УДК 004.8/73, 333.738
DOI https://doi.org/10.32782/2524-0374/2024-11/72

МАСОВЕ СПОСТЕРЕЖЕННЯ ТА РОЗПІЗНАВАННЯ ОБЛИЧЧЯ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ: ПРАВОВІ ВИКЛИКИ ТА ПЕРСПЕКТИВИ РЕГУЛЮВАННЯ В УКРАЇНІ

MASS SURVEILLANCE AND FACIAL RECOGNITION USING ARTIFICIAL INTELLIGENCE: LEGAL CHALLENGES AND REGULATORY PROSPECTS IN UKRAINE

Машталяр О.М., аспірант кафедри інформаційних технологій
Навчально-науковий інститут права та психології Національної академії внутрішніх справ

Хахановський В.Г., д.ю.н., професор,
професор кафедри інформаційних технологій
Навчально-науковий інститут права та психології Національної академії внутрішніх справ

У статті розглянуто актуальні питання впровадження та використання технологій масового спостереження і розпізнавання обличчя за допомогою штучного інтелекту (ШІ) у контексті правового регулювання в Україні. Автор акцентує увагу на стрімкому розвитку технологій штучного інтелекту та їх застосуванні у сфері безпеки, зокрема для правоохоронної діяльності, громадського контролю та воєнних цілей. Водночас підкреслюється необхідність забезпечення балансу між впровадженням інновацій та дотриманням прав і свобод громадян.

У дослідженні проаналізовано основні правові виклики, що виникають при використанні біометричних даних, такі як ризики порушення приватності, зловживання персональними даними, етичні дилеми, а також недостатнє регулювання в діючому українському законодавстві. Розглянуто ключові аспекти національного законодавства, зокрема Закон України «Про захист персональних даних», та встановлено, що існує низка прогалин, які створюють ризики неправомірного використання технологій розпізнавання обличчя.

Особливу увагу приділено міжнародному досвіду правового регулювання, включно з нормами Загального регламенту захисту даних (GDPR) та Закону ЄС про штучний інтелект (AI Act). Наведено приклади регулювання у країнах ЄС та інших державах, які можуть стати основою для гармонізації українського законодавства з міжнародними стандартами. Визначено необхідність адаптації національної нормативно-правової бази для забезпечення прозорості використання систем масового спостереження і захисту біометричних даних.

Дослідження демонструє, що технології масового спостереження за допомогою ШІ здатні значно підвищити ефективність систем громадської безпеки та сприяти боротьбі зі злочинністю, проте водночас підвищують ризики зловживань і порушень прав людини. У статті наведено конкретні рекомендації щодо удосконалення законодавства, серед яких розробка спеціалізованих законів, створення незалежних регуляторів для моніторингу використання ШІ, впровадження етичних стандартів та підвищення обізнаності громадян щодо їхніх прав.

Автор підкреслює, що впровадження систем розпізнавання обличчя повинно супроводжуватися суворим контролем, щоб уникнути недовіри суспільства до державних органів. Окремо висвітлено важливість використання технологій ШІ в умовах воєнного стану, зокрема для ідентифікації загарбників та запобігання терористичним актам, але з обов'язковим дотриманням етичних і правових стандартів.

Ключові слова: масове спостереження, штучний інтелект, розпізнавання обличчя, біометричні дані, правове регулювання, приватність, Україна, AI Act, GDPR, біометрична інформація.

The article addresses pressing issues related to the implementation and use of mass surveillance and facial recognition technologies powered by artificial intelligence (AI) in the context of legal regulation in Ukraine. The author emphasizes the rapid development of AI technologies and their application in the security sector, particularly for law enforcement activities, public oversight, and military purposes. At the same time, the need to ensure a balance between the introduction of innovations and the protection of citizens' rights and freedoms is highlighted.

