Механізми юридичного захисту людини від неправомірного використання її біометричних даних у системах штучного інтелекту

Горгіладзе Нодарі Русланович[1]

Опубліковано	Секція	УДК
17.11.2025	Право	342.7:347.77:004.8

DOI: https://doi.org/10.5281/zenodo.17673664

Анотація. Метою статті є аналіз правових механізмів забезпечення захисту особи від незаконного збору, обробки та використання її біометричних даних у процесах функціонування систем штучного інтелекту. У дослідженні застосовано формально-юридичний, порівняльно-правовий, системно-структурний, логіко-нормативний і функціональний методи. На основі аналізу норм міжнародного та національного законодавства виокремлено систему принципів правового захисту біометрії – законність і пропорційність обробки, мінімізація даних, точність і безпека, інформування, право на забуття та заборона повної автоматизації рішень без участі людини. Визначено чотири основні групи ризиків: дискримінація внаслідок алгоритмічного упередження, порушення приватності, обмеження автономії особи та відсутність ефективного правового захисту. Запропоновано інституційні та процедурні механізми підвищення рівня захисту прав людини у сфері біометрії, зокрема запровадження обов'язкового алгоритмічного аудиту систем ШІ, створення державного реєстру високоризикових алгоритмів та законодавче закріплення процесуального права особи на пояснення логіки прийнятого рішення.

Ключові слова: фізіологічні та поведінкові характеристики, ідентифікація, право на приватність, дискримінація, автоматизації рішень.

Mechanisms for the legal protection of people from illegal use of biometric data in artificial intelligence systems

Annotation. In the digital environment, biometric data has become a key category of personal information, and its mass processing by artificial intelligence systems poses unprecedented risks to the implementation of fundamental human rights, particularly the right to privacy, dignity, and legal certainty. The purpose of the article is to analyze legal mechanisms aimed at ensuring the protection of a person from the illegal collection, processing and use of their biometric data in the processes of functioning of artificial intelligence systems. During the

[1] директор програми, NOTA Digital Currencies Research Center Inc., м. Сакраменто, Каліфорнія, США, nodari.gorgiladze@gmail.com, ORCID: https://orcid.org/0009-0007-2384-0036

research process, a set of general scientific and specialized legal methods was employed: formal-legal, comparative-legal, system-structural, logical-normative, and functional. The source base consisted of international legal acts and the national legislation of Ukraine. It was established that biometric data is a unique category of personal information that combines a technical identification function and the legal status of the object of protection. Based on an analysis of international and national legislation, a system of principles for the legal protection of biometrics has been identified, including the legality and proportionality of processing, data minimization, accuracy and security, information, the right to be forgotten, and the prohibition of full automation of decisions without human participation. Four main groups of risks have been identified: discrimination due to algorithmic bias, violation of privacy, restriction of individual autonomy and lack of adequate legal protection. It has been proven that the absence of a mechanism for the «right to explanation» and algorithmic accountability leads to legal uncertainty, making it impossible to challenge automated decisions. It is proposed to introduce institutional and procedural mechanisms to increase the level of human rights protection in the field of biometrics, in particular, the introduction of a mandatory algorithmic audit of AI systems, the creation of a state register of high-risk algorithms and the legislative consolidation of a person's procedural right to explain the logic of the decision made.

Keywords: physiological and behavioral characteristics, identification, right to privacy, discrimination, decision automation.

Вступ

Розвиток систем штучного інтелекту (далі – ШІ) супроводжується зростанням масштабів обробки біометричних даних – унікальних фізіологічних або поведінкових характеристик людини, що дозволяють її ідентифікувати. Технології розпізнавання обличчя, відбитків пальців, голосу, райдужної оболонки ока та навіть ходи інтегруються у фінансові, медичні, транспортні, освітні й державні сервіси. Водночас концентрація таких даних у цифрових системах створює ризики порушення фундаментальних прав людини – права на приватність, на захист персональних даних і на гідність. Проблема ускладнюється тим, що алгоритми штучного інтелекту, здатні до самонавчання, можуть використовувати біометричну інформацію поза межами первинної мети збору, що породжує загрозу масового стеження, дискримінації та маніпуляцій поведінкою осіб.

