

УДК 343.98:004.8

DOI <https://doi.org/10.24144/2307-3322.2025.90.4.41>

АЛГОРИТМІЧНІ СИСТЕМИ І ПРЕЗУМПЦІЯ НЕВИНУВАТОСТІ: ПРАВОВИЙ АНАЛІЗ УПЕРЕДЖЕНЬ ТА МЕХАНІЗМІВ ЗАХИСТУ

Крикніцький Я.І.,

аспірант кафедри кримінального процесу та криміналістики

Навчально-наукового інституту права,

Київський національний університет

імені Тараса Шевченка

ORCID: 0009-0008-3745-8142

e-mail: slawik9122000@gmail.com

Крикніцький Я.І. Алгоритмічні системи і презумпція невинуватості: правовий аналіз упереджень та механізмів захисту.

У статті розглядається вплив сучасних технологій штучного інтелекту на фундаментальне право особи бути визнаною невинуватою до набрання вироком суду законної сили. В результаті проведеного аналізу встановлено, як автоматизоване розпізнавання обличчя, алгоритмічні інструменти оцінки ризику рецидиву та системи прогнозного поліцейського профілювання можуть породжувати упередження внаслідок некоректної вибірки даних, непрозорих алгоритмічних припущень та недосконалої методології моделювання. Встановлено, що застосування таких технологій без належного контролю загрожує зміщенням тягаря доказування й порушенням принципу «in dubio pro geo», закріпленого в ст. 6 Європейської конвенції з прав людини. У роботі проаналізовано Директиву (EU) 2016/343 та Regulation (EU) 2024/1689 (AI Act), що встановлює мінімальні стандарти кримінального судочинства, вимоги прозорості та відповідальності алгоритмічних систем, а також європейські резолюції й рекомендації організацій Fair Trials та Amnesty International щодо забезпечення доступу захисту до вихідного коду й результатів аудиту алгоритмів. На основі виявлених ризиків обґрунтовано необхідність запровадження інструментів пояснюваності (explainability), створення незалежних органів аудиту ІІІ та законодавчих обмежень на автономне застосування високоризикових технологій без участі людини. Також наголошено на потребі професійного навчання суддів, прокурорів і адвокатів у сфері застосування штучного інтелекту та алгоритмічної справедливості, а також на гарантуванні захисту права підозрюваного на ознайомлення з експертними висновками щодо роботи алгоритмічних систем, що слугують доказами. Встановлено необхідність законодавчого закріплення права сторони захисту на доступ до технічної документації алгоритму (включно з описом джерел навчальних даних, методів валідації і результатів незалежних аудитів) з урахуванням режимів захисту комерційної таємниці. Проаналізовано важливість передбачення механізмів конфіденційного ознайомлення в суді та фінансування експертних перевірок за рахунок держави у випадку, коли особа не може самостійно забезпечити таку перевірку. Обґрунтовано доцільність встановлення процесуальної заборони на використання повністю автономних рішень у питаннях, що безпосередньо обмежують свободу особи (наприклад, підстави для арешту або продовження запобіжного заходу) – у таких випадках рішення повинно ухвалюватися людиною з обов'язковим врахуванням наданого алгоритмом пояснення та з фіксацією підстав для відхилення або прийняття його висновків. Рекомендовано запровадити на національному рівні наглядові та сертифікаційні процедури для алгоритмів високого ризику, включно з періодичними незалежними аудитами й публічними звітами про їхню ефективність та виявлені упередження. У контексті транснаціональних електронних доказів акцентовано на доцільності врахування практики проєктів SIRIUS і TREIO при гармонізації правил доступу до даних і співпраці з іноземними юрисдикціями, щоб не допустити, аби алгоритмічні докази, отримані з-за кордону, уникали належної перевірки.

Ключові слова: досудове розслідування, гарантії та захист прав особи, алгоритмічні системи, презумпція невинуватості, кримінальне провадження, підозра, обвинувачення, захист, упередження, ІІІ.

Kryknitskyi Y.I. Algorithmic systems and the presumption of innocence: legal analysis of biases and protection mechanisms.

