АКАДЕМІЧНІ ВІЗІЇ
Випуск 48/2025

АЛГОРИТМІЧНЕ ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ГРОМАДСЬКОГО ПОРЯДКУ: ПРАВОВІ МЕЖІ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Варинський Владислав[1]

Опубліковано	Секція	УДК
30.10.2025	Право	340:004.8:351.74(477)

DOI: https://doi.org/10.5281/zenodo.64899<:9

Анотація. У статті досліджено правові межі застосування штучного інтелекту у правоохоронній діяльності та сфері охорони громадського порядку та безпеки в контексті цифровізації публічного управління, розвитку алгоритмічних систем аналізу даних та адаптації національного законодавства до європейських стандартів. Обґрунтовано, що технології штучного інтелекту здатні підвищити ефективність правоохоронної діяльності шляхом автоматизованого опрацювання великих масивів інформації, ідентифікації осіб, виявлення зв'язків між подіями, прогнозування криміногенних ризиків, оптимізації розподілу поліцейських ресурсів та структурування доказової інформації. Водночас в статті доведено, що використання таких систем у публічному просторі та в діяльності органів, наділених владними повноваженнями, формує підвищені ризики непропорційного втручання у право на приватність, непрямої дискримінації, алгоритмічного профілювання, помилкової біометричної ідентифікації, формування «цифрової тіні» особи, посилення презумпції підозрілості та неконтрольованого масового спостереження. Особливу увагу в статті приділено проблемі недостатньої прозорості алгоритмічних моделей, залежності результатів їх функціонування від якості навчальних даних, небезпеці автоматизаційного упередження та ризику фактичної підміни людського розсуду машинними висновками. На підставі аналізу положень AI Act, практики Європейського суду з прав людини, та зарубіжних прикладів застосування систем розпізнавання облич і предиктивної поліцейської аналітики запропоновано модель правового обмеження використання штучного інтелекту у правоохоронній сфері України. Така модель має передбачати законодавче розмежування заборонених, високоризикових і допоміжних застосувань, обов'язковий людський нагляд, оцінку впливу на права та свободи людини, зовнішній аудит, логування алгоритмічних операцій, судовий контроль, оскаржуваність результатів та спеціальні гарантії використання таких систем в умовах воєнного стану.

Ключові слова: штучний інтелект, правоохоронна діяльність, охорона громадського порядку, публічна безпека, біометрична ідентифікація, предиктивна поліція, алгоритмічне профілювання, AI Act, права людини, людський нагляд.

[1] кандидат політичних наук, доцент,
доцент кафедри філософії та українстики
Національного університету «Одеська морська академія»
ORCID: https://orcid.org/0000-0001-5837-6201
Vlad.varinskiy@gmail.com

ALGORITHMIC SUPPORT FOR PUBLIC ORDER PROTECTION: LEGAL LIMITS OF USING ARTIFICIAL INTELLIGENCE IN LAW ENFORCEMENT ACTIVITIES

Abstract. The article explores the legal limits of the application of artificial intelligence in law enforcement and the field of public order and security in the context of the digitalization of public administration, the development of algorithmic data analysis systems and the adaptation of national legislation to European standards. It is substantiated that artificial intelligence technologies are capable of increasing the efficiency of law enforcement through automated processing of large amounts of information, identification of individuals, identification of connections between events, prediction of criminogenic risks, optimization of the distribution of police resources and structuring of evidentiary information. At the same time, the article proves that the use of such systems in public space and in the activities of bodies vested with power creates increased risks of disproportionate interference with the right to privacy, indirect discrimination, algorithmic profiling, erroneous biometric identification, the formation of a "digital shadow" of a person, strengthening the presumption of suspicion and uncontrolled mass surveillance. The article pays special attention to the problem of insufficient transparency of algorithmic models, the dependence of the results of their functioning on the quality of training data, the danger of automation bias and the risk of actual replacement of human judgment with machine conclusions. Based on the analysis of the provisions of the AI Act, the practice of the European Court of Human Rights, and foreign examples of the use of facial recognition systems and predictive police analytics, a model of legal restrictions on the use of artificial intelligence in the law enforcement sector of Ukraine is proposed. Such a model should provide for a legislative delimitation of prohibited, high-risk and auxiliary applications, mandatory human supervision, an assessment of the impact on human rights and freedoms, an external audit, logging of algorithmic operations, judicial control, the appealability of results and special guarantees for the use of such systems in martial law.