The study analyzes key legal challenges arising from the use of biometric data, such as privacy risks, misuse of personal data, ethical dilemmas, and insufficient regulation in existing Ukrainian legislation. Key aspects of national legislation, including the Law of Ukraine "On Personal Data Protection" are examined, revealing several gaps that pose risks of unlawful use of facial recognition technologies.

Particular attention is paid to international legal regulation practices, including the provisions of the General Data Protection Regulation (GDPR) and the EU Artificial Intelligence Act (AI Act). Examples of regulation in EU countries and other states are presented as potential foundations for harmonizing Ukrainian legislation with international standards. The necessity of adapting the national legal framework to ensure transparency in the use of mass surveillance systems and the protection of biometric data is emphasized.

The research demonstrates that AI-powered mass surveillance technologies can significantly enhance public safety systems and support crime prevention efforts. However, they also increase risks of misuse and human rights violations. The article provides specific recommendations for improving legislation, including the development of specialized laws, the establishment of independent regulators to monitor AI usage, the introduction of ethical standards, and raising public awareness about their rights.

The author stresses that the implementation of facial recognition systems must be accompanied by strict oversight to prevent societal distrust in state institutions. The importance of using AI technologies in wartime conditions is particularly highlighted, including their application for identifying invaders and preventing terrorist acts, while ensuring compliance with ethical and legal standards.

Key words: mass surveillance, artificial intelligence, facial recognition, legal regulation, biometric data, privacy, Ukraine, AI Act, GDPR, biometric information.

Постановка проблеми: Масове спостереження та розпізнавання обличчя за допомогою технологій на основі штучного інтелекту (ШІ) стають все більш поширеними інструментами у сучасних суспільствах, зокрема і в Україні. Використання даних технологій відкриває нові можливості для забезпечення безпеки, в тому числі громадської безпеки. Проте одночасно викликає серйозні правові та етичні питання щодо захисту приватності та біометричних даних, не тільки громадян України, а і іноземних громадян, які перебувають на її території. З огляду на швидкий розвиток ШІ та його впровадження у різні сфери життя, стає необхідним розглянути правові виклики та перспективи регулювання цієї діяльності в Україні.

Масове спостереження з використанням ШІ може значно підвищити ефективність правоохоронних органів, сприяти боротьбі з тероризмом та злочинністю, допомогти ЗСУ стримувати натиск агресора, а також оптимізувати управління громадським простором в Україні [1, с. 9]. Проте, ці переваги супроводжуються ризиками зловживань, порушенням прав людини та недовірою суспільства

до державних інституцій. Тому важливо розробити комплексний підхід до регулювання використання ШІ у сфері масового спостереження, який забезпечить баланс між безпекою та захистом приватності наших громадян.

Ситуація в Україні потребує чіткого правового регулювання, оскільки технології розпізнавання обличчя використовуються без належної правової бази. Наприклад, у 2022 році система Clearview AI почала використовуватися для ідентифікації осіб, причетних до військових злочинів, однак це викликало обговорення щодо правового статусу використання таких даних.

Метою даної статті є аналіз правових викликів, пов'язаних з масовим спостереженням та розпізнаванням обличчя за допомогою штучного інтелекту в Україні, а також визначення перспектив регулювання цієї сфери з урахуванням захисту біометричних даних та приватності громадян.

Аналіз останній досліджень та публікацій. Питання масового спостереження та розпізнавання обличчя за допомогою ШІ в Україні з'явилося нещодавно і тому воно потребує додаткового вивчення. Проте, серед наукових досліджень, що можуть бути пов'язані з використання ШІ у масовому спостереженні та розпізнаванні обличчя, виділяються роботи таких дослідників, як В. Г. Хахановський та Т. Г. Чашницька [2, с. 9], які освітлювали теоретичні та практичні проблеми застосування інформаційних технологій на основі ШІ для ідентифікації особи за матеріалами відеозапису. В. Брижко, А. Баранов, В. Пилипчук, які вивчали питання приватності та захисту персональних даних [3, с. 9]. Є ще наукова праця О. Петришина та О. Гиляка [4, с. 9], які розглядають права людини в цифрову епоху. Вони досліджують виклики, загрози та перспективи захисту прав людини у контексті цифрових технологій, підкреслюючи необхідність адаптації правової системи до нових реалій. Також, в мережі Інтернет є достатньо публікацій, які пов'язані з правовими аспектами систем відеомоніторингу, де звертають увагу на необхідність балансування між безпекою та правами громадян [5, с. 9].