The article examines the impact of modern artificial intelligence technologies on the fundamental right of an individual to be presumed innocent until a court judgment becomes final and legally binding. The analysis establishes how automated facial recognition, algorithmic risk-assessment tools for recidivism, and predictive policing systems can introduce bias due to flawed data sampling, opaque algorithmic assumptions, and imperfect modeling methodologies. It finds that deploying these technologies without adequate oversight threatens to shift the burden of proof and to violate the “in dubio pro reo” principle enshrined in Article 6 of the European Convention on Human Rights. The study analyzes Directive (EU) 2016/343 and Regulation (EU) 2024/1689 (the AI Act), which establish minimum standards for criminal proceedings and set requirements for the transparency and accountability of algorithmic systems, and it reviews European Parliament resolutions and recommendations from Fair Trials and Amnesty International concerning defense access to source code and algorithmic audit results. Based on the identified risks, the article argues for the introduction of explainability mechanisms, the creation of independent AI audit bodies, and legislative restrictions on the autonomous use of high-risk technologies without human involvement. It also emphasizes the need for specialized training of judges, prosecutors, and defense attorneys in artificial intelligence and algorithmic fairness, as well as for guaranteeing the accused’s right to review expert assessments of the algorithmic tools used as evidence. It is established that the defense should have a statutory right to access the technical documentation of an algorithm (including descriptions of the sources of training data, validation methods, and the results of independent audits), while duly taking into account regimes for protecting trade secrets. The importance of providing mechanisms for confidential in-court review and of state-funded expert examinations where an individual cannot secure such review independently is analyzed. The advisability of imposing a procedural prohibition on the use of fully autonomous decisions in matters that directly restrict an individual’s liberty (for example, grounds for arrest or for extending a preventive measure) is substantiated – in such cases, the decision must be made by a human decision-maker who is required to consider the explanation provided by the algorithm and to record the reasons for accepting or rejecting its conclusions. It is recommended to introduce, at the national level, supervisory and certification procedures for high-risk algorithms, including periodic independent audits and public reports on their effectiveness and on any biases detected. In the context of transnational electronic evidence, emphasis is placed on the need to take into account the practices of the SIRIUS and TREIO projects when harmonizing rules on data access and cooperation with foreign jurisdictions, in order to prevent algorithmic evidence obtained abroad from evading proper scrutiny.

Key words: pre-trial investigation, guarantees and protection of individual rights, algorithmic systems, presumption of innocence, criminal proceedings, biases, AI.

Постановка проблеми. В умовах стрімкого впровадження штучного інтелекту (ШІ) та алгоритмічних систем у сфері кримінального провадження питання збереження і гарантування реалізації презумпції невинуватості, як однієї основних засад кримінального провадження, набуває особливої актуальності. По-перше, автоматизовані інструменти, що застосовуються на різних етапах кримінального процесу (від прогностичного поліцейського профілювання до алгоритмів оцінки ризику, систем розпізнавання обличчя тощо), можуть створювати приховані упередження та знижувати прозорість ухвалення рішень. По-друге, європейські ініціативи з регулювання ШІ (зокрема AI Act) прямо вказують на можливі загрози для прав людини, зокрема права на справедливий суд і презумпції невинуватості, якщо системи не відповідають високим вимогам прозорості, точності та документованості. По-третє, практичні кейси неправомірного арешту осіб на підставі ненадійних алгоритмічних висновків підкреслюють необхідність глибокого наукового аналізу цієї проблематики. Таким чином, обрана тема поєднує правові принципи і сучасні технологічні виклики, що робить її важливою як для наукового осмислення, так і для практичних рекомендацій.

Наведені факти свідчать про широкий розмах використання ШІ в кримінальній юстиції та потенційні ризики для фундаментальних гарантій. Це обґрунтовує необхідність дослідження впливу технологій на презумпцію невинуватості як складову права на справедливий суд.

Стан опрацювання. У юридичній літературі значну увагу питанням, присвяченим використанню ШІ в кримінальному провадженні, у тому числі в аспекті забезпечення презумпції невинуватості, приділяли такі вчені-процесуалісти, як Капліна О.В., Костюченко О.Ю., Туманяц А.Р.,

Крицька І.О., Верхогляд-Герасименко О.В. та інші. Разом із тим, залишається багато проблемних та не вирішених питань в даній сфері.

Метою даної статті є комплексний аналіз впливу алгоритмічних систем (зокрема технологій розпізнавання обличчя, алгоритмічних інструментів оцінки ризику та прогнозного поліцейського профілювання) на реалізацію принципу презумпції невинуватості в кримінальному провадженні.