У роботах останніх років простежується поступове формування міждисциплінарного підходу, який поєднує правові, етичні та технологічні аспекти захисту особистих даних у процесах, що залучають алгоритми ШІ. Вагомий внесок у дослідження вітчизняного контексту зробив В. О. Гончаренко [1], який акцентував на відсутності системного законодавчого підґрунтя для регулювання використання технологій розпізнавання обличчя в Україні. Автор довів, що чинні норми права не забезпечують належного балансу між суспільною безпекою та правом особи на приватність, а механізми контролю за обробкою біометричних даних залишаються фрагментарними. Аналізуючи правове забезпечення захисту персональних даних крізь призму практики Європейського суду з прав людини (далі – ЄСПЛ), О. А. Тимошенко [2] виявила прогалини у впровадженні принципів пропорційності та необхідності у вітчизняному правозастосуванні. Авторка встановила, що українські норми недостатньо відображають вимоги ЄСПЛ щодо забезпечення ефективних засобів правового захисту у випадках втручання в приватне життя, зокрема, при автоматизованій обробці біометричної інформації. Питання правового реагування на використання ШІ в системах спостереження висвітлили О. М. Машталяр і В. Г. Хахановський [3]. Науковці визначили, що поєднання масового відеоспостереження та алгоритмів розпізнавання облич

створює високий ризик порушення основоположних прав людини. Вони відзначили відсутність у національному законодавстві чітких процедур ліцензування та незалежного моніторингу використання ШІ-технологій, запропонувавши запровадити модель «алгоритмічного аудиту» та спеціальний державний реєстр високоризикових систем.

Суттєвий внесок у розуміння специфіки правового захисту персональних даних зробили О. Явор та ін. [4], які проаналізували проблему охорони даних неповнолітніх у контексті вимог Загального регламенту Європейського Союзу про захист даних (General Data Protection Regulation, GDPR). Вони виявили, що в Україні відсутні ефективні механізми перевірки згоди на обробку персональних даних дітей, а освітні та розважальні платформи часто порушують принципи мінімізації даних. У контексті дослідження взаємозв'язку між цифровими технологіями, доказовою діяльністю та правовими механізмами захисту особи заслуговують на увагу результати А. М. Тимчишина [5], який розглянув судову експертизу як ключову процесуальну форму використання спеціальних знань у кримінальному провадженні. Автор встановив, що застосування цифрових технологій та інтелектуальних систем у сфері судової експертизи створює нові можливості для виявлення, перевірки й оцінки доказів, однак водночас вимагає чіткого нормативного визначення меж використання алгоритмів. Розвиток цієї проблематики також знайшов відображення у роботі Х. А. Аль-Абабнех (H. A. Al-Ababneh) та ін. [6], які дослідили використання технологій Big Data для виявлення економічних злочинів у сфері публічних закупівель. Науковці довели, що алгоритми машинного аналізу великих даних здатні ефективно виявляти корупційні ризики та аномальні фінансові транзакції, але водночас створюють небезпеку втручання в приватне життя осіб через масову обробку персональної інформації. Правові ризики використання технологій розпізнавання обличчя у правоохоронній діяльності ЄС проаналізувала Г. Гюльтекін-Варконьї (G. Gültekin-Várkonyi) [7]. Вона встановила, що чинне законодавство Євросоюзу не створює достатніх гарантій недискримінаційності алгоритмічних рішень, а механізми контролю за поліцейськими базами даних залишаються обмеженими. Її висновки підтверджують необхідність уведення спільних європейських стандартів прозорості та незалежного нагляду. Крім того, В. Х. Стевіч (V. H. Stević) [8] розкрив проблему узгодження національних нормативів із європейськими вимогами щодо обробки біометричних даних у країнах Західних Балкан. Автор дійшов висновку, що впровадження положень міжнародних конвенцій вимагає не лише нормативного, а й інституційного забезпечення – створення незалежних органів моніторингу етичності штучного інтелекту. Отже, узагальнення наукових напрацювань свідчить про поступове усвідомлення ризиків, пов'язаних із біометричними технологіями та системами ШІ, але водночас виявляє недостатню кількість комплексних досліджень, присвячених правовим механізмам контролю за алгоритмічною обробкою біометричних даних в Україні.

Метою статті є визначення правових механізмів, що забезпечують захист людини від неправомірного використання її біометричних даних у системах ШІ. Для досягнення поставленої мети передбачено вирішення таких завдань: проаналізувати поняття, правову природу та особливості біометричних даних як об'єкта правового захисту у контексті розвитку ШІ; визначити ключові ризики та форми неправомірного використання біометричної інформації у процесах автоматизованої ідентифікації, верифікації та прогнозування поведінки осіб; сформулювати пропозиції щодо удосконалення національного законодавства та розроблення процедурних гарантій контролю над обробкою біометричних даних.