В деяких публікація їхні автори, зосереджуються на аналізі чинного законодавства України щодо захисту персональних даних, чітко не вказуючи на існуючі прогалини та необхідність їх усунення. Наприклад Котенський досліджує використання систем розпізнавання обличчя в Україні, зокрема впровадження системи Clearview AI, що викликає значні дискусії щодо приватності та етики [6, с. 9]. В свою чергу Бугера розглядає використання ШІ для запобігання злочинності, аналізуючи правові та етичні аспекти цієї практики [7, с. 10].

Питання масового відео нагляду та розпізнавання обличчя до початку повномасштабного вторгнення в Україну майже не вивчалося та не було таким актуальним. На даний момент на законодавчому рівні проводяться певні рухи для часткового врегулювання даного питання, проте це тільки частина необхідних заходів для врегулювання питання створення та користування системами відеомоніторингу за допомогою ШІ [8, 9, с. 10]. Також вагомий внесок для вивчення та удосконалення регулювання даного питання в Україну відіграють міжнародні законодавчі акти. Наприклад, GDPR [10, 11, 12, 13, с. 10] описує основні принципи захисту персональних даних у Європейському Союзі, які є основою для регулювання використання біометричних даних. Нещодавно Рада ЄС ухвалила Закон про штучний інтелект (AI Act), що детально розглядає нормативні вимоги щодо використання ШІ та може слугувати прикладом для України [14, с. 11]. Конвенція Ради Європи також встановлює стандарти захисту осіб у зв'язку з автоматизованою обробкою персональних даних, що має значний вплив на національні законодавства [15, с. 11]. В Україні нещодавно також зрушилася робота з розробкою та впровадження діючих законодавчих норм, які пов'язані з відеофіксацією.

Виклад основного матеріалу. Масове спостереження за допомогою ШІ включає використання камер відеоспостереження, систем розпізнавання обличчя на основі ШІ та аналізу великих обсягів даних для ідентифікації осіб у публічних місцях [16, с. 11]. Дані технології дозволяють оперативно реагувати на потенційні загрози, проте водночас піднімають питання щодо можливості зловживання та порушення прав людини, включаючи Україну. Наприклад, у Південній Кореї державні установи впроваджують пропускні системи зі ШІ для підвищення безпеки на території певних об'єктів [17, с. 11], а в Індії ШІ використовується для захисту жінок від домагань на вулиці [18, с. 11]. Китай активно використовує ШІ для створення систем тотального спостереження, визначення соціального рейтингу, порушення громадського порядку, що призводить до встановлення «диктатури стеження» [19, с. 11].

Законодавча база України щодо використання біометричних даних та масового спостереження наразі є недостатньо розвиненою, як в інших країнах світу. Закон України «Про захист персональних даних» не містить чітких положень щодо розпізнавання обличчя та використання ШІ в цій сфері [20, с. 11]. Це створює правову невизначеність та ризики для приватності не тільки звичайних громадян, а й державних службовців, співробітників силових структур та дипломатичних установ в тому числі. Постанова Кабінету Міністрів України № 1073-2017-п встановлює основні принципи національної системи біометричної верифікації, проте не враховує всі нюанси використання ШІ в масовому контролі через систем тотального спостереження [16, с. 11]. Закон «Про оперативно-розшукову діяльність» також не регулює використання біометричних даних, що ускладнює контроль за їх використанням [21, с. 11].