Keywords: artificial intelligence, law enforcement, public order protection, public safety, biometric identification, predictive policing, algorithmic profiling, AI Act, human rights, human surveillance.

Актуальність. Цифровізація правоохоронної діяльності змінює традиційні механізми охорони громадського порядку, запобігання кримінальним правопорушенням та розслідування злочинів. Якщо класична модель поліцейської діяльності спиралася переважно на людське спостереження, оперативну інтуїцію, досвід, локальні бази даних і процесуальні рішення конкретних посадових осіб, то сучасна модель дедалі частіше включає алгоритмічний аналіз великих масивів інформації, автоматизоване зіставлення зображень, розпізнавання облич, прогнозування криміногенних осередків, аналіз соціальних мереж, відеопотоків, фінансових операцій і цифрових слідів. Унаслідок цього штучний інтелект поступово перетворюється з допоміжної технології на чинник, здатний реально впливати на правовий статус особи, інтенсивність поліцейського контролю, порядок реалізації права на приватність, свободу пересування, свободу мирних зібрань та гарантії недискримінації.

Проблема полягає не в самому факті використання штучного інтелекту правоохоронними органами. Такий інструментарій може бути суспільно корисним, особливо в умовах зростання обсягів цифрових даних, дефіциту кадрових ресурсів, високої динаміки злочинності та потреби швидкого реагування на загрози публічній безпеці. Наукова суперечність полягає в іншому: правоохоронна сфера потребує технологій, здатних швидко виявляти приховані закономірності та підвищувати ефективність превенції, але саме ці технології здатні непомітно трансформувати охорону громадського

порядку в режим алгоритмічного нагляду, де особа оцінюється не за правовими фактами, а за статистичними кореляціями, поведінковими профілями та непрозорими машинними висновками.

Така суперечність особливо гостра для України. Воєнний стан, протидія збройній агресії, потреба ідентифікації диверсійно-розвідувальних груп, колаборантів, військовослужбовців держави-агресора, осіб, причетних до воєнних злочинів, а також необхідність швидкого аналізу значних масивів фото-, відео- та OSINT-інформації об'єктивно стимулюють використання систем штучного інтелекту у правоохоронній сфері. Водночас надзвичайний безпековий контекст не повинен ставати підставою для постійної інституціоналізації масового біометричного спостереження або неконтрольованого алгоритмічного профілювання після повернення до звичайного правопорядку.

Проблематика застосування штучного інтелекту в правоохоронній сфері розглядається у декількох взаємопов'язаних площинах: технологічній, криміналістичній, адміністративно-правовій, інформаційно-правовій, правозахисній та етичній. У працях, присвячених практичному використанню штучного інтелекту для потреб кримінальної юстиції, наголошується на його здатності імітувати людське розпізнавання закономірностей, аналізувати значні обсяги інформації та підтримувати ухвалення рішень у складних слідчих ситуаціях [1]. Е. Бриньйольфссон та Е. Макафі, аналізуючи бізнесову й управлінську природу штучного інтелекту, підкреслюють, що машинне навчання означає перехід від програмування конкретного результату до навчання системи на прикладах, що має ключове значення для розуміння як переваг, так і ризиків таких технологій [2].

У вітчизняному науковому дискурсі перспективи проактивної діяльності поліції та використання алгоритмічних інструментів у правоохоронній сфері пов'язуються з аналізом даних, машинним навчанням, розпізнаванням образів та здатністю швидко обробляти великі обсяги інформації для виявлення закономірностей і потенційних підозрюваних [3]. О.І. Зачек, Ю.І. Дмитрик та В.В. Сеник звертають увагу на роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності, зокрема в контексті українських безпекових викликів і використання інструментів ідентифікації [4].

Зарубіжна література й аналітика демонструють неоднозначність алгоритмічної трансформації правоохоронної діяльності. З одного боку, приклади використання Qlik Sense, Clearview AI, Dejaview та аналітичних платформ на зразок Söze підтверджують практичний потенціал штучного інтелекту для швидкого зіставлення даних, пошуку осіб, аналізу доказової інформації та прогнозування криміногенних ризиків [5; 6; 7; 8]. З іншого боку, дослідження ProPublica щодо COMPAS, наукові дискусії про алгоритмічну упередженість і праці, присвячені дебатам навколо справедливості алгоритмічного оцінювання, демонструють ризики расової, соціальної або територіальної дискримінації, які виникають унаслідок використання історично викривлених даних [9; 10; 11].