Виклад основного матеріалу дослідження. У цифровому середовищі біометричні дані посідають центральне місце серед категорій персональної інформації, що потребують особливого правового захисту. Їхня специфіка полягає в тому, що вони

безпосередньо пов'язані з фізіологічними або поведінковими характеристиками людини, які дозволяють однозначно її ідентифікувати. Згідно зі статтею 4(14) GDPR, біометричними визнаються персональні дані, отримані внаслідок спеціальної технічної обробки, які стосуються фізичних, фізіологічних або поведінкових характеристик фізичної особи і забезпечують або підтверджують її унікальну ідентифікацію [9]. Таке визначення охоплює, зокрема, відбитки пальців, зображення обличчя, сканування райдужної оболонки ока, дані голосу, динаміку підпису або шаблони ходи. В оновленій Конвенції Ради Європи № 108+ «Про захист осіб щодо автоматизованої обробки персональних даних» термін «біометричні дані, що однозначно ідентифікують особу» використовується у контексті особливих категорій даних, обробка яких допускається лише за наявності спеціальних гарантій [10]. Конвенція підкреслює нерозривний зв'язок між біометричними параметрами та правом людини на приватність і гідність, наголошуючи на необхідності мінімізації обробки таких даних і забезпечення прозорості алгоритмічних процесів. Додаткове уточнення поняття пропонує Регламент Європейського Союзу про штучний інтелект (Artificial Intelligence Act, AI Act) [11], який класифікує системи біометричної ідентифікації як такі, що створюють підвищений ризик для основних прав людини. Відповідно до статті 3(33) цього Регламенту, біометричні дані – це персональні дані, отримані внаслідок спеціальної технічної обробки, які описують або дозволяють ідентифікувати фізичні, фізіологічні чи поведінкові особливості особи. Таким чином, законодавство Європейського Союзу (ЄС) формує уніфікований підхід, що поєднує технічний критерій (спосіб отримання даних) та юридичний (здатність забезпечити унікальну ідентифікацію).

У законодавстві України визначення біометричних даних закріплено у низці нормативних актів спеціального характеру. Так, Закон України «Про Єдиний державний демографічний реєстр» від 20 листопада 2012 р. № 5492-VI [12] визначає біометричні дані як сукупність параметрів людини, що характеризують її фізіологічні та біологічні ознаки, зафіксовані у формі цифрових даних та придатні для автоматизованої перевірки її ідентичності (ст. 3). Аналогічні підходи містяться в Законі України «Про захист персональних даних» № 2297-VI від 01.06.2010 р. [13], який передбачає, що обробка біометричних персональних даних належить до категорії обробки з підвищеним рівнем ризику та може здійснюватися лише за наявності згоди суб'єкта або передбачених законом підстав (ст. 7). Таким чином, біометричні дані становлять специфічний об'єкт правового регулювання, який поєднує властивості персональної, біологічної та цифрової інформації. На основі проведеного аналізу джерел літератури можна виокремити систему основоположних правових принципів, що регулюють обробку та захист біометричної інформації (табл. 1).

Таблиця 1

Правові принципи захисту біометричних даних

Принцип	Зміст і нормативне закріплення
Законність і пропорційність обробки	Обробка біометричних даних допускається лише за наявності чітко визначених правових підстав – згоди суб'єкта, виконання законного обов'язку чи захисту суспільного інтересу. Вимога пропорційності передбачає, що обсяг і спосіб обробки не можуть перевищувати необхідного для досягнення мети (ст. 5(1)(a–b) GDPR; ст. 6 Конвенції 108+; ст. 9 AI Act)
Обмеження мети	Біометричні дані мають збиратися виключно для конкретних, чітко визначених і законних цілей і не можуть надалі оброблятися у спосіб, несумісний із цими цілями (ст. 5(1)(b) GDPR). В AI Act ця вимога відображена у забороні вторинного використання даних для маніпуляцій або масового стеження
Мінімізація даних	Передбачає збір лише тих біометричних параметрів, які є необхідними для досягнення визначеної мети, без створення надлишкових баз даних.