Основними правовими викликами для України є:

1. **Недостатній захист біометричних даних:** Відсутність спеціалізованого законодавства щодо захисту біометричної інформації, що включає в себе фото обличчя, робить дані вразливими до зловживань Закон України «Про захист персональних даних» та інші законодавчі акти не передбачають окремих норм, які б регулювали заходи, під час зберігання та використання біометричних даних, що створює ризики їхнього неправомірного використання.
2. **Відсутність прозорості:** Відсутність чітких правил щодо збору, обробки, використання та зберігання біометричних даних призводить до недовіри громадян та потенційних порушень прав. Без прозорих механізмів контролю, громадяни не мають можливості знати, як їхні дані використовуються та захищаються [2, с. 9].
3. **Етичні питання:** Використання ШІ у розпізнаванні обличчя піднімає етичні питання щодо дискримінації, неправомірного контролю та втручання у приватне життя. Наприклад, системи розпізнавання обличчя можуть мати вищу похибку при ідентифікації осіб певних етнічних груп, що веде до дискримінації [4, с. 9].
4. **Міжнародні стандарти та відповідність:** Відсутність адаптації до міжнародних стандартів, таких як GDPR та AI Act ускладнює інтеграцію з європейськими та світовими ринками та законодавствами. Гармонізація українського законодавства з міжнародними стандартами є необхідною для забезпечення адекватного захисту даних [14, 15, с. 11] та полегшення міжнародного співробітництва [10, 11, 12, 13, с. 10].

Міжнародний досвід показує, що країни, які запровадили спеціальні закони щодо використання біометричних даних, можуть ефективніше балансувати між безпекою та захистом прав громадян. Наприклад, Європейський Союз у рамках GDPR та Закону про штучний інтелект встановив суворі правила щодо обробки персональних даних, включаючи біометричні. Дані закони визначають біометричні дані як особливу категорію даних, які

потребують додаткового захисту [23, с. 12]. У Південній Кореї державні установи впроваджують системи розпізнавання обличчя для підвищення безпеки громадських місць [17, с. 11]. У США існує різний рівень регулювання на федеральному та штатному рівнях, що створює комплексну систему захисту [6, с. 9]. В Азії, такі країни, як Китай, активно впроваджують системи стеження за допомогою ШІ, що призводить до встановлення тоталітарного режиму [19, с. 11].

Для удосконалення правового регулювання масового спостереження та розпізнавання обличчя в Україні необхідно:

1. **Розробка спеціалізованого законодавства:** Включення положень щодо захисту біометричних даних та регулювання використання ШІ у масовому відеоспостереженні та розпізнаванні обличчя. Це може включати визначення умов збору, обробки та зберігання біометричної інформації, а також механізми її захисту [14, с. 11]. Законодавчі ініціативи повинні передбачати чіткі критерії для використання ШІ у громадських місцях та відповідальність за порушення цих правил.

2. **Створення механізмів контролю та нагляду:** Впровадження органів, відповідальних за моніторинг дотримання законодавства та захист прав громадян. Наприклад, створення незалежного регулятора з питань захисту даних [8, 9, с. 10]. Цей орган повинен мати повноваження проводити аудит систем масового спостереження та забезпечувати дотримання правових норм.

3. **Підвищення обізнаності громадян:** Інформування населення про їхні права щодо захисту біометричних даних та можливості звернення за захистом. Також є важливим інформування де системи на основі ШІ задіяні в Україні. Це може включати освітні кампанії та прозорі інформаційні ресурси [22, с. 12]. Обізнаність громадян є ключовим фактором у забезпеченні їхнього захисту та довіри до систем масового спостереження.

4. **Адаптація до міжнародних стандартів:** Гармонізація національного законодавства з міжнародними стандартами, такими як GDPR, Закон ЄС про штучний інтелект, для забезпечення сумісності та підвищення рівня захисту даних [23, с. 12]. Це дозволить Україні інтегруватися в глобальні технологічні ланцюги та забезпечити адекватний захист персональних даних.

