DOI: 10.34015/2523-4552.2026.1.22
УДК 34:004.8:351.74

Варинський В. О.,
кандидат політичних наук, доцент,
доцент кафедри філософії та україністики
Національного університету «Одеська
морська академія»
ORCID: https://orcid.org/0000-0001-5837-6201

ЕТИЧНІ ТА ПРАВОВІ РИЗИКИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ ТА ДІЯЛЬНОСТІ СПЕЦСЛУЖБ

У статті досліджено основні практики застосування штучного інтелекту (ШІ) у правоохоронній діяльності та діяльності спецслужб і визначено ключові етичні та правові ризики, що виникають унаслідок використання предикативних моделей, аналітики великих даних (Big Data) і біометричних технологій. Показано, що ШІ здатен підвищувати оперативність превенції та розслідування правопорушень завдяки інтеграції розрізнених інформаційних ресурсів, швидкому опрацюванню значних масивів даних, підтримці оперативно-службових рішень і частковій автоматизації рутинних процедур досудового розслідування. Водночас встановлено, що робота з Big Data може відтворювати й посилювати упередження, закладені у даних та практиках їх збирання, формуючи дискримінаційні ефекти й алгоритмічне профілювання груп, а також створюючи ризики непропорційного втручання в приватність. Особливо гостро ці загрози проявляються у практиках прогнозування зон підвищеного ризику, пріоритизації ресурсів і застосуванні розпізнавання облич у публічному просторі, де технологічна «точність» сама по собі не гарантує правомірності та справедливості. Наголошено, що статистичні закономірності й прогнозні оцінки не можуть підміняти юридичну оцінку, доказові стандарти та індивідуалізацію рішень; результати роботи ШІ мають бути допоміжними, а відповідальність за рішення та втручання у права людини — залишатися за уповноваженим суб'єктом правозастосування за наявності належних процедурних гарантій і можливості оскарження. Зроблено висновок, що допустиме використання ШІ у правоохоронній діяльності та діяльності спецслужб можливе лише за умов чітких меж застосування, дієвого контролю та механізмів оскарження, а також збереження пріоритету людської гідності та верховенства права.

Ключові слова*: правоохоронна діяльність; штучний інтелект (ШІ); етичні та правові ризики; права людини.*

Постановка проблеми. Стрімке впровадження систем штучного інтелекту (далі — ШІ) у сфері безпеки та правопорядку трансформує способи здійснення правоохоронної й спеціальної діяльності: від аналізу великих масивів даних (Big Data) і підтримки оперативно-службових рішень до біометричної ідентифікації, прогнозування ризиків та автоматизації окремих процедур досудового розслідування. Разом із потенціалом підвищення ефективності такі технології створюють якісно нові правові та етичні виклики, оскільки застосовуються у найбільш чутливих контекстах, де будь-яка помилка або упередженість може призводити до непропорційного втручання в права людини.

Проблемність використання ШІ у правоохоронній діяльності полягає в тому, що алгоритмічні рішення нерідко мають опосередкований характер: вони не лише обробляють інформацію, а фактично формують підстави для вибору тактики, пріоритизації ресурсів, визначення зон підвищеної уваги, а інколи — впливають на оцінку особи та її процесуальний статус. За відсутності належних запобіжників це породжує ризики алгоритмічної упередженості, непрямої дискримінації, масового нагляду, порушення принципів законності, необхідності та пропорційності, а також зниження ролі людини до пасивного виконавця алгоритмічних висновків, що несумісно з логікою правопорядку, заснованого на верховенстві права. Особливо гостро ці загрози проявляються у випадках застосування біометричних технологій (зокрема розпізнавання облич) у публічному просторі та при побудові прогнозних моделей злочинності, де статистичні закономірності можуть перетворюватися на механізми стигматизації цілих груп.

Актуальність дослідження додатково посилюється воєнним контекстом і зростанням навантаження на систему кримінальної юстиції, що підвищує попит на технологічні інструменти швидкого аналізу інформації та ідентифікації осіб. Водночас саме в умовах кризи зростає ризик некритичного застосування технологій та нормалізації практик, які в мирний час були б очевидно неприйнятними.

Зазначене зумовлює наукову й практичну потребу в окресленні ключових ризиків застосування ШІ у правоохоронній діяльності та діяльності спецслужб і визначенні критеріїв їх мінімізації, що поєднували б інтереси безпеки з гарантіями прав і свобод людини.

