. 19-23. URL: https://ekmair.ukma.edu.ua/handle/123456789/30834 (дата звернення: 25.06.2025).

28. Троцький, О. О. Правове регулювання та потенційні ризики застосування штучного інтелекту в правоохоронній діяльності. Штучний інтелект у правовій практиці: межі та можливості. *Збірник тез Всеукраїнського круглого столу.* Львів, 2024. С. 181-187. URL: https://files.znu.edu.ua/files/Bibliobooks/Inshi79/0059014.pdf#page=180 (дата звернення: 25.06.2025).

Information about the author:
Kravchuk Svitlana Mykolaivna,
Senior Lecturer at the Department of Legal Theory and Constitutionalism, Institute of Law, Psychology and Innovative Education,
Lviv Polytechnic National University
12, Stepana Bandera Str., Lviv, 79000, Ukraine,
Juror of the Shevchenkivskyi District Court of Lviv
12, Sichovykh Striltsiv Str., Lviv, 79000, Ukraine