Принцип	Зміст і нормативне закріплення
	Закріплено у ст. 5(1)(c) GDPR та імплементовано в українському законі «Про захист персональних даних» № 2297-VI (ст. 6)
Точність і збереження безпеки	Вимагає забезпечення актуальності даних, їх захисту від втрати, пошкодження, несанкціонованого доступу або модифікації. Принцип охоплює технічні й організаційні заходи безпеки, включно з шифруванням, псевдонімізацією (ст. 5(1)(d–f) GDPR; ст. 10 Конвенції 108+)
Право на інформування та згоду	Суб'єкт біометричних даних має бути чітко поінформований про мету, обсяг, строки та умови обробки, а також про можливість відкликати згоду. Це право закріплене у ст. 12–14 GDPR і ст. 8 Конвенції 108+
Право на видалення («право бути забутим»)	Особа має право вимагати видалення своїх біометричних даних у разі відкликання згоди або відсутності законних підстав для подальшої обробки (ст. 17 GDPR; ст. 9 Конвенції 108+). Це положення має особливе значення у контексті незворотності біометричних ідентифікаторів
Заборона повної автоматизації рішень без участі людини	Автоматизоване прийняття рішень, включно з профілюванням на основі біометрії, не може застосовуватися без можливості людського перегляду та втручання (ст. 22 GDPR; ст. 14 AI Act). Принцип забезпечує дотримання людської автономії у процесах, керованих алгоритмами

Джерело: сформовано автором на основі [9-13]

Система принципів, закріплена у міжнародному та національному праві, відображає зміщення акценту від формального регулювання процедур обробки персональних даних до змістовного забезпечення прав людини у цифровому середовищі. У сфері біометрії ці принципи мають підвищене значення, оскільки біометричні ідентифікатори є незмінними, унікальними та невіддільними від фізичної особи. Порушення принципів законності чи пропорційності в такому контексті призводить до довготривалих і часто незворотних наслідків для приватності.

Біометричні дані відрізняються від інших видів персональної інформації кількома суттєвими рисами. Насамперед вони є невід'ємними від фізичної сутності людини – на відміну від звичайних персональних даних (ім'я, адреса, телефон), біометричні ознаки неможливо змінити чи відкликати після їхнього розголошення. Це зумовлює особливо високий ризик порушення приватності у разі несанкціонованого доступу або повторного використання даних. Крім того, біометрія має постійний характер: у більшості випадків її параметри залишаються стабільними протягом життя особи, що робить ці дані привабливими для технологічних систем, але водночас небезпечними у разі втрати контролю над ними [14].

Важливою особливістю біометричних даних є також їх функціональний дуалізм – вони водночас виступають технічним інструментом ідентифікації та об'єктом юридичного захисту. У сфері штучного інтелекту такі дані використовуються не лише для верифікації, а й для навчання алгоритмів, прогнозування поведінки або оцінки емоційних станів, що виходить за межі первинної мети збору. Це створює потенційну колізію між технологічною ефективністю та принципом пропорційності обробки, закріпленим у статтях 5 і 6 GDPR**.** Особливістю цих ризиків є їх транснаціональний характер: біометричні дані передаються та обробляються у хмарних середовищах, розташованих поза межами державної юрисдикції. Це унеможливлює ефективний контроль з боку національних регуляторів і ставить під сумнів застосовність правових гарантій, встановлених внутрішнім законодавством. Як зазначає Європейська комісія у пояснювальній записці до AI Act, обробка біометрії має бути визнана діяльністю підвищеного ризику саме через її глобальний масштаб і потенційну здатність впливати на основоположні права людини [11]. Більшість порушень у цій сфері зумовлена дефіцитом правових механізмів контролю та непрозорістю алгоритмів, які приймають рішення без участі людини. Додатковим фактором ризику є комерціалізація біометрії приватними корпораціями. Дані, що первісно збиралися для ідентифікації або безпеки,

дедалі частіше використовуються для маркетингу, кредитного скорингу або соціального прогнозування. Це порушує принципи пропорційності та обмеження мети, визначені статтями 5–6 GDPR, і підриває довіру громадян до інститутів цифрової держави. На основі узагальнення наукових підходів [15; 16] та аналізу міжнародно-правових актів можна виділити чотири ключові групи ризиків, які концентрують основні форми порушень прав людини в умовах використання біометричних систем ШІ (табл. 2).

Таблиця 2

Основні ризики порушення прав людини, пов'язані з використанням біометричної інформації у процесах ШІ