Аналіз останніх досліджень і публікацій. Застосування технологій ШІ у сфері безпеки й правопорядку в сучасних фахових та медійних публікаціях осмислюється у двох взаємопов’язаних площинах: практичної доцільності та ефективності, з одного боку, і правової регулятивності – з іншого. Зокрема, розглядається потенціал ШІ щодо інтеграції розрізнених баз, пришвидшення обробки інформації та підтримки управлінських рішень, спрямованих на превенцію правопорушень. Ці підходи ілюструються матеріали *Financial Times* про поліцейську аналітику та практику *Met Police*. Водночас аналізуються нормативні межі допустимості таких підходів (М. Карчевський, О. Зачек, Ю. Дмитрик, В. Сеник, В. Пядишев та ін.).

Дискурс ризиків для прав людини, пов'язаних із використанням ШІ у правоохоронному контексті, охоплює питання конфіденційності, масового нагляду та захисту персональних даних, передусім у вимірі дотримання вимог приватності (privacy compliance) (Veritone, GIP Digital Watch, IBM Think), а також академічні підходи до екосистемних ризиків обробки даних, включно з деанонімізацією (K. Martin і J. Zimmermann). Таким чином, у наявних джерелах наскрізною є теза про необхідність поєднання технологічної ефективності ШІ з жорсткими правовими гарантіями підзвітності, пропорційності та недискримінації у найбільш чутливих практиках правоохоронної й спеціальної діяльності.

Постановка задання. Метою статті є окреслення основних практик застосування ШІ у право охоронній діяльності та діяльності спецслужб і визначення ключових етичних і правових ризиків, що виникають унаслідок використання предиктивних моделей, аналітики великих даних (Big Data) і біометричних технологій.

Виклад основного матеріалу. ШІ суттєво вплинув на розвиток різних галузей, зокрема сфери правоохоронної діяльності, запропонувавши нові інструменти та можливості для підвищення рівня суспільної безпеки. Хоча ШІ має величезний потенціал для підвищення ефективності превенції, виявлення та розслідування злочинів, його застосування супроводжується істотними етичними та юридичними викликами. У цій статті аналізуються перспективи та ризики, пов'язані з інтеграцією ШІ у правоохоронну діяльність.

Розслідування злочинів традиційно спиралося на людську інтуїцію, дедуктивні міркування та дослідницькі навички. Проте з упровадженням ШІ у процеси виявлення та розслідування правопорушень відбуваються якісні зміни. Системи ШІ здатні посилювати інформаційно-аналітичну підтримку досудового розслідування, зокрема через розширений аналіз даних, підтримку оцінювання ризиків і оптимізацію процесів розслідування.

Однією із суттєвих переваг застосування ШІ під час досудового розслідування є його здатність швидко та точно аналізувати величезні обсяги даних. Алгоритми ШІ можуть аналізувати значні масиви інформації, у тому числі звіти про злочини, записи камер спостереження та фінансові дані, щоб виявити закономірності та зв'язки, які людина може залишити поза увагою. Такі можливості здатні суттєво допомогти слідчим (детективам) у розкритті складних справ, ідентифікації ключових підозрюваних та встановленні прихованих зв'язків між, на перший погляд, непов'язаними інцидентами.

ШІ може використовуватися для прогнозування ризиків правопорушень, опрацьовуючи масиви дані та виявляючи закономірності, які часто передують вчиненню правопорушень. Ураховуючи такі фактори, як час, місце та соціально-демографічні характеристики (за умови законності та обґрунтованості їх використання), алгоритми ШІ можуть формувати прогнозні оцінки щодо потенційних зон підвищеного ризику та допомогти право охоронним органам раціональніше розподіляти ресурси. Такий превентив-

ний підхід потенційно сприяє зниженню рівня злочинності та підвищенню суспільної безпеки.

Крім того, інструменти ШІ дають змогу частково автоматизувати рутинні та трудомісткі процедури досудового розслідування. Наприклад, алгоритми розпізнавання облич можуть порівнювати зображення можливих підозрюваних із наявними базами даних, зменшуючи часові витрати слідчих на первинну ідентифікацію. Аналогічно, інструменти на базі ШІ можуть швидко аналізувати телефонні з'єднання або фінансові операції, допомагаючи виявляти підозрілі зв'язки та точніше встановлювати часову послідовність подій.

