

Біометричні системи і технології: поняття, види, функції та основи регулювання у праві ЄС

Андрій Олександрович Гачкевич*

Навчально-науковий інститут права, психології та інноваційної освіти

Національного університету «Львівська політехніка»,

Львів, Україна

**e-mail: andrii.o.hachkevych@lpnu.ua*

Анотація

Актуальність порушеної проблеми обумовлена, по-перше, зростанням унаслідок розвитку штучного інтелекту впровадження біометричних систем і технологій у різних галузях, по-друге, відповідним посиленням ризиків та загроз від використання біометрії. Мета статті полягає у висвітленні теоретико-методологічних підходів до вивчення та правових основ регулювання біометричних систем і технологій з урахуванням положень законодавства ЄС, а також правозастосовної практики, включаючи рішення Європейського суду справедливості та наглядових органів держав-учасниць із захисту персональних даних. У процесі дослідження автор використав такі методи: класифікації, для того, щоб пояснити наявні можливості біометрії; порівняння – при зіставленні біометричної ідентифікації (визначення особи) та верифікації (перевірки особи) як ключових функцій біометричних систем і технологій; систематизації – для формування переліку найважливіших актів законодавства ЄС щодо біометрії як орієнтирів для українського законодавця, а також аналізу – при вивченні правозастосовної практики. Автор пояснює поняття біометричних технологій як виду технологій, які обробляють біометричні дані для розпізнавання особи, а біометричною системою вважає інформаційну систему, яка завдяки перетворенню біологічних характеристик у машиночитану форму та подальшого їх аналізу, встановлює зв'язок між біометричними даними, тим самим сприяючи розпізнаванню особи, а також встановлює належність особи до певної категорії. У статті біометричні системи і технології класифіковані за видом і кількістю використовуваних біологічних характеристик, необхідністю фізичного контакту та сферою застосування. Результати дослідження свідчать про те, що підтверджені правозастосовною практикою ЄС суперечності, які виникають через біометрію, зокрема, щодо того, наскільки обґрунтованими є збір, зберігання та використання відбитків пальців та інших біометричних ідентифікаторів за відсутності виразної згоди суб'єкта, підкреслюють необхідність удосконалення правового регулювання. Висновки статті показують, що, крім положень про захист персональних даних,

важливе значення для впорядкування застосування біометрії у суспільстві має законодавство у сфері штучного інтелекту, а також правове забезпечення галузевого впровадження біометричних технологій.

Ключові слова: біометричні технології; біометричні системи; біометричні дані; персональні дані; штучний інтелект; Система в'їзду/виїзду (EES).

Biometric Systems and Technologies: Concepts, Types, Functions and Legal Fundamentals in EU Law

Andrii O. Hachkevych*

Institute for Law, Psychology and Innovative Education

Lviv Polytechnic National University,

Lviv, Ukraine

**e-mail: andrii.o.hachkevych@lpnu.ua*

Abstract

The issue raised is relevant, firstly, to the growing implementation of biometric systems and technologies across various fields due to the development of artificial intelligence, and secondly, to the corresponding increase in risks and threats associated with their use. The purpose of this article is to explore the theoretical and methodological approaches to studying the use of biometric systems and technologies. It will also address the legal foundations surrounding their regulation, taking into account the provisions of the EU legislation, as well as law enforcement practices. This includes examining decisions made by the European Court of Justice, as well as supervisory authorities of EU member states regarding personal data protection. In this research, the author employed several methods: classification, to explain the existing capabilities of biometrics; comparison, to differentiate between biometric identification (determining identity) and verification (checking identity) as the key functions of biometric systems and technologies; systematization, to compile a list of the most important acts of EU legislation on biometrics, which will serve as guidelines for Ukrainian legislators; and analysis, to examine law enforcement practice. The author describes biometric technologies as a type of technology that processes biometric data for personal identification. A biometric system is defined as an information system that, by converting a person's biological characteristics into a machine-readable format and analyzing them, establishes both a link between biometric data samples, thereby facilitating personal identification, or a belonging of a person to a particular group. In the article, biometric systems and technologies are classified based on the type and number of biological characteristics used, the need for physical contact, and their range of applications. The results of the study reveal contradictions arising from the adoption of biometrics, as confirmed by EU law applications, particularly regarding the justification for the collection, storage, and use of fingerprints and other biometric identifiers without an individual's explicit consent. This underscores the need to improve legal regulation. The article concludes that, alongside