Виклад основного матеріалу. Стаття 6 ЄКПЛ гарантує право на справедливий суд у всіх кримінальних провадженнях. Зокрема, пункт 2 прямо встановлює презумпцію невинуватості: «Кожен, кого обвинувачено у вчиненні кримінального правопорушення, вважається невинуватим доти, доки його вину не буде доведено в законному порядку» [1]. Практика Європейського суду з прав людини (ЄСПЛ) розгортає зміст цього принципу як процедурну гарантію. Зокрема:

1) Рішення органів влади чи суду не повинні апіорі посилювати враження про винуватість особи до остаточного вироку.

2) Тягар доведення лежить на стороні обвинувачення, а будь-які сумніви слід тлумачити на користь обвинуваченого.

Забезпечується право захисту на доступ до доказів та можливість їх оскарження, щоб виключити ситуації, коли «чорні скриньки» доказів залишаються недоступними для перевірки з боку захисту чи суду.

ЄСПЛ неодноразово наголошував, що порушення презумпції може відбутися як прямим чином (наприклад, публічні заяви посадовців про «винуватість» до вироку), так і опосередковано (допуск неналежних доказів, непрозора експертна інформація тощо) [2].

Директива (ЄС) 2016/343 щодо посилення окремих аспектів презумпції невинуватості та права бути присутнім на судовому розгляді встановлює мінімальні спільні стандарти для держав-членів ЄС у кримінальному процесі. Зокрема:

- Тягар доведення винуватості залишається на обвинуваченні, без перенесення його на захист; водночас директива підкреслює обов'язок суду шукати як докази провини, так і виправдувальні докази за можливістю та закріплює цей принцип без введення єдиного європейського стандарту «поза розумним сумнівом».

- Забезпечує право обвинуваченого бути присутнім на всіх стадіях судового розгляду, що унеможливорює виключення сторони з процесу без достатніх підстав.

- Зауважує, що публічні заяви або дії органів, які можуть створювати враження про винуватість (наприклад, формулювання у рішеннях про запобіжні заходи), не повинні прямо чи опосередковано подавати обвинуваченого як винного.

- Закликає до індивідуалізації заходів, наприклад фізичних обмежень (при необхідності), з чітким обґрунтуванням, щоб не підривати презумпцію. [3]

Таким чином, директива розгортає загальні положення Статті 6 ЄКПЛ у напрямі уніфікації процедурних гарантій у межах ЄС та підкреслює прозорість і рівність сторін у кримінальному процесі.

Велике значення для забезпечення реалізації презумпції невинуватості мають Європейські ініціативи з регулювання штучного інтелекту (ШІ). Зокрема, Regulation (EU) 2024/1689 (AI Act) класифікує застосування ШІ за рівнем ризику. Системи, що використовуються в правоохоронних чи судових цілях (predictive policing, алгоритми оцінки ризику рецидиву, розпізнавання обличчя тощо), розглядаються як високоризикові застосунки й підлягають суворим вимогам прозорості, документованості, тестування на упередження та аудита [4]. Системи з неприпустимим ризиком підлягають забороні, а для інших запроваджуються механізми оцінки та моніторингу, щоб гарантувати, що рішення не підривають основні права, зокрема право вважатися невинуватим до винесення вироку.

Європейські парламентські ініціативи: Резолюція Європейського парламенту від 6 жовтня 2021 р. «Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters» прямо зазначає, що системи прогнозування, профілювання та автоматизованого ухвалення рішень у кримінальному праві можуть порушувати фундаментальні права, включно з презумпцією невинуватості, і наполягає на відповідних обмеженнях чи заборонах [5].

Інші документи Ради Європи та ЄС: Європейський етичний статут СЕРЕП щодо використання ШІ в судових системах підкреслює необхідність прозорості й підзвітності у випадку застосування автоматизованих рішень у кримінальних процесах. Комунікації Єврокомісії та висновки груп експертів (High-Level Expert Group) також наголошують на балансі між інноваціями та гарантуванням прав людини.