Група ризиків	Характеристика порушення
Ризики дискримінації та порушення принципу рівності	Виникають унаслідок алгоритмічного упередження, коли моделі машинного навчання відтворюють расові, гендерні чи вікові стереотипи, притаманні навчальним наборам даних. Це призводить до нерівного ставлення в доступі до послуг, працевлаштування чи правосуддя
Ризики для права на приватність і захист персональних даних	Пов'язані з масовим збором біометричних ідентифікаторів без згоди суб'єктів через системи відеоспостереження, мобільні застосунки або соціальні мережі. Такі дії порушують ст. 8 Європейської конвенції з прав людини (ЄКПЛ) та принципи законності обробки (GDPR, ст. 5). Додатковою загрозою є повторне використання даних для інших цілей, зокрема комерційних
Ризики порушення права на автономію та людську гідність	Виявляються у використанні біометрії для профілювання, аналізу емоцій чи прогнозування поведінки. Такі практики можуть обмежувати свободу волевиявлення та формувати маніпулятивні моделі контролю над поведінкою людини. AI Act (ст. 5) забороняє системи, що експлуатують вразливість осіб або підривають їх автономію
Ризики для права на ефективний захист і правову визначеність	Стосуються відсутності прозорих механізмів оскарження автоматизованих рішень, ухвалених на підставі біометричних даних. Суб'єкт часто не має доступу до інформації про алгоритм, що приймає рішення, або права вимагати людського перегляду (ст. 22 GDPR). Це призводить до правової невизначеності й обмеження доступу до правосуддя

Джерело: сформовано автором на основі [9; 11; 17]

Проблема алгоритмічного упередження в системах ШІ становить одну з найбільш складних і суперечливих загроз правам людини у сфері біометричних технологій. Її сутність полягає в тому, що алгоритми машинного навчання, які використовуються для обробки біометричних даних, як-от зображення обличчя, голосові записи чи рухові патерни, здатні не лише відтворювати, але й підсилювати соціальні, расові або гендерні стереотипи, притаманні даним, на яких вони були навчені. Джерелом цього явища є системна упередженість у вихідних наборах даних: якщо навчальний масив непропорційно представлений певними групами (наприклад, чоловіками, людьми світлої шкіри чи європейського походження), алгоритм виробляє похибки в ідентифікації представників інших категорій. Емпіричним підтвердженням цього стала серія досліджень Дж. Буоламвіні (J. Buolamwini) та Т. Гебру (T. Gebru), яка продемонструвала, що провідні комерційні системи відеорозпізнавання облич, розроблені компаніями IBM, Microsoft і Face++, показували рівень помилок до 35% при ідентифікації темношкірих жінок, тоді як для білих чоловіків цей показник не перевищував 1% [18]. Такі результати засвідчили, що навіть високотехнологічні ШІ-рішення залишаються залежними від структурних упереджень, вбудованих у вихідні дані. Подібні випадки були зафіксовані й у криміналістичних системах розпізнавання

облич у США та Великій Британії, де хибні збіги призводили до неправомірного затримання осіб з темною шкірою або азійського походження [19].

Ці практики мають не лише технічний, а й правовий вимір, оскільки порушують низку базових норм європейського права. Зокрема, стаття 21 Хартії основних прав Європейського Союзу [20] прямо забороняє будь-яку дискримінацію за ознаками раси, кольору шкіри, етнічного чи соціального походження, статі або віку. Зі свого боку, стаття 14 ЄКПЛ [17] встановлює загальний принцип недискримінації у користуванні правами та свободами, гарантованими Конвенцією. Системне відтворення нерівності в алгоритмічних процесах розпізнавання є порушенням цих статей, навіть якщо збір та обробка біометричних даних формально здійснюються на законних підставах. Небезпеку становить те, що алгоритмічне упередження має прихований характер – його неможливо виявити без спеціального аудиту або прозорості вихідних моделей. Це призводить до ситуації, коли легально розроблені системи ШІ функціонують у спосіб, який створює соціально несправедливі наслідки: відмови у працевлаштуванні, необґрунтовані перевірки в аеропортах, дискримінаційні банківські скоринги тощо. Відповідно до статей 5, 6 і 22 GDPR, такі наслідки підпадають під правову відповідальність за порушення принципів прозорості, пропорційності та обмеження автоматизованого прийняття рішень без участі людини.

Одним із викликів у сфері використання біометричних технологій системами ШІ є відсутність у суб'єкта біометричних даних реального доступу до інформації про те, як і ким використовуються його дані. Незважаючи на формальне закріплення права на інформування у статтях 12–14 GDPR, практична реалізація цього права залишається номінальною. Алгоритми машинного навчання функціонують як «чорні скриньки», де процеси збору, аналізу й передачі даних відбуваються без відома і згоди особи. Унаслідок цього суб'єкт позбавлений можливості контролювати життєвий цикл власної біометричної інформації – від моменту її фіксації до подальшого комерційного або державного використання.