Окреме значення має практика Європейського суду з прав людини щодо приватності, масового спостереження, зберігання біометричних даних і прихованого стеження. Рішення у справах S. and Marper v. the United Kingdom, Big Brother Watch and Others v. the United Kingdom, Roman Zakharov v. Russia та Glukhin v. Russia формують правовий контекст, у межах якого будь-яке використання біометричних і наглядових технологій має оцінюватися крізь призму законності, необхідності, пропорційності, передбачуваності правового регулювання та ефективності зовнішнього контролю [12; 13; 14; 15]. На рівні Європейського Союзу ключовим нормативним орієнтиром є Regulation (EU) 2024/1689, який закріплює ризикоорієнтовану модель регулювання штучного інтелекту, зокрема для правоохоронної сфери [16].

Метою статті є формування науково обґрунтованої моделі правових меж застосування штучного інтелекту у правоохоронній діяльності та сфері охорони громадського порядку з урахуванням ризиків для прав людини, положень AI Act, практики ЄСПЛ та безпекового контексту України.

Для досягнення мети поставлено такі завдання: визначити функціональний потенціал штучного інтелекту для правоохоронної діяльності; охарактеризувати основні ризики його застосування у сфері громадського порядку; проаналізувати ризикоорієнтовану модель AI Act щодо правоохоронних систем; сформулювати пропозиції щодо правового обмеження використання штучного інтелекту в Україні.

Методологічну основу становлять діалектичний метод, який дозволив розкрити суперечність між ефективністю алгоритмічних інструментів і ризиками для прав людини; системний метод, застосований для розгляду штучного інтелекту як елементу правоохоронної інфраструктури; формально-юридичний метод, використаний для аналізу AI Act і стандартів прав людини; порівняльно-правовий метод, необхідний для зіставлення зарубіжних моделей використання штучного інтелекту з потребами українського регулювання; аксіологічний метод, спрямований на оцінку допустимості алгоритмічного втручання у приватність, свободу та рівність особи.

Виклад основного матеріалу. Штучний інтелект у правоохоронній сфері виконує не одну, а декілька різних функцій. Найпростішим є використання алгоритмів як інструментів пошуку, класифікації та зіставлення даних. На цьому рівні система не ухвалює юридично значущого рішення щодо особи, а лише прискорює технічну роботу з інформацією: аналізує відеозаписи, зіставляє обличчя з базами даних, обробляє телефонні з’єднання, фінансові транзакції, повідомлення в соціальних мережах, відкриті джерела та інші цифрові сліди. Такий рівень використання штучного інтелекту є найближчим до допоміжної криміналістичної функції та за належного контролю може істотно підвищити ефективність розслідування.

Другий рівень пов’язаний із предиктивною аналітикою. Алгоритми аналізують історичні дані про час, місце, спосіб, повторюваність і соціальний контекст правопорушень, після чого формують прогнози щодо потенційних криміногенних осередків. Для охорони громадського порядку це може мати практичне значення: органи поліції отримують можливість раціональніше розподіляти патрульні ресурси, планувати превентивні заходи, прогнозувати місця концентрації ризиків під час масових заходів, оперативно реагувати на сигнали про можливі загрози публічній безпеці. Водночас саме предиктивна функція є однією з найбільш юридично чутливих, оскільки вона легко зміщується від прогнозу події до прогнозу «небезпечності» конкретної особи або групи осіб.

Третій рівень полягає у використанні штучного інтелекту для біометричної ідентифікації. Системи розпізнавання облич можуть мати легітимну мету: розшук осіб, зниклих безвісти, ідентифікація загиблих, встановлення осіб, причетних до тяжких злочинів, перевірка інформації на блокпостах в умовах воєнного стану, документування воєнних злочинів. У цьому аспекті показовим є досвід застосування Clearview AI, зокрема для ідентифікації осіб в умовах російської агресії проти України [4; 17; 18]. Проте правова оцінка такої технології не може вичерпуватися її ефективністю. Необхідно одночасно з’ясовувати джерела даних, правові підстави їх збирання, строки зберігання, межі доступу, процедури виправлення помилок і можливість оскарження результатів ідентифікації.