Опрацювання великого обсягу актуальних зображень і відеозаписів точно та в стислі строки є трудомістким і кропітким завданням, де зростає ризик людської помилки через втому та інші людські чинники. На відміну від людини, алгоритмічні системи не знають втоми, що робить їх потенційно корисними для масштабного аналізу мультимедійних даних.Наприклад, у межах ініціатив на кшталт «Intelligence Advanced Research» [1], включно з проєктами комп'ютерного зору (наприклад, «Janus Activity»), проводяться випробування алгоритмів, які можуть навчитися ідентифікувати одну людину від іншої, використовуючи риси обличчя, за принципом, подібним до роботи людського аналітика [2].

Окремі приклади аналітичних платформ на базі ШІ застосовуються в практиці поліції. Так, за наведеними джерелами, у підрозділах поліції Великої Британії використовується Qlik Sense - програмне забезпечення, розроблене Qlik Technologies [3], яке забезпечує інтеграцію понад 10 раніше розрізнених баз даних, включно із журналом усіх екстрених викликів, реєстрами зареєстрованих злочинів, даними про судимості, відомостями про предмети/техніку, пов'язаними із злочинами тощо. Повідомляється, що така система застосовується на рівні патрульних підрозділів, може використовуватися як складова первинного реагування та перевірки відомостей на місці події, а також підтримує ухвалення превентивних рішень щодо запобігання правопорушень. За даними джерела, у 2024 році лондонська поліція розгорнула понад 117 точок застосування цієї технології [4], що позиціонується як підтвердження її результативності.

У Південній Кореї застосовується система розпізнавання облич Dejaview [5], розроблена ETRI, яка здійснює не лише моніторинг у реальному часі, а й аналізує докримінальні ситуації та може сприяти запобіганню окремих правопорушень [6]. Ця система використовує машинне навчання для дослідження ситуативних патернів і виявлення ознак потенційних злочинів, враховуючи такі фактори, як час доби, місце події та історію інцидентів [7].

Однією з найвідоміших технологій ШІ у сфері ідентифікації осіб (розпізнавання облич) у правоохоронній практиці є Clearview AI [8] - американська система з розпізнавання облич, яка використовується, зокрема, правоохоронними органами.

Зазначена технологія позиціонується як інструмент підтримки розкриття злочинів у США [8] і дозволяє правоохоронним органам за фотографією особи перевіряти на-

явність збігів у базі даних, формувати посилання на відповідні зображення в мережі Інтернет та водночас опрацьовувати значні масиви фото- і відеоданих, в тому числі кадри вебкамер. Технологія також застосовувалася для розшуку жертв злочинів [9]. Водночас твердження про «лише кілька» випадків помилкової ідентифікації потребують критичної оцінки з огляду на обмеженість публічних даних, різницю методик обліку та можливу нерепрезентативність відомих випадків. У публічних джерелах повідомлялось про поодинокі випадки помилкової ідентифікації за допомогою розпізнавання обличчя Clearview Al [10], і, як стверджують розробники, такі помилки пов'язані переважно з якістю аналізованих світлин [8], а не з якістю роботи технології.

У березні 2022 року компанія Clearview Al надала Україні доступ до своєї технології для підтримки оборони від російського нападу. Спочатку доступ було надано Міністерству оборони України, а згодом до проєкту приєдналися й інші відомства, зокрема Національна поліція України [11] для ідентифікації осіб, пов’язаних з агресією та виявлення колаборантів. За наведеними даними, станом на 2023 рік завдяки технології було опрацьовано понад 30 млрд фотографій із соцмереж та інформаційних стрічок [12, с. 151], а її використання в окремих джерелах оцінюється як результативне [13]. Повідомляється, що технологія застосовується для перевірки осіб на блокпостах, ідентифікації загиблих військовослужбовців і військовополонених, а також пошуку зниклих безвісти. Водночас застосування технологій розпізнавання облич у воєнному контексті має відбуватися з дотрманням вимог законності, необхідності та пропорційності, а також процесуальних гарантій, зокрема під час розслідування воєнних злочинів.