Додаткову проблему становить відсутність у правових системах більшості держав, включно з Україною, ефективного механізму реалізації «права на пояснення», що має забезпечувати прозорість алгоритмічних рішень. Стаття 22 GDPR надає особі право не бути об'єктом рішення, яке ґрунтується виключно на автоматизованій обробці, включно з профілюванням, якщо таке рішення має юридичні наслідки або істотно впливає на неї. Однак на практиці це право не реалізується через технічну непрозорість алгоритмів і відсутність обов'язку розробників надавати доступ до логіки прийняття рішень. У сфері біометрії це означає, що особа не може оскаржити, наприклад, відмову в працевлаштуванні, банківському кредиті чи візовому дозволі, якщо таке рішення ухвалено на основі автоматизованого аналізу її зображення або поведінкових даних.

Така ситуація прямо суперечить статті 13 ЄКПЛ [17], яка гарантує право на ефективний засіб правового захисту в разі порушення конвенційних прав. Європейський суд з прав людини у своїй практиці неодноразово наголошував, що держава має забезпечити особі не лише формальну можливість звернення до суду, а й реальний механізм оскарження втручання у приватне життя, зокрема, при обробці персональних або біометричних даних [21; 22]. Відсутність прозорих процедур розкриття інформації про алгоритмічні рішення унеможливлює ефективне застосування цього права. У більшості національних правових систем, включно з Україною, не створено спеціалізованих органів або процедур контролю за алгоритмічною обробкою біометрії, що значно послаблює інституційні гарантії захисту. Повноваження органів із питань захисту персональних даних (наприклад, Уповноваженого Верховної Ради України з прав людини) здебільшого обмежуються перевіркою законності збору та зберігання персональних даних, тоді як алгоритмічна підзвітність і верифікація рішень систем ШІ залишаються поза межами регуляторної компетенції. У результаті суб'єкт даних

фактично не має дієвого способу відновити свої права у випадку автоматизованої дискримінації чи технічної помилки.

Таким чином, відсутність механізмів пояснення, апеляції та інституційного контролю за використанням біометричних даних у системах ШІ створює правовий вакуум, що підриває ефективність фундаментальних гарантій, закріплених у ЄКПЛ та GDPR. Для його подолання необхідно впровадити спеціальні процедури «алгоритмічного аудиту», обов'язкову реєстрацію високоризикових систем ШІ, а також законодавчо визначити процесуальне право суб'єкта на отримання зрозумілого пояснення логіки прийнятого рішення. Лише за цих умов буде забезпечено реальну, а не декларативну, правову визначеність і ефективний захист людської автономії в умовах цифрової трансформації.

Алгоритмічний аудит має стати обов'язковою формою незалежної перевірки систем ШІ, які використовують або обробляють біометричні дані. Його метою є виявлення потенційних ризиків дискримінації, упередженості чи порушення принципу пропорційності у процесах автоматизованого прийняття рішень. Такий аудит повинен проводитися не лише на етапі розроблення системи, а й упродовж усього життєвого циклу її використання. У правовій площині доцільно закріпити вимогу про періодичний аудит у національному законодавстві за аналогією до статей 16–29 AI Act, які передбачають оцінку відповідності високоризикових систем та їх постійний моніторинг. Участь у таких аудитах повинні брати незалежні експерти з питань кіберправа, етики штучного інтелекту та захисту даних, а їх результати мають бути публічними для забезпечення довіри суспільства.

Усі системи, що обробляють біометричну інформацію для ідентифікації, верифікації або прогнозування поведінки осіб, повинні бути внесені до державного реєстру високоризикових систем ШІ. Такий реєстр має виконувати функцію інструменту прозорості, забезпечуючи доступ громадян до відомостей про те, які алгоритмічні технології застосовуються, ким вони розроблені та які категорії даних обробляються. Запровадження реєстру відповідатиме вимогам статей 51–55 AI Act, які передбачають створення єдиного європейського реєстру високоризикових систем, доступного як для регуляторів, так і для громадськості. В українському контексті таку функцію міг би виконувати спеціалізований підрозділ при Міністерстві цифрової трансформації або Уповноваженому з питань захисту персональних даних, який здійснював би реєстрацію та сертифікацію систем ШІ, що використовують біометрію.

Удосконалення національного законодавства у сфері регулювання біометричних технологій вимагає системного перегляду підходів до захисту прав суб'єктів даних. Передусім доцільним є імплементація в українську правову систему принципів алгоритмічної підзвітності, закріплених у статтях 13–14, 22 GDPR і розвинених у AI Act. Йдеться не лише про формальне декларування права особи на отримання інформації про обробку даних, а й про створення обов'язкових процедур, які забезпечують реальний доступ до пояснення логіки алгоритмічних рішень. Для цього необхідно внести зміни до Закону України «Про захист персональних даних», доповнивши його окремими положеннями про право суб'єкта вимагати індивідуалізоване пояснення результату автоматизованої обробки, а також право на апеляцію рішення, ухваленого системою ШІ.