Слід також проаналізувати міжнародні рекомендації та позиції неурядових організацій щодо реалізації права на справедливий суд і презумпцію невинуватості. Зокрема, Fair Trials та подібні організації фіксують, що автоматизовані системи профілювання та прогнозування ризику часто посилюють дискримінацію та ускладнюють реалізацію права на справедливий суд і презумпцію невинуватості. Наприклад, у звіті «Automating Injustice» описано випадки, коли алгоритмічні рішення призводили до непропорційного орієнтування на окремі групи населення і порушення базових гарантій [6]. Fair Trials закликає до заборони певних застосувань (наприклад, predictive policing) та впровадження жорстких механізмів прозорості, перевірок даних і прав на оскарження автоматизованих рішень.

Інші міжнародні рекомендації також спрямовані на забезпечення того, щоб автоматизовані інструменти не підривали процедури доказування та не ставили захист у завідомо невинуватого становище.

Наведені нормативно-правові орієнтири демонструють, що як класичні гарантії (Стаття 6 ЄКПЛ, Директива 2016/343), так і сучасні ініціативи щодо регулювання ШІ (AI Act, резолюції ЄП, етичні статuti CEREP) поєднуються у прагненні зберегти й посилити презумпцію невинуватості в умовах цифровізації кримінального судочинства. Водночас позиції організацій на кшталт Fair Trials вказують на реальні загрози непрозорих алгоритмічних рішень. Отже, мета подальшого дослідження — виявити, наскільки існуючі процедури та норми здатні забезпечити рівний доступ до процедурних гарантій у разі застосування ШІ та якими можуть бути доповнення чи зміни для посилення презумпції невинуватості в новому технологічному контексті.

Слід зазначити, що певні технології, викликають занепокоєння, зокрема: 1) розпізнавання обличчя в розслідуваннях становлять проблеми прозорості, точності, інформування підозрюваного; 2) алгоритмічні системи оцінки ризику (bail / risk assessment tools) можуть впливати на рішення щодо запобіжних заходів.

Системи розпізнавання обличчя (face recognition) стають дедалі поширенішими в роботі правоохоронних органів: від автоматичного відбору підозрюваних за відеозаписами до «сканування» вулиць у реальному часі. Проте практичні кейси демонструють низку суттєвих ризиків.

Непрозорість алгоритмів («чорна скринька»). Більшість комерційних та навіть державних систем розпізнавання обличчя працюють як закриті рішення без відкритого доступу до вихідного коду чи докладної методології навчання. Це унеможливорює глибоку перевірку коректності роботи алгоритму захистом чи незалежними експертами, що ослаблює процедуру оскарження доказів, отриманих з його допомогою [7].

Через відсутність прозорості захист не може з'ясувати, наскільки надійні конкретні співпадіння; це послаблює стандарт «поза розумним сумнівом» і може призвести до ситуацій, коли підозрюваного фактично звинувачують на основі ненадійного інструменту.

Похибка й упередження (точність). Дослідження підтверджують, що системи розпізнавання обличчя можуть демонструвати значно вищі рівні хибних позитивів для певних груп населення (зокрема за расовою чи гендерною ознакою) [8]. Це підсилює ризик неправомірних арештів, особливо коли система подає підозрюваного як «збіг» без подальшої ретельної перевірки.

Хибні позитиви підривають довіру до всього процесу: якщо особу затримано через помилкове розпізнавання, це вже ставить її у положення, яке важко повністю компенсувати навіть у разі виправдання. Крім того, непропорційний вплив на вразливі або групи меншин суперечить принципу рівності перед законом.

Є також проблема в інформуванні підозрюваного і у реалізації його права на захист. Часто правоохоронці застосовують розпізнавання обличчя без належного інформування особи: підозрюваний може не знати про використання такої технології проти нього і, отже, не може належно підготувати аргументи захисту чи запросити експертизу алгоритму [9].

Невідомість щодо методів отримання доказів призводить до ситуації, коли захист опиняється в нерівних умовах: без доступу до вихідних даних чи методології неможливо визначити, чи належним був сам процес і чи варто оскаржувати результати алгоритму.

Алгоритмічні інструменти оцінки ризику (pretrial risk assessment) використовуються судами в низці країн (зокрема в США) для прогнозування ймовірності неявки підозрюваного до суду або ризику рецидиву, з метою прийняття рішень про заставу чи інші запобіжні заходи.

Формування оцінки на основі історичних даних зі збереженням упереджень. Дані, на яких формуються алгоритми, походять із системи правосуддя, яка вже демонструє нерівності (напри-

клад, більш інтенсивне поліцейське стеження за певними громадами). Тому інструменти часто відтворюють і навіть підсилюють ці упередження [10].