Отже, потенціал використання ШІ у правоохоронній діяльності є значним: за його допомогою правоохоронні органи можуть здійснювати ідентифікацію та аналітичну підтримку в стислі строки завдяки обробці великих масивів даних (Big Data) з веб-камер, соціальних мереж, сайтів, блогів, форумів та інших джерел. Крім того, ШІ може також застосовуватися для оцінювання надійності (довіри) до окремих джерел інформації – за умови визначених і прозорих критеріїв та обов’язкової верифікації людиною. Водночас ризик порушення прав людини з використанням ШІ суттєво зростає, адже, працюючи з великими масивами даних, ШІ самостійно формує закономірності та прогнозні оцінки, зокрема у сфері криміногенної активності, а в окремих конфігураціях – і для виявлення корупційних ризиків. За відсутності належних запобіжників (якість даних, контроль упереджень, підзвітність і можливість оскарження) це може посилювати дискримінаційні практики через непряме «профілювання» за формально об’єктивними ознаками (місце проживання, соціально-демографічні характеристики, типові маршрути тощо) в різних регіонах.

Відомі випадки алгоритмічної дискримінації, пов’язані з машинною обробкою даних і ризик-стратифікацією груп населення. Зокрема, використання алгоритмічних інструментів оцінювання ризику (небезпеки особи) у деяких штатах

США призводило до дискримінаційних наслідків щодо афроамериканців, які не мали попереднього кримінального досвіду: алгоритм оцінював їх як "більш ризикових/небезпечних", ніж білих правопорушників, які мали суттєвий попередній кримінальний досвід [14], хоча за фактичними обставинами окремі з них могли становити більший реальний ризик [15]. Цей приклад демонструє, що "об'єктивність" автоматизованих оцінок може бути уявною: результати залежать від якості даних, обраних змінних та припущень, закладених у модель.

Також ШІ може використовуватися для аналітичного прогнозування злочинності шляхом опрацювання данх і виявлення закономірностей, які часто передують злочинній діяльності. Однак застосування таких інструментів допустиме лише за наявності чіткої правової підстави та визначеної легітимної мети, із дотриманням вимог законності, необхідності й пропорційності, а також за умови мінімізації даних і недопущення втручання в приватність. Ураховуючи такі фактори, як час, місцезнаходження та соціально-демографічні характеристики (лише настільки, наскільки це обґрунтовано метою та не створює дискримінаційного ефекту), алгоритми ШІ можуть формувати прогнозні оцінки щодо потенційних зон підвищеного ризику та допомагати правоохоронним органам раціональніше розподіляти ресурси. Водночас такий підхід може мати подвійний ефект: поряд з потенційним зниженням рівня правопорушень і підвищенням суспільної безпеки він здатен посилювати профілювання та непряму дискримінацію, якщо моделі навчаються на упереджених даних або застосовуються без належного людського контролю, прозорості критеріїв і можливості оскарження.

Системи ШІ, здатні формувати оцінки щодо локальних «сплесків» злочинності, можуть бути корисними для планування розподілу ресурсів, формування кадрового і фахового складу, залучення необхідних фахівців, вибору систем захисту та спеціальних засобів тощо. Разом з тим рішення, що ґрунтуються на таких оцінках, мають залишатися підконтрольними людині та підлягати перевірці й процедурі оскарження, аби мінімізувати ризики порушення прав людини.

Інтелектуальні алгоритми можуть аналізувати величезні обсяги даних, виявляючи закономірності та тенденції, які можуть підтримувати дії правоохоронних органів, визначати потенційні осередки злочинності та групи, що перебувають у зоні ризику, а також виокремлювати типи правопорушень, що найчастіше трапляються у певних локаціях або сферах. Більше того, «предиктивна поліцейська діяльність» (predictive policing) – один із найбільш дискусійних прикладних напрямів ШІ у правоохоронній діяльності – використовує можливості аналізу даних для прогнозування ймовірності злочинних подій у певних місцях/періодах, а не «злочинів до того, як вони відбудуться» у буквальному розумінні.

Як зазначає В. Г. Пядишев, «на відміну від традиційних методів, штучний інтелект пропонує динамічний підхід до розкриття злочинів, використовуючи можливості аналізу даних, машинного навчання та розпізнавання образів. Здатність систем

штучного інтелекту швидко обробляти величезні обсяги інформації дозволяє правоохоронним органам виявляти закономірності, виявляти потенційних підозрюваних та активно запобігати злочинам» [16, с. 409]. Такі заходи можуть допомогти правоохоронним органам стати більш ефективними, зосередивши свої ресурси там, де вони найбільше потрібні.