Важливим напрямом реформування є законодавче закріплення інституту алгоритмічного аудиту. Необхідно передбачити обов'язковість регулярної незалежної перевірки всіх високоризикових систем, що використовують біометричні дані, із визначенням критеріїв ризиків, процедур перевірки, складу експертних груп та вимог до публічності результатів. У національному законодавстві варто передбачити норми, аналогічні статтям 16–29 AI Act, які встановлюють вимоги до оцінки відповідності, тестування, моніторингу та документування функціонування алгоритмів. Це дозволить

забезпечити технічну і правову прозорість систем ШІ та мінімізувати ризики автоматизованої дискримінації.

Подальшим кроком є створення державного реєстру високоризикових систем ШІ, що обробляють біометричні дані. Такий реєстр має містити інформацію про розробника, мету обробки, категорії даних, технічні характеристики моделі та результати проведених аудитів. У перспективі він може стати елементом інтегрованої європейської інфраструктури відповідно до статей 51–55 AI Act. У національному контексті створення реєстру доцільно покласти на спеціалізований підрозділ в структурі Уповноваженого Верховної Ради України з прав людини або Міністерства цифрової трансформації, забезпечивши їх розширеними повноваженнями щодо сертифікації та моніторингу таких систем.

З огляду на відсутність ефективних інституційних засобів реагування, необхідно створити спеціалізований наглядовий орган або підрозділ, який здійснюватиме контроль за алгоритмічною обробкою біометричної інформації. Його компетенція має охоплювати перевірку технічних моделей, аналіз наявності упередженості, оцінку відповідності принципам пропорційності та мінімізації даних, а також розгляд скарг громадян щодо рішень, ухвалених ШІ. Крім того, варто законодавчо закріпити процедурні гарантії подання індивідуальної скарги на неправомірне використання біометрії, що дозволить реалізувати вимоги статті 13 ЄКПЛ щодо ефективного засобу правового захисту.

Необхідними також є зміни до процесуального законодавства з метою визнання доказового статусу алгоритмічного звіту і технічного журналу обробки біометричних даних. Це забезпечить можливість судового контролю за діяльністю автоматизованих систем та дозволить судам здійснювати повноцінний аналіз правомірності рішень, які їх породжують. У цьому контексті доречно передбачити в Цивільному та Адміністративному процесуальних кодексах України окремі норми щодо порядку витребування інформації про алгоритм, його налаштування та джерела тренувальних даних. Отже, формування комплексної моделі правового захисту біометричних даних потребує не лише внесення точкових поправок до законодавства, а й розбудови інституційних та процедурних механізмів, які забезпечують алгоритмічну прозорість, підзвітність і ефективне відновлення порушених прав.

Висновки

Встановлено, що біометричні дані становлять особливу категорію персональної інформації, невід'ємно пов'язаної з фізіологічними та поведінковими характеристиками людини, які забезпечують її унікальну ідентифікацію. У міжнародному праві сформовано уніфікований підхід до розуміння біометрії як об'єкта правового захисту, що поєднує технічні та юридичні критерії.

Виявлено, що ключовими загрозами у сфері застосування біометричних технологій є порушення принципів приватності, недискримінації, автономії особи та правової визначеності. Алгоритмічне упередження у системах штучного інтелекту відтворює соціальні та расові стереотипи, що призводить до дискримінаційних наслідків навіть за формальної законності обробки даних. Масовий збір біометричної інформації без згоди суб'єктів, відсутність прозорих механізмів контролю та комерціалізація біометрії приватними корпораціями створюють системну загрозу для реалізації права на повагу до приватного життя (ст. 8 ЄКПЛ) і принципів законності та пропорційності, закріплених у статтях 5–6 GDPR.

Для підвищення ефективності правового захисту запропоновано: запровадити процедури алгоритмічного аудиту, які дозволять виявляти ризики дискримінації та порушення пропорційності при обробці біометрії; створити державний реєстр високоризикових систем штучного інтелекту, що забезпечить прозорість та публічний

контроль за технологіями, які оперують біометричними даними; законодавчо закріпити процесуальне право на пояснення логіки алгоритмічного рішення, гарантувавши можливість його оскарження; посилити повноваження органів із захисту персональних даних у сфері моніторингу алгоритмічних процесів і транскордонної передачі біометричної інформації.