Якщо алгоритм видає високий ризик на основі арештів, які відбулись через упереджене патрулювання, він може привести до суворіших запобіжних заходів для представників вже маргіналізованих спільнот. Це підриває презумпцію невинуватості, адже рішення ухвалюється з урахуванням ймовірності ризику, сформованої з упереджених даних, а не лише конкретних обставин справи.

Використання суддями як «підсилювач» власних рішень. Дослідження показують, що судді іноді використовують результати ризик-оцінки для підтвердження рішення, яке вони мали намір ухвалити спочатку, а не як незалежний інструмент перевірки [11].

Така вибіркова інтеграція алгоритмічних порад може приховувати потенційні проблеми системи від критичного розгляду і створювати ілюзію об'єктивності, коли насправді рішення ухвалюється на суб'єктивних засадах, підкріплених «цифровим» показником.

Неповідомлення підозрюваному про критерії та джерела даних. Підозрюваному часто не розкривають, як сформовано його оцінку ризику, які дані були задіяні, і чи може він оскаржити оцінку чи вказати на неточності в інформації. Відсутність прозорості щодо методології порушує право на ефективний захист: неможливо перевірити або спростувати дані, що лягли в основу рішення про запобіжний захід. Це суперечить ідеї, що будь-які сумніви слід тлумачити на користь підозрюваного.

Зміщення фокусу з конкретних обставин справи. Замість аналізу індивідуальних обставин (особистісні характеристики, реальні умови проживання, сімейні зв'язки тощо) ухвалюють рішення, спираючись на узагальнену статистичну модель. Алгоритмічний підхід може обнуляти нюанси справи й підводити всіх під єдину лінійку ризику, що суперечить індивідуалізованому розгляду та принципу *in dubio pro reo*, коли кожний випадок розглядається окремо з урахуванням обставин.

Слід наголосити, що «міжнародне співтовариство докладає багато зусиль для реформування процедури отримання транснаціональних електронних доказів під час адаптації до сучасних вимог. Нові правила ЄС щодо надання та зберігання транснаціональних електронних доказів охоплюють категорії даних абонентів, доступу до транзакцій та контенту. Встановлено, що проекти SIRIUS і TREIO є важливими інструментами для підтримки правоохоронних органів ЄС у питаннях, пов'язаних з транснаціональними електронними доказами. В Україні необхідно вдосконалити законодавство щодо порядку отримання транснаціональних електронних доказів з урахуванням міжнародної практики. Використання рекомендацій проектів SIRIUS та TREIO в Україні може сприяти вдосконаленню процедури міжнародного співробітництва щодо доступу до транснаціональних електронних доказів у кримінальних розслідуваннях.» [12]

Висновки. У статті проаналізовано вплив алгоритмічних та штучно-інтелектуальних технологій на реалізацію принципу презумпції невинуватості як складової права на справедливий суд. Проведений огляд нормативно-правових орієнтирів (Стаття 6 ЄКПЛ, Директива 2016/343, AI Act та ін.), ключові технології, що викликають занепокоєння, дозволяють сформулювати наступні висновки:

Наразі існуючі гарантії презумпції невинуватості залишаються фундаментально важливими, але потребують адаптації до нових реалій.

Класичні норми (Стаття 6 ЄКПЛ, Директива 2016/343) і сучасні ініціативи щодо регулювання ШІ (AI Act, резолюції ЄП, рекомендації Fair Trials) створюють міцну базу для захисту прав підозрюваних. Однак швидкий розвиток «чорних скриньок» алгоритмічних систем вимагає оновлення процедурних механізмів щодо доступу до даних, пояснення рішень і незалежного аудиту (European Parliament & Council, 2021; Fair Trials, 2022).

Непрозорість алгоритмів і недостатня explainability суттєво ускладнюють рівність сторін у кримінальному процесі.

Обмежений доступ захисту до внутрішньої логіки моделей перетворює алгоритмічні висновки на фактичний «недосяжний доказ», який важко оскаржити. Це підриває стандарт «поза розумним сумнівом» і може призводити до ситуацій, коли машинами підтверджується позиція обвинувачення, хоча якість і надійність такого доказу сумнівні.

Автоматичне підсилення упереджень (data bias) становить серйозну загрозу справедливості, особливо для вразливих або маргіналізованих спільнот.