Виклики, з якими стикається українська правоохоронна та судова системи у воєнний час, зокрема «блокування чи ускладнення роботи установ на деокупованих та прифронтових територіях, нестача кадрів, велика кількість справ та ін.», підвищують об'єктивну потребу технологічної підтримки та звернення до інструментів ШІ у сфері кримінальної юстиції в Україні, однак через підвищені ризики для прав людини, вимоги до процесуальних гарантій та наслідки помилок для свободи та гідності особи її водночас «називають найменш перспективною для імплементації ШІ» [17].

Л. Еліот, з метою оцінювання ступеня залученості ШІ в правничу діяльність, запропонував таку класифікацію [18] рівнів автоматизації правозастосовчої діяльності:

- рівень 0 – рівень, на якому автоматизація повністю відсутня;

- рівень 1 – рівень, за якого наявна базова автоматизація (використання електронного документообігу, онлайн-сервісів нормативної інформації);

- рівень 2 – рівень, на якому необхідна «розширена автоматизація»: використання систем машинного навчання для класифікації даних щодо юридичної практики, інтелектуалізований пошук у юридичних базах даних із застосуванням методів обробки природної мови;

- рівень 3 – застосування напівавтономних систем, у тому числі експертних систем підтримки ухвалення рішень/формулювання висновків для конкретних справ;

- рівень 4 – рівень галузевої автономності, де можуть ухвалюватися повністю автономні рішення для окремих сегментів юридичної практики (наприклад, частково автономний нотаріат, автономний адміністративний документообіг);

- рівень 5 –висока автономність, за якої правозастосовча діяльність може функціонувати переважно автономною на основі систем «сильного» ШІ, які моделюють людський інтелект;

- рівень 6 – гіпотетична повна автономність на основі штучного інтелекту, який перевищує інтелект людини [18].

У правоохоронній діяльності така шкала особливо показова, адже зі зростанням рівня автоматизації зростають і ризики для прав людини та вимоги до контролю.

Інтеграція ШІ в оперативно-службову та слідчу (розшукову) діяльність не позбавлена проблем як конфіденційності, так і ризиків упередженості й порушення принципу пропорційності. Водночас використання ШІ в такій діяльності має значний потенціал: здатність ШІ аналізувати величезні обсяги даних, формувати прогнозні оцінки щодо осередків злочинності та частково автоматизувати рутинні завдання досудового розслідування може значно підвищити ефективність роботи правоохоронних органів. За таких умов визначальними є етичні міркування, процесуальні гарантії та

принципи відповідального впровадження ШІ, які мають забезпечувати правомірність застосування і дотримання прав людини, а також суспільних цінностей.

Узагальнюючи викладене, можна констатувати, що розглянуті практики застосування ШІ у сфері безпеки й правопорядку демонструють подвійний ефект таких технологій: з одного боку, вони істотно підсилюють аналітичні можливості правоохоронних органів (інтеграція баз, обробка великих масивів даних, часткова автоматизація окремих процедур, прогнозування ризиків), а з іншого — створюють підвищені ризики для прав людини у випадках, коли алгоритмічні результати стають фактичною підставою для управлінських або процесуальних рішень без належної перевірки, контролю та можливості оскарження. Саме тому використання таких інструментів потребує чітко визначених меж допустимості та процедурних запобіжників, які зберігають пріоритет людської відповідальності у правозастосуванні.

Висновки. Штучний інтелект уже став важливою складовою сучасної правоохоронної та спеціальної діяльності, насамперед як інструмент аналітики великих даних, підтримки оперативно-службових рішень, прогнозування ризиків і біометричної ідентифікації. Його застосування здатне підвищувати швидкість і результативність розслідувань та превентивної діяльності, однак водночас створює підвищену небезпеку для прав людини у найбільш чутливих контекстах правозастосування. Зокрема залишаються актуальними ключові ризики пов’язані з тим, що алгоритмічні моделі, працюючи з великими масивами даних, можуть відтворювати та посилювати упередження, формуючи дискримінаційні ефекти й профілювання окремих груп. У поєднанні з біометричними технологіями (зокрема розпізнаванням облич) це здатне трансформуватися у практики масового нагляду та непропорційного втручання в приватність, особливо за відсутності чітких меж застосування, процедурного контролю та реальної можливості оскарження.

Проведений аналіз засвідчує, що окрему загрозу становить зміщення ролі людини у бік пасивного виконавця «алгоритмічних результатів». У правоохоронній сфері це є критичним, адже статистичні закономірності та прогнозні оцінки не можуть автоматично підміняти юридичну оцінку, доказові стандарти й індивідуалізацію рішень. Тому результати роботи ШІ мають розглядатися як допоміжні, а відповідальність за втручання в права людини повинна залишатися за уповноваженим суб’єктом правозастосування.