Четвертий рівень пов’язаний з аналізом доказової інформації. Інструменти на зразок Söze демонструють здатність алгоритмічних систем обробляти масиви доказових матеріалів, які за обсягом істотно перевищують можливості ручного аналізу [7; 8]. Для

правоохоронної діяльності це має очевидну практичну користь: скорочення часу опрацювання матеріалів, виявлення неочевидних зв'язків між подіями, аналіз відео, фінансових операцій, електронного листування та інших цифрових даних. Однак у цій сфері також зберігається ключове обмеження: алгоритм може допомагати слідчому чи аналітику, але не повинен замінювати процесуальне мислення, оцінку доказів і юридичну відповідальність людини за прийняте рішення.

Основний ризик використання штучного інтелекту у правоохоронній сфері полягає в тому, що статистична закономірність може бути помилково сприйнята як юридичний факт. Право оперує доказами, підставами, процесуальними гарантіями, презумпцією невинуватості та індивідуальною відповідальністю. Алгоритм натомість працює з даними, кореляціями, імовірностями та моделями. Якщо правоохоронний орган некритично переносить алгоритмічний висновок у сферу владного рішення, виникає небезпека підміни юридичного доведення математичною імовірністю.

Першою групою ризиків є дискримінаційні наслідки алгоритмічної аналітики. Досвід COMPAS показав, що системи оцінювання ризиків можуть відтворювати історичні соціальні перекоси, якщо навчаються на даних, у яких уже закладено нерівність у діяльності поліції, судів або пенітенціарної системи [9]. Подальша наукова дискусія щодо цього прикладу засвідчила, що проблема не зводиться лише до помилки конкретного алгоритму. Вона полягає у складності визначення самої справедливості алгоритмічного оцінювання, оскільки різні статистичні критерії «точності», «неупередженості» та «рівності» можуть конфліктувати між собою [10; 11]. Для України це означає, що імпорт або розроблення систем предиктивної поліції без попередньої оцінки навчальних даних може спричинити територіальне, соціальне або етнічне профілювання.

Другою групою ризиків є втручання у приватність. Масове відеоспостереження, автоматизоване розпізнавання облич, моніторинг соціальних мереж і об'єднання різних баз даних створюють ситуацію, коли правоохоронний орган отримує не окрему інформацію про конкретний факт, а майже безперервний цифровий профіль поведінки людини. Такий профіль може охоплювати маршрути пересування, коло спілкування, участь у масових заходах, політичну активність, соціальні зв'язки та інші аспекти приватного життя. У практиці ЄСПЛ саме передбачуваність правового регулювання, наявність незалежного контролю, обмеження цілей обробки даних і можливість ефективного захисту визнаються ключовими умовами допустимості втручання держави у приватність [12; 13; 14].

Третьою групою ризиків є помилкова ідентифікація. У правоохоронній діяльності навіть одинична помилка системи розпізнавання облич може мати тяжкі наслідки: незаконне затримання, обшук, кримінальне переслідування, репутаційна шкода, обмеження свободи пересування. Відомі приклади помилкових арештів, пов'язаних із використанням технологій розпізнавання облич, демонструють, що технічна похибка у правоохоронній сфері не є нейтральною. Вона трансформується у владну дію держави щодо конкретної особи [19].

Четверта група ризиків пов'язана з формуванням «цифрової тіні» особи. Йдеться про ситуацію, коли алгоритмічний інструмент формує прихований ризиковий профіль людини, який впливає на інтенсивність поліцейської уваги, але сама особа не знає про існування такого профілю, не розуміє критеріїв його створення і не має реального механізму оскарження. У такій моделі особа формально не зазнає покарання, але фактично потрапляє в режим підвищеного нагляду. Саме тому правова система має вимагати не лише точності алгоритму, а й процедурної прозорості настільки, наскільки це сумісно з інтересами оперативної діяльності та безпеки.

AI Act не виходить із презумпції повної заборони штучного інтелекту в правоохоронній сфері. Його логіка інша: заборонити практики, несумісні з основоположними правами, а для високоризикових систем встановити суворий режим попереднього та поточного контролю. Для України такий підхід є продуктивним, оскільки дозволяє уникнути двох крайнощів: технологічного романтизму, за якого ефективність виправдовує будь-яке втручання, і технологічного заперечення, за якого штучний інтелект повністю вилучається з правоохоронної діяльності навіть там, де він може бути легітимним і корисним.