Технічні аспекти використання ШІ у розпізнаванні обличчя включають точність алгоритмів, швидкість обробки даних та здатність системи адаптуватися до різних умов освітлення та кутів зору [6, с. 9]. Наприклад, системи можуть мати різну ефективність залежно від типу освітлення, ракурсу обличчя та віку осіб. Проте, технічні досягнення повинні супроводжуватися етичними принципами, які гарантують, що технології не використовуються для дискримінації чи неправомірного контролю [8, 9, с. 10].

Масове спостереження може мати різні соціальні наслідки, включаючи зниження рівня приватності, підвищення почуття безпеки серед населення, але також і ризик зловживань з боку державних органів та приватних компаній. Важливо забезпечити баланс між використанням технологій для забезпечення громадської безпеки та захистом прав людини [20, 21, с. 11]. В умовах війни з Російською Федерацією, використання ШІ для розпізнавання обличчя набуває особливої важливості для забезпечення безпеки та оборони країни. Використання ШІ може сприяти підвищенню ефективності оборони та безпеки, проте потребує ретельного регулювання для уникнення зловживань. ШІ може допомогти в ідентифікації загарбників, відстеженні їх переміщень та запобіганні терористичним актам. Проте, це також підвищує ризики порушення приватності та зловживань владою [22, 24, с. 12]. Наприклад, використання систем розпізнавання обличчя може сприяти швидшій ідентифікації ворожих сил, але без належного контролю це може призвести до неправомірного переслідування громадян.

Висновки. Масове спостереження та розпізнавання обличчя за допомогою штучного інтелекту в Україні стикаються з численними правовими викликами, зокрема щодо захисту біометричних даних та приватності громадян. Аналіз сучасних досліджень показує необхідність удосконалення законодавчої бази для регулювання цієї сфери. Перспективи подальших розвідок включають розробку ефективних правових механізмів, що забезпечать баланс між безпекою та захистом прав людини, а також підвищення обізнаності громадян щодо їхніх прав у контексті використання технологій ШІ. Впровадження спеціалізованого законодавства, створення незалежних органів контролю та адаптація до міжнародних стандартів є ключовими кроками для забезпечення ефективного та етичного використання ШІ у сфері масового спостереження та розпізнавання обличчя в Україні.

ЛІТЕРАТУРА

1. Безпека vs приватність. Чи потрібен Україні повсюдний відеонагляд URL: https://ms.detector.media/trendi/post/34349/2024-03-05-bezpeka-vspryvatnist-chy-potriben-ukraini-povsyudnyy-videonaglyad/ (дата звернення: 19.09.2024).

2. Хахановський В. Г., Чашницька Т. Г. Ідентифікація особи за ходою, зафіксованою в матеріалах відеозапису. Криміналістичний вісник. 2020. № 1(33). С. 72–79.

3. Брижко В. М., Пилипчук В. Г. Приватність, конфіденційність та безпека персональних даних. Інформація і право. № 1(32)/2020. С. 33–46; Становлення і розвиток правових основ та системи захисту персональних даних в Україні: монографія / В. Г. Пилипчук, В. М. Брижко, О. А. Баранов, К. С. Мельник ; за ред. В. М. Брижка, В. Г. Пилипчука. Київ: ТОВ "Видавничий дім "АртЕк", 2017. 226 с.; Пилипчук В.Г., Брижко В.М. та ін. Захист прав, приватності та безпеки людини в інформаційну епоху: монографія ; за заг. ред. акад. НАПрН України В. Г. Пилипчука. Київ-Одеса: Фенікс, 2020. 260 с.

4. Петришин О. В., Гиляка О. С. Права людини в цифрову епоху: виклики, загрози та перспективи. *Вісник* Академії правових наук. 2021. № 1. С. 15–23.

5. Бердиченко, І. О. Системи відеомоніторингу стану публічної безпеки: проблеми правового регулювання // *ОЛЬВІЙСЬКИЙ ФОРУМ–2024: стратегії країн Причорноморського регіону в геополітичному просторі*, Миколаїв, 2024. С. 20–24.