Історично упереджені дані (зокрема дані про арешти чи правопорушення) закладені в моделі оцінки ризику і прогнозного профілювання, що призводить до feedback loop і стигматизації спільнот. Відтак навіть невинні особи можуть опинитися під посиленням контролю або отримати суворіші запобіжні заходи на основі статистичних маркерів, а не індивідуального аналізу обставин.

Алгоритмічні «висновки» не повинні автоматично розглядатися як основний доказ.

Результати розпізнавання обличчя або ризик-скорінгу можуть бути корисними орієнтирами, але без незалежного аудиту та пояснення не варто надавати їм надмірної ваги. Існує ризик, що судді, під впливом уявлення про «об'єктивність» комп'ютерних систем, будуть оцінювати такі результати як достатній доказ, що зміщує тягар доказування з обвинувачення на захист.

5. Необхідні комплексні заходи для збереження презумпції невинуватості в умовах застосування ШІ:

- Прозорість і explainability: законодавче і регуляторне закріплення вимог до зрозумілих пояснень алгоритмічних рішень або доступу до документації, що дозволяє перевірку.
- Незалежні аудити та валідація: регулярні перевірки моделей і даних спеціалізованими експертами, фінансовані державою або здійснювані під наглядом уповноважених органів.
- Регуляторні обмеження: заборона або суворі умови застосування алгоритмів у критичних етапах, де рішення може безпосередньо обмежити свободу особи, з урахуванням потенційних похибок і впливу на правову позицію підозрюваного.
- Підготовка учасників процесу: системні освітні програми для суддів, прокурорів і захисників щодо особливостей алгоритмів, ризиків упереджень та методів перевірки.
- Гарантії доступу до експертиз захисту: створення механізмів, що забезпечують захист можливістю ініціювати незалежну перевірку алгоритмічних інструментів без непропорційних витрат.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Конвенція про захист прав людини і основоположних свобод URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 14.08.2025).
2. Guide on Article 6 of the European Convention on Human Rights: Right to a fair trial (criminal limb). Council of Europe. 2022. URL: <https://rm.coe.int/1680304c4e> (дата звернення: 24.07.2025).
3. Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on strengthening certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings : Directive EU from 09.03.2016 // Official Journal of the European Union. L65, 1–11, 11.03.2016. URL: <https://eur-lex.europa.eu/eli/dir/2016/343/oj> (дата звернення: 24.07.2025).
4. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 12 July 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) : Regulation EU from 12.07.2024. Official Journal of the European Union. L229, 1–181, 12.07.2024. URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (дата звернення: 24.07.2025).
5. European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)) : Resolution of European Parliament from 06.10.2021. Official Journal of the European Union. C132, 17–26, 14.03.2022. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2022.132.01.0017.01.ENG (дата звернення: 24.07.2025).
6. Automating injustice: The impact of predictive policing and risk assessment algorithms on fair trial rights. Fair Trials. 2022. URL: <https://www.fairtrials.org/report/automating-injustice> (дата звернення: 24.07.2025).
7. Facial recognition technology needs stricter regulation. The Guardian. 17.06.2025. URL: <https://www.theguardian.com/technology/2025/jun/17/facial-recognition-technology-needs-stricter-regulation> (дата звернення: 24.07.2025).
8. Predictive policing has prejudice built in. The Guardian. 10.04.2025. URL: <https://www.theguardian.com/uk-news/2025/apr/10/predictive-policing-has-prejudice-built-in> (дата звернення: 24.07.2025).

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. 23.05.2016. URL: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> (дата звернення: 24.07.2025).
10. Pattison-Gordon J. Risk assessment algorithms can unfairly impact court decisions. GovTech. 27.09.2021. URL: <https://www.govtech.com/public-safety/risk-assessment-algorithms-can-unfairly-impact-court-decisions> (дата звернення: 24.07.2025).
11. Pretrial algorithms and racial disparities. The Bail Project. 2022. URL: <https://bailproject.org/policy/pretrial-algorithms/> (дата звернення: 24.07.2025).
12. Костиuchenko O., Akhtyrskaya N., Sereda Y., Vynohradova A., Miroshnykov I. The role of transnational electronic evidence in the investigation of crimes . Amazonia Investiga, Volume 12 – Issue 71 / November (2023). P. 293-303. URL: <https://doi.org/10.34069/AI/2023.71.11.26> (дата звернення: 14.08.2025).