До заборонених практик у логіці AI Act належать, зокрема, системи, що маніпулюють поведінкою людини, експлуатують уразливість окремих груп, здійснюють соціальний скоринг або біометричну категоризацію за чутливими ознаками. Для правоохоронної діяльності особливе значення має обмеження дистанційної біометричної ідентифікації в режимі реального часу у публічному просторі. Така ідентифікація не може розглядатися як звичайна поліцейська технологія, оскільки вона потенційно охоплює невизначене коло осіб, які не є підозрюваними, не вчиняють правопорушення і перебувають у громадському просторі на законних підставах [16].

Системи штучного інтелекту, які використовуються для правоохоронних цілей, як правило, мають визнаватися високоризиковими. Це означає, що для них необхідні спеціальні вимоги до управління ризиками, якості навчальних даних, технічної документації, прозорості, точності, кібербезпеки, логування, аудиту та людського нагляду. У правоохоронній сфері ці вимоги не можуть бути суто технічними. Вони мають безпосередній юридичний зміст: якість даних впливає на недискримінацію; логування забезпечує можливість відповідальності; технічна документація створює умови для судового контролю; людський нагляд гарантує, що остаточне владне рішення не буде передане алгоритму.

Особливої уваги потребує принцип людського нагляду. Для правоохоронних застосувань неприйнятною має бути модель «human-out-of-the-loop», за якої система після запуску самостійно формує обов'язковий для виконання результат без реальної можливості втручання людини. Модель «human-on-the-loop» може бути допустимою лише для технічного моніторингу або попереднього аналізу, але не для рішень, що істотно впливають на права особи. Найбільш відповідною для демократичного правопорядку є модель «human-in-the-loop», у межах якої посадова особа не лише формально підтверджує результат, а й реально здатна зрозуміти, перевірити, відхилити або скоригувати алгоритмічний висновок.

Звідси випливає вимога пояснюваності. Для правоохоронних органів не може бути достатнім посилання на те, що «система визначила ризик». Якщо алгоритмічний результат стає підставою для посиленої перевірки, затримання, оперативної розробки, обшуку, обмеження доступу до масового заходу або іншого втручання, орган влади має бути здатним пояснити хоча б загальну логіку такого рішення. Повна непрозорість алгоритму не може компенсуватися авторитетом розробника або режимом комерційної таємниці.

Український контекст відрізняється від багатьох європейських юрисдикцій через поєднання двох чинників: воєнного стану та прискореної цифровізації публічних функцій. В умовах збройної агресії держава об'єктивно потребує технологій, які дозволяють швидко ідентифікувати осіб, аналізувати великі масиви візуальної інформації, виявляти колабораційну діяльність, встановлювати причетність до воєнних злочинів, перевіряти ризики на блокпостах, шукати зниклих безвісти та загиблих. Саме тому повна заборона

використання штучного інтелекту у правоохоронній сфері не відповідала б реальним потребам національної безпеки.

Однак воєнний стан не повинен руйнувати межі правового регулювання. Надзвичайна ситуація може виправдати розширення окремих інструментів безпеки лише за умови, що такі інструменти мають чітку правову підставу, визначену мету, часові межі, коло уповноважених суб'єктів, процедури доступу до даних, правила зберігання й видалення інформації, механізми внутрішнього та зовнішнього контролю. Інакше тимчасові інструменти воєнного часу можуть перетворитися на постійні механізми поліцейського нагляду у звичайних умовах.

Для сфери охорони громадського порядку це має особливе значення. Масові заходи, громадські зібрання, евакуаційні процеси, робота блокпостів, комендантські обмеження, контроль за переміщенням осіб у прифронтових регіонах можуть створювати ситуації, у яких правоохоронні органи будуть зацікавлені у використанні біометричної ідентифікації або предиктивного аналізу. Проте участь особи у публічному просторі не повинна автоматично означати її згоду на повне алгоритмічне відстеження. У демократичній державі охорона громадського порядку має забезпечувати безпеку, але не перетворювати громадський простір на простір постійної біометричної перевірки.