Список використаних джерел

1. Гончаренко, В. О. (2021). Правове регулювання використання технологій розпізнавання обличчя. *Часопис цивілістики*, 41, 56–60. https://dspace.onua.edu.ua/items/007fafa4-859e-4fa4-a55b-c7ff26205646

2. Тимошенко, О. А. (2023). Захист персональних даних в цивільних правовідносинах: вітчизняне правове забезпечення крізь призму практики Європейського суду з прав людини. *Аналітично-порівняльне правознавство,* 165–172. https://doi.org/10.24144/2788-6018.2023.04.27

3. Машталяр, О. М., Хахановський, В. Г. (2024). Масове спостереження та розпізнавання обличчя за допомогою штучного інтелекту: правові виклики та перспективи регулювання в Україні. *Юридичний науковий електронний журнал*, 11, 317–320. https://doi.org/10.32782/2524-0374/2024-11/72

4. Явор, О., Піддубна, В., Рубан, О. (2023). Правові питання щодо захисту персональних даних неповнолітніх відповідно до національного законодавства та вимог GDPR. *ScienceRise: Juridical Science*, 3 (25), 23–34. http://doi.org/10.15587/2523-4153.2023.286647

5. Тимчишин, А. М. (2023). Судова експертиза як процесуальна форма використання спеціальних знань у кримінальному провадженні. *Південноукраїнський правовий часопис, 1*, 228–235. https://doi.org/10.32850/sulj.2023.1.40

6. Al-Ababneh, H. A., Fedorchuk, Y., Tymchyshyn, A., Pishchenko, G., & Hrytsai, S. (2024). The use of big data in the detection of economic crimes in public procurements. *Journal of Theoretical and Applied Information Technology, 102*(24), 8860–8872. https://www.jatit.org/volumes/Vol102No24/3Vol102No24.pdf

7. Gültekin-Várkonyi, G. (2024). Navigating data governance risks: Facial recognition in law enforcement under EU legislation. *Internet Policy Review, 13*(3). https://doi.org/10.14763/2024.3.1798

8. Stević, B. H. (2024). Biometric data and artificial intelligence: EU standards and BiH alignment. *Journal of Ethics and Legal Technologies, 6*(2), 109–127. https://jelt.padovauniversitypress.it/system/files/papers/JELT-2024-2-6.pdf

9. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR) (2016). *Official Journal L 119, 4 May 2016*. https://eur-lex.europa.eu/eli/reg/2016/679/oj

10. Convention 108+ for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 223) (2018). *Strasbourg: Council of Europe.* https://www.coe.int/en/web/data-protection/convention108-and-protocol

11. 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) (2024). Official Journal L 202, 12 July 2024. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

12. Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» № 5492-VI від 20 листопада 2012 р. Верховна Рада України. https://zakon.rada.gov.ua/laws/show/5492-17#Text

13. Закон України «Про захист персональних даних» № 2297-VI від 1 червня 2010 р. (ред. 2023 р.). Верховна Рада України. https://zakon.rada.gov.ua/laws/show/2297-17#Text

14. Pizzolo, C. (2025). AI, biometric data and the effective protection of fundamental rights in the recent ECJ case-law. *Unione europea e Diritti, 1*, 145–159. https://doi.org/10.1400/300816

15. Arnal, J. (2025). AI at Risk in the EU: It's Not Regulation, It's Implementation. *European Journal of Risk Regulation,* 1-10. https://doi.org/10.1017/err.2025.19

16. Sarra, C. (2025). Artificial intelligence in decision-making: A test of consistency between the «EU AI Act» and the «General Data Protection Regulation». *Athens Journal of Law, 11*(1), 45–62. https://doi.org/10.30958/ajl.11-1-3

17. Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights) (1950). Council of Europe. https://www.echr.coe.int/documents/convention_eng.pdf

18. Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of Machine Learning Research, 81, 77–91. https://proceedings.mlr.press/v81/buolamwini18a.html

19. Garvie, C. (2019). Garbage in, garbage out: Face recognition on flawed data. *Georgetown Law Center on Privacy & Technology.* https://www.flawedfacedata.com/

20. Charter of Fundamental Rights of the European Union (2012). *European Union.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT

21. European Court of Human Rights (2008). *S. and Marper v. the United Kingdom (Applications nos. 30562/04 and 30566/04)*. https://hudoc.echr.coe.int/eng?i=001-90051

22. European Court of Human Rights (2020). *Gaughran v. the United Kingdom (Application no. 45245/15).* https://hudoc.echr.coe.int/eng?i=001-200965