6. Андрій Котенський. Україна використовує систему розпізнання Clearview AI. URL: https://portal.lviv.ua/news/2022/03/14/ukraina-vykorystovuie-systemu-rozpiznannia-clearview-ai (дата звернення: 19.09.2024).

7. Бугера О.І. Використання штучного інтелекту для запобігання злочинності. Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки. Том 32(71). № 6. 2021. С. 82–86.

8. Про єдину систему відеомоніторингу стану публічної безпеки : Проект Закону України від 20.02.2024 р. № 11031. Дата оновлення: 20.02.2024. URL: https://ips.ligazakon.net/document/JI10713A (дата звернення: 19.09.2024).

9. Про внесення змін до деяких законодавчих актів України щодо систем моніторингу стану безпеки : Проект Закону України від 01.03.2019 р. № 10120. Дата оновлення: 01.03.2019. URL: https://ips.ligazakon.net/document/JH7T400A (дата звернення: 19.09.2024).

10. General Data Protection Regulator (GDPR) від 25 травня 2016 року. – Art 4. URL: https://gdpr-text.com/uk/read/article-4 (дата звернення: 19.09.2024).

11. General Data Protection Regulator (GDPR) від 25 травня 2016 року. – Art 17. URL: https://gdpr-text.com/uk/read/article-17/ (дата звернення: 19.09.2024).

12. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27.04.2016 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС. Дата оновлення: 27.04.2016. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 19.09.2024).
13. General Data Protection Regulator (GDPR) від 25 травня 2016 року. – Art 9. URL: https://gdpr-text.com/uk/read/article-9 (дата звернення: 19.09.2024).
14. Головне про Європейський закон про штучний інтелект. URL: https://www.robert-schuman.eu/ua/visnyk/1076 (дата звернення: 19.09.2024).
15. Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних. Дата оновлення: 01.01.2011. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 19.09.2024).
16. Про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства: Постанова Кабінету Міністрів України від 27.12.2017 р. № 1073-2017-п. Дата оновлення: 13.02.2024. URL: https://zakon.rada.gov.ua/laws/show/1073-2017-%D0%BF#Text (дата звернення: 19.09.2024).
17. У Південній Кореї держустанови облаштують пропускною системою зі штучним інтелектом. URL: https://www.ukrinform.ua/rubric-technology/3150230-u-pivdennij-korei-oblastuut-derzustanovi-propusknousistemou-zi-stucnim-intelektom.html (дата звернення: 19.09.2024).
18. В Індії штучний інтелект «захищатиме» жінок від домагань на вулиці. URL: https://www.ukrinform.ua/rubric-technology/3176317-v-indii-stucnij-intelekt-zahisatime-zinok-vid-domagan-na-vulici.html (дата звернення: 19.09.2024).
19. Китай створює диктатуру стеження за допомогою ШІ URL: https://dv-gazeta.info/news/kitay-stvoryuye-diktaturu-stezhennya-za-dopomogoyu-shi.html (дата звернення: 19.09.2024).
20. Про захист персональних даних : Закон України від 01 червня 2010 р. № 2297-VI. Дата оновлення: 27.04.2024. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 19.09.2024).
21. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 р. № 2135-XII. Дата оновлення: 09.08.2024. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text (дата звернення: 19.09.2024).
22. Штучний інтелект воює в Україні URL: https://zaxid.net/shtuchniy_intelekt_voyuye_v_ukrayini_n1576239 (дата звернення: 19.09.2024).
23. Законодавча резолюція Європейського Парламенту від 13.03.2024 стосовно регламенту Європейського Парламенту та Ради з гармонізації правил щодо Штучного Інтелекту. URL: https://www.europarl.europa.eu/doceo/document/TA-9-2024- 0138_EN.html (дата звернення: 19.09.2024).
24. Війну виграють технології». Як штучний інтелект допоможе перемогти у війні з РФ? URL: https://www.epravda.com.ua/publications/2023/12/4/707197/ (дата звернення: 19.09.2024).