Окремим питанням є співвідношення правоохоронної діяльності та діяльності спецслужб. У сфері національної безпеки рівень секретності об'єктивно вищий, однак це не скасовує потреби у правових межах. Навпаки, саме таємність створює додатковий ризик зловживань, тому використання штучного інтелекту для контррозвідки, аналізу комунікацій, виявлення мереж впливу або ризикових осіб має супроводжуватися спеціальними процедурами авторизації, внутрішнього документування, парламентського або іншого незалежного контролю, а також відкладеними механізмами перевірки законності після завершення чутливої операції.

Правове регулювання штучного інтелекту у правоохоронній діяльності доцільно будувати не за принципом загального дозволу або загальної заборони, а за принципом диференційованих режимів. Перший режим має охоплювати заборонені практики. До них слід віднести соціальний скоринг громадян для правоохоронних цілей; біометричну категоризацію за чутливими ознаками; використання алгоритмів, спрямованих на маніпулятивний вплив на поведінку особи; масову дистанційну біометричну ідентифікацію в реальному часі у публічному просторі без чітко визначених законом винятків і без попереднього судового або іншого незалежного контролю.

Другий режим має стосуватися високоризикових правоохоронних систем. До нього доцільно віднести алгоритми предиктивної поліції, системи оцінки ризику особи, інструменти автоматизованого відбору об'єктів оперативної уваги, системи розпізнавання облич для розшукових цілей, алгоритмічні платформи аналізу доказів і великомасштабні інтегровані системи відеоспостереження. Їх використання не повинно бути заборонене автоматично, але має допускатися лише за наявності попередньої оцінки впливу на права людини, перевірки якості даних, документації логіки обробки, режиму логування, зовнішнього аудиту, періодичного перегляду ефективності та правової пропорційності.

Третій режим може охоплювати допоміжні низько- або помірно ризикові інструменти: автоматизований переклад, технічне сортування документів, пошук за відкритими джерелами, анонімізовану статистичну аналітику, інформаційно-довідкову підтримку працівників поліції. Такі системи не повинні обтяжуватися надмірними процедурами, однак навіть для них необхідні правила кібербезпеки, захисту даних,

службового використання, заборони несанкціонованого копіювання інформації та фіксації відповідальної посадової особи.

У законодавчому вимірі така модель потребує внесення змін до актів, що регулюють діяльність Національної поліції, оперативно-розшукову діяльність, захист персональних даних, інформаційну безпеку та використання цифрових технологій органами публічної влади. Центральним має бути не формальне проголошення можливості використання штучного інтелекту, а встановлення умов допустимості: законна мета, правова підстава, пропорційність, мінімізація даних, людський контроль, заборона автоматизованого остаточного рішення щодо особи, журналювання дій системи, аудит, можливість оскарження та відповідальність посадових осіб.

Для практики охорони громадського порядку доцільно закріпити окремий стандарт: штучний інтелект може використовуватися для попереднього аналізу ризиків, планування сил і засобів, виявлення об'єктивних ознак загроз, пошуку осіб, щодо яких наявні законні підстави для розшуку або ідентифікації, але не може бути самостійною підставою для обмеження свободи пересування, припинення участі у мирному зібранні, затримання чи іншого примусового заходу без індивідуальної оцінки посадовою особою. Алгоритмічний сигнал має бути інформаційним приводом для перевірки, а не замінником правової підстави владного втручання.

Окремо слід передбачити механізм післявоєнного перегляду алгоритмічних практик. Усі системи штучного інтелекту, впроваджені у правоохоронній сфері з мотивів воєнної необхідності, мають пройти ревізію після скасування воєнного стану. Така ревізія повинна оцінювати, чи зберігається потреба у відповідній системі, чи відповідає вона звичайним стандартам прав людини, чи не виходить її використання за первісну мету, чи не накопичено надмірні масиви персональних даних, які підлягають знищенню або деперсоніфікації. Без такого механізму надзвичайні цифрові інструменти мають високий ризик стати постійною інфраструктурою прихованого нагляду.