Отже, подальше впровадження ШІ у сфері безпеки й правопорядку потребує фокусування не лише на технологічній ефективності, а й на забезпеченні правових та етичних запобіжників, які мінімізують ризики дискримінації, непропорційного нагляду та автоматизації правозастосування всупереч вимогам верховенства права.

Список використаних джерел

1. About IARPA. Intelligence Advanced Research Projects Activity (IARPA). URL: https://www.iarpa.gov/who-we-are/about-us (дата звернення: 20.02.2026).

2. Brynjolfsson, E. and Mcafee, A. (2017) The Business of Artificial Intelligence. Harvard Business Review, 7, 3-11. https://starlab-alliance.com/wp-content/uploads/2017/09/The-Business-of-Artificial-Intelligence.pdf (дата звернення: 20.02.2026).

3. 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 (дата звернення: 20.02.2026).

4. Met Police Use of Facial Recognition in London Surges. *Financial Times*. 2024. URL: https://www.ft.com/content/c33322a7-eba7-4299-8172-4ce1d4e88908 (дата звернення: 20.02.2026).

5. *ETRI, making the first leap towards a real-life "Minority Report" with AI CCTVs: development of "Dejaview" technology.* EurekAlert!, 12 Sept. 2024. URL: https://www.eurekalert.org/news-releases/1057493 (дата звернення: 20.02.2026).

6. Ahmed Z. This AI Claims to Predict Crimes before They Happen Based on Real-Time CCTV Analysis. *TechSpot*. 15 Sept. 2024. URL: https://www.techspot.com/news/104723-ai-claims-predict-crimes-before-they-happen-based.html (дата звернення: 20.02.2026).

7. 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/ (дата звернення: 20.02.2026).

8. Clayton J., Derico B. Clearview AI Used Nearly 1m Times by US Police, It Tells the BBC. *BBC News*. 27 Mar. 2023. URL: https://www.bbc.com/news/technology-65057011 (дата звернення: 20.02.2026).

9. Hill K. What We Learned About Clearview AI and Its Secret "Co-Founder". *The New York Times*. 18 Mar. 2021. URL: https://www.nytimes.com/2021/03/18/technology/clearview-facial-recognition-ai.html (дата звернення: 20.02.2026).

10. Mac R., Hill K. Clearview AI Settles Suit and Agrees to Limit Sales of Facial Recognition Database. *The New York Times*. 9 May 2022. URL: https://www.nytimes.com/2022/05/09/technology/clearview-ai-suit.html (дата звернення: 20.02.2026).

11. Bergengruen V. *Ukraine's 'Secret Weapon' Against Russia Is a Controversial U.S. Tech Company*. *TIME*, 14 Nov. 2023. URL: https://time.com/6334176/ukraine-clearview-ai-russia/ (дата звернення: 20.02.2026).

12. Зачек О.І., Дмитрик Ю.І., Сеник В.В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності. *Науковий вісник Львівського державного університету внутрішніх справ*. 2023. № 3. С. 148–156. DOI: https://doi.org/10.32782/2311-8040/2023-3-19

13. *In Ukraine, Identifying the Dead Comes at a Human Rights Cost.* Wired, 22 Feb. 2023. URL: https://www.wired.com/story/russia-ukraine-facial-recognition-technology-death-military (дата звернення: 21.02.2026).

14. Angwin J. et al. 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 (дата звернення: 21.02.2026).

15. Courtland R. Bias Detectives: The Researchers Striving to Make Algorithms Fair. *Nature*. 2018. Vol. 558, no. 7710. P. 357–360. URL: https://www.nature.com/articles/d41586-018-05469-3 (дата звернення: 21.02.2026).

16. Пядишев В. Г. Перспективи розвитку проактивної діяльності поліції: зарубіжний погляд. Право і суспільство. 2024. № 1, т. 2. С. 403–412. DOI: https://doi.org/10.32842/2078-3736/2024.1.2.61

17. Перспективи та межі використання штучного інтелекту в кримінальному процесі. Україна. Центр Дністрянського / Міжнародний фонд «Відродження». 2024. URL: https://www.irf.ua/wp-content/uploads/2024/02/ai.pdf,

18. Eliot L.B. An Impact Model of AI on the Principles of Justice: Encompassing the Autonomous Levels of AI Legal Reasoning. *arXiv.* 25 Aug. 2020. URL: https://www.academia.edu/44020078/An_Impact_Model_of_AI_on_the_Principles_of_Justice_Encompassing_the_Autonomous_Levels_of_AI_Legal_Reasoning (дата звернення: 21.02.2026).