Узагальнена модель правового режиму застосування ШІ у правоохоронній сфері

Режим застосування	**Приклади систем**	**Основні ризики**	**Необхідні гарантії**
Заборонені практики	Соціальний скоринг; біометрична категоризація за чутливими ознаками; невиправдана масова біометрична ідентифікація в реальному часі	Масове спостереження; дискримінація; стигматизація; порушення свободи зібрань і приватності	Пряма законодавча заборона; Вузько визначені винятки; Судовий або незалежний контроль
Високоризикові системи	Предиктивна поліція; оцінка ризику особи; розпізнавання облич для розшуку; аналіз доказових масивів	Помилкова ідентифікація; непряма дискримінація; «цифрова тінь»; непрозорість рішення	HRIA; аудит; якість даних; логування; людський нагляд; можливість оскарження
Допоміжні системи	Пошук у відкритих джерелах; технічне	Витік даних; помилки	Кібербезпека; службові

Режим застосування	Приклади систем	Основні ризики	Необхідні гарантії
	сортування документів; анонімізована статистика; службові інформаційні помічники	класифікації; несанкціоноване використання	регламенти; мінімізація даних; відповідальна посадова особа

Висновки. Застосування штучного інтелекту у правоохоронній діяльності та сфері охорони громадського порядку є об'єктивним наслідком цифровізації публічної безпеки. Його потенціал полягає у прискоренні аналізу великих масивів даних, підвищенні ефективності розшуку, ідентифікації осіб, прогнозуванні криміногенних ризиків, опрацюванні доказової інформації та раціональнішому розподілі правоохоронних ресурсів. Проте саме у цій сфері штучний інтелект набуває підвищеної правової чутливості, оскільки його результати можуть безпосередньо впливати на свободу, приватність, репутацію, рівність і процесуальний статус людини.

Ключова наукова суперечність полягає у тому, що алгоритмічні інструменти, які підвищують ефективність правоохоронної діяльності, одночасно створюють ризики масового спостереження, дискримінаційного профілювання, помилкової ідентифікації, витоку персональних даних і формування прихованої «цифрової тіні» особи. Тому правове регулювання має бути спрямоване не на абстрактне стимулювання використання штучного інтелекту, а на встановлення чітких меж його допустимості.

Оптимальною для України є диференційована модель регулювання, що поєднує: заборону найбільш небезпечних практик; спеціальний режим високого ризику для систем, які впливають на права людини; полегшений режим для допоміжних технічних інструментів. У правоохоронній сфері обов'язковими мають стати людський нагляд, оцінка впливу на права людини, якість і репрезентативність даних, зовнішній аудит, логування алгоритмічних дій, прозорість настільки, наскільки це сумісно з оперативною таємницею, та можливість судового контролю.

В умовах воєнного стану використання штучного інтелекту правоохоронними органами може бути ширшим, ніж у звичайний період, але воно має залишатися цільовим, пропорційним, строковим і контрольованим. Після завершення воєнного стану всі алгоритмічні практики, впроваджені з мотивів безпеки, повинні пройти ревізію на предмет відповідності стандартам демократичного правопорядку. Без такої ревізії існує ризик перетворення тимчасових безпекових інструментів на постійну інфраструктуру алгоритмічного нагляду.

Отже, штучний інтелект у правоохоронній сфері має розглядатися не як самостійний суб'єкт владного рішення, а як контрольований технологічний інструмент, підпорядкований принципам законності, пропорційності, недискримінації, захисту персональних даних, людського контролю та судового захисту.

Список використаних джерел

1. Rigano C. Using Artificial Intelligence to Address Criminal Justice Needs. National Institute of Justice. URL: https://www.ojp.gov/pdffiles1/nij/252038.pdf
2. Brynjolfsson E., McAfee A. The Business of Artificial Intelligence. Harvard Business Review. 2017. URL: https://starlab-alliance.com/wp-content/uploads/2017/09/AI-Article.pdf

3. Пядишев В.Г. Перспективи розвитку проактивної діяльності поліції: зарубіжний погляд. Право і суспільство. 2024. № 1. Т. 2. С. 403–412.
4. Зачек О.І., Дмитрик Ю.І., Сеник В.В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності. Вісник Львівського державного університету внутрішніх справ. 2023. № 3. С. 148–156. URL: http://journals.lvduvs.lviv.ua/index.php/law/article/view/637/628
5. How Police Force Uses Data to Assess Risk and Predict Crime. Financial Times. 2 July 2018. URL: https://www.ft.com/content/81af2e14-7fb9-11e8-bc55-50daf11b720d
6. Dejaview: A Crime Prevention Technology from South Korea. iConext. 27 Jan. 2025. URL: https://iconext.co.th/2025/01/27/dejaview-a-technology-for-crime-prevention/
7. Söze - minimizing risks and improving outcomes in police investigations. Akkodis. URL: https://www.akkodis.com/en/tech-practices/ai-solutions-data-analytics/soze-solution-platform
8. Vaughan H. AI Tool That Can Do '81 Years of Detective Work in 30 Hours' Trialled by Police. Sky News. 24 Sept. 2024. URL: https://news.sky.com/story/ai-tool-that-can-do-81-years-of-detective-work-in-30-hours-trialled-by-police-13220891
9. Angwin J., Larson J., Mattu S., Kirchner L. Machine Bias: There's Software Used across the Country to Predict Future Criminals. And It's Biased against Blacks. ProPublica. 23 May 2016. URL: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing
10. Flores A.W., Bechtel K., Lowenkamp C.T. False Positives, False Negatives, and False Analyses: A Rejoinder to 'Machine Bias'. Federal Probation. 2016. Vol. 80. No. 2. P. 38–46. URL: https://www.uscourts.gov/sites/default/files/80_2_6_0.pdf
11. Washington A.L. How to Argue with an Algorithm: Lessons from the COMPAS–ProPublica Debate. Colorado Technology Law Journal. 2019. Vol. 17. No. 1. P. 131–160. URL: https://ctlj.colorado.edu/wp-content/uploads/2021/02/17.1_4-Washington_3.18.19.pdf
12. S. and Marper v. the United Kingdom, nos. 30562/04 and 30566/04, European Court of Human Rights, 4 Dec. 2008. URL: https://hudoc.echr.coe.int/
13. Big Brother Watch and Others v. the United Kingdom, nos. 58170/13, 62322/14 and 24960/15, European Court of Human Rights, 25 May 2021. URL: https://hudoc.echr.coe.int/
14. Roman Zakharov v. Russia, no. 47143/06, European Court of Human Rights, 4 Dec. 2015. URL: https://hudoc.echr.coe.int/
15. Glukhin v. Russia, no. 11519/20, European Court of Human Rights, 4 July 2023. URL: https://hudoc.echr.coe.int/
16. European Union. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). Official Journal of the European Union. L 2024/1689. 12 July 2024. P. 1–144. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj
17. Clearview AI. Війна в Україні. URL: https://www.clearview.ai/ukraine
18. Ukrainian Officials Now Using Facial Recognition Tech to ID Russian Soldiers. NBC News / Clearview AI – As Seen on TV. URL: https://www.clearview.ai/as-seen-on-tv/ukrainian-officials-now-using-facial-recognition-tech-to-id-russian-soldiers
19. Johnson K. Face Recognition Software Led to His Arrest. It Was Dead Wrong. Wired. 28 Feb. 2023. URL: https://www.wired.com/story/face-recognition-software-led-to-his-arrest-it-was-dead-wrong/
20. Simmler M., Canova G. Facial Recognition Technology in Law Enforcement: Regulating Data Analysis of Another Kind. Computer Law & Security Review. 2024. URL: https://www.sciencedirect.com/science/article/pii/S0267364924001572

21. Ліманте А., Москвитин Ю. Технологія розпізнавання обличчя: ризики застосування у воєнний час. Юридична газета. 13 вересня 2024. URL: https://yur-gazeta.com/dumka-eksperta/tehnologiya-rozpiznavannya-oblichchya-riziki-zastosuvannya-u-voenniy-chas.html
22. Amnesty International закликає заборонити використання технологій розпізнавання облич для масового стеження. Amnesty International в Україні. URL: https://www.amnesty.org.ua/amnesty-international-zaklykaye-zaboronyty-vykorystannya-tehnologij-rozpiznavannya-oblych-dlya-masovogo-stezhennya/
23. Система розпізнавання обличчя: правові аспекти використання в Україні та в ЄС. Українська Гельсінська спілка з прав людини. URL: https://www.helsinki.org.ua/articles/systema-rozpiznavannia-oblychchia-pravovi-aspekty-vykorystannia-v-ukraini-ta-v-yes/
24. Martin K.D., Zimmermann J. Artificial Intelligence and Its Implications for Data Privacy. Journal of Responsible Technology. 2024. Vol. 19. URL: https://www.sciencedirect.com/science/article/abs/pii/S2352250X24000423