References

1. Intelligence Advanced Research Projects Activity. (n.d.). *About IARPA*. https://www.iarpa.gov/who-we-are/about-us

2. Brynjolfsson, E., & McAfee, A. (2017). The business of artificial intelligence. *Harvard Business Review*, *7*, 3–11. https://starlab-alliance.com/wp-content/uploads/2017/09/The-Business-of-Artificial-Intelligence.pdf

3. *How police force uses data to assess risk and predict crime*. (2018, July 2). *Financial Times*. https://www.ft.com/content/81af2e14-7fb9-11e8-bc55-50daf11b720d

4. *Met police use of facial recognition in London surges*. (2024). *Financial Times*. https://www.ft.com/content/c33322a7-eba7-4299-8172-4ce1d4e88908

5. Electronics and Telecommunications Research Institute. (2024, September 12). *ETRI making the first leap towards a real-life "Minority Report" with AI CCTVs: Development of "Dejaview" technology*. *EurekAlert!*. https://www.eurekalert.org/news-releases/1057493

6. Ahmed, Z. (2024, September 15). This AI claims to predict crimes before they happen based on real-time CCTV analysis. *TechSpot*. https://www.techspot.com/news/104723-ai-claims-predict-crimes-before-they-happen-based.html

7. *Dejaview: A crime prevention technology from South Korea*. (2025, January 27). *iConext*. https://iconext.co.th/2025/01/27/dejaview-a-technology-for-crime-prevention/

8. Clayton, J., & Derico, B. (2023, March 27). Clearview AI used nearly 1m times by US police, it tells the BBC. *BBC News*. https://www.bbc.com/news/technology-65057011

9. Hill, K. (2021, March 18). What we learned about Clearview AI and its secret "co-founder". *The New York Times*. https://www.nytimes.com/2021/03/18/technology/clearview-facial-recognition-ai.html

10. Mac, R., & Hill, K. (2022, May 9). Clearview AI settles suit and agrees to limit sales of facial recognition database. *The New York Times*. https://www.nytimes.com/2022/05/09/technology/clearview-ai-suit.html

11. Bergengruen, V. (2023, November 14). Ukraine's "secret weapon" against Russia is a controversial U.S. tech company. *TIME*. https://time.com/6334176/ukraine-clearview-ai-russia/

12. Zachek, O. I., Dmytryk, Yu. I., & Senyk, V. V. (2023). Rol shtuchnoho intelektu v pidvyshchenni efektyvnosti pravookhoronnoi diialnosti [The role of artificial intelligence in improving the efficiency of law enforcement activities]. *Naukovyi Visnyk Lvivskoho Derzhavnoho Universytetu Vnutrishnikh Sprav*, *3*, 148–156. https://doi.org/10.32782/2311-8040/2023-3-19

13. *In Ukraine, identifying the dead comes at a human rights cost*. (2023, February 22). *Wired*. https://www.wired.com/story/russia-ukraine-facial-recognition-technology-death-military

14. Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016, May 23). Machine bias: There's software used across the country to predict future criminals—and it's biased against

Blacks. *ProPublica*. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

15. Courtland, R. (2018). Bias detectives: The researchers striving to make algorithms fair. *Nature*, *558*(7710), 357–360. https://www.nature.com/articles/d41586-018-05469-3

16. Piadyshev, V. H. (2024). Perspektyvy rozvytku proaktyvnoi diialnosti politsii: Zarubizhnyi pohliad [Prospects for the development of proactive police activity: A foreign perspective]. *Pravo i Suspilstvo*, *1*(2), 403–412. https://doi.org/10.32842/2078-3736/2024.1.2.61

17. Centre Dnistryanskyi & International Renaissance Foundation. (2024). *Perspektyvy ta mezhi vykorystannia shtuchnoho intelektu v kryminalnomu protsesi* [Prospects and limits of the use of artificial intelligence in criminal proceedings]. https://www.irf.ua/wp-content/uploads/2024/02/ai.pdf

18. Eliot, L. B. (2020, August 25). *An impact model of AI on the principles of justice: Encompassing the autonomous levels of AI legal reasoning*. arXiv. https://www.academia.edu/44020078/An_Impact_Model_of_AI_on_the_Principles_of_Justice_Encompassing_the_Autonomous_Levels_of_AI_Legal_Reasoning

***Varynskyi V. O.**, Candidate of Political Sciences, Associate Professor of the Department of Philosophy, National University «Odesa Maritime Academy»*

ORCID: https://orcid.org/0000-0001-5837-6201

Ethical and Legal Risks of Using Artificial Intelligence in Law Enforcement and Special Services

The article examines the main practices of using artificial intelligence (AI) in law enforcement and special services and identifies key ethical and legal risks arising from the deployment of predictive models, big data (Big Data) analytics, and biometric technologies. It is shown that AI can enhance the operational capacity of prevention and investigation by integrating fragmented information resources, rapidly processing large datasets, supporting operational decision-making, and partially automating routine pre-trial investigative procedures. At the same time, it is established that working with Big Data may reproduce and amplify biases embedded in the data and in data-collection practices, producing discriminatory effects and algorithmic profiling of groups, as well as creating risks of disproportionate interference with privacy. These threats are particularly acute in practices of forecasting high-risk areas, prioritizing resources, and deploying facial recognition in public spaces, where technological “accuracy” alone does not ensure legality or fairness. The article emphasizes that statistical patterns and predictive assessments cannot replace legal evaluation, evidentiary standards, or individualized decision-making; AI outputs must remain auxiliary, while responsibility for decisions and interferences with human rights should rest with an authorized law-enforcement actor, provided that adequate procedural safeguards and avenues for appeal are available. The article concludes that permissible use of AI in law enforcement and special services is possible only under clearly defined limits of deployment, effective oversight and redress mechanisms, and the preservation of the primacy of human dignity and the rule of law.

Key words: *law enforcement; artificial intelligence (AI); ethical and legal risks; human rights.*

Цитування за ДСТУ 8302:2015: **Варинський В. О. Етичні та правові ризики застосування штучного інтелекту у правоохоронній діяльності та діяльності спецслужб.** *Вісник Пенітенціарної асоціації України*. 2026. № 1(35). С. 245-256. DOI: https://doi.org/10.34015/2523-4552.2026.1.22

Citation APA: Varynskyi, V. O. (2026). Etychni ta pravovi ryzyky zastosuvannia shtuchnoho intelektu u pravookhoronnii diialnosti ta diialnosti spetssluzhb [Ethical and legal risks of using artificial intelligence in law enforcement and special services]. *Bulletin of the Penitentiary association of Ukraine*, *1(35)*, 245-256. https://doi.org/10.34015/2523-4552.2026.1.22

Внесок автора. Автор самостійно здійснив концептуалізацію дослідження, аналіз джерел, підготовку тексту статті та формулювання висновків. Автор ознайомився з остаточною версією рукопису, схвалив її та погодився з поданням статті до публікації.
Академічна доброчесність. Автор підтверджує оригінальність, точність і достовірність тексту статті та наведених у ній результатів, а також дотримання принципів академічної доброчесності.
Використання інструментів штучного інтелекту. Автор засвідчує, що під час підготовки цієї статті інструменти штучного інтелекту не використовувалися.
Конфлікт інтересів. Автор заявляє про відсутність реального чи потенційного конфлікту інтересів.
Фінансування. Дослідження виконано в межах наукової діяльності автора у відповідних установах і не мало окремого зовнішнього фінансування.

Author Contribution. The author independently conceptualized the study, analyzed the sources, prepared the text of the article, and formulated the conclusions. The author reviewed the final version of the manuscript, approved it, and agreed to submit the article for publication.
Academic Integrity Statement. The author confirms the originality, accuracy, and reliability of the text of the article and the results presented therein, as well as compliance with the principles of academic integrity.
Use of Artificial Intelligence Tools. The author certifies that no artificial intelligence tools were used in the preparation of this article.
Conflict of Interest. The author declares that there is no actual or potential conflict of interest.
Funding. The research was conducted within the framework of the author's academic activities at the relevant institutions and did not receive special external funding.

Надійшла: 27.02.2026 Received: 27 February 2026
Прийнята до друку: 30.03.2026 Accepted for publication: 30 March 2026
Опублікована: 30.04.2026 Published: 30 April 2026