provisions on the protection of personal data, an important role in determining the use of biometric systems and technologies is played by both legislation regarding artificial intelligence and legal support for the sectoral implementation of biometric technologies.

Keywords: biometric technologies; biometric systems; biometric data; personal data; artificial intelligence; Entry/Exit System (EES).

Вступ

Використання біометричних даних як унікальних характеристик особи – поведінкових або, частіше, фізіологічних (наприклад, зображення обличчя), для розпізнавання завдяки сучасним технологіям, набуває дедалі більшого поширення. Ідентифікація та інші функції біометричних систем та технологій призначені для різних завдань – від перевірки особи власника мобільного телефону через сканування відбитків його пальців до встановлення належності голосу клієнтові банку, від з'ясування, чи шукач притулку є тим, за кого себе видає, до визначення особи з метою боротьби зі злочинністю.

Водночас зростання впровадження біометричних систем у різних галузях, яке пришвидшує розвиток штучного інтелекту, породжує дискусії з приводу того, наскільки це етично та законно, – особливо гостро це питання постає щодо відеоспостереження у громадських місцях. Незважаючи на незрівнянні нові можливості в органів державної влади та приватних компаній, використання біометричних технологій посилює ризики та небезпеки, а отже, має здійснюватися у відповідному правовому полі. Можливі наслідки помилки в ідентифікації є дуже серйозними, а самі по собі біометричні дані є важливим проявом особи у матеріальному світі.

Порушена у цій статті проблема регулювання біометричних систем та технологій, з одного боку, належить до сфери захисту персональних даних як досліджувана в контексті використання технологій для розпізнавання осіб завдяки збору та подальшого аналізу їхніх унікальних біологічних характеристик. З іншого боку, ця проблема так само стосується регламентації відносин у сфері штучного інтелекту, зважаючи на те, що сучасні біометричні системи функціонують на його базі, а також – інформаційної безпеки з огляду на необхідність більш ефективної правової охорони безпеки баз даних.

Огляд літератури

Серед українських авторів, які вивчали використання біометричних даних у правовій площині, – І. Бердиченко [1], А. Бойко (Мартінова) [2; 3; 4 – одне з найбільш комплексних досліджень в українській науці]; С. Бригинець [5]; В. Бродкевич та М. Гуцалюк [6]; К. Дубонос [7; 8]; В. Романов, І. Гале-

люка та О. Галелюка [9]; М. Стефанчук [10]; Т. Тарасевич [11]; Я. Щербак-кова та Л. Бзова [12] та ін. Зауважимо, що, поряд із вивченням передового досвіду регулювання біометричної ідентифікації у праві ЄС та США (на рівні штатів), відзначено те, що слід вносити зміни до чинних нормативно-правових актів, насамперед Закону України «Про захист персональних даних» [11], а також приймати нові спеціальні закони щодо використання біометричних технологій [13, с. 241].

Велика кількість авторів досліджувала застосування біометрії для цілей боротьби зі злочинністю та у правоохоронній діяльності (Р. Демчишак, І. Жуковський, О. Заярний, С. Книженко, В. Негребецький, О. Пчеліна, І. Савельєва, А. Стах, С. Філіппов, О. Шарабан). Щоправда, здебільшого вони розглядали дактилоскопічні як вид біометричних даних. Цікаво, що на початку 2010-х в Україні навіть був підготовлений та зареєстрований проект Закону України «Про ідентифікацію людини шляхом дактилоскопії» [14], згодом – відкликаний (у визначеннях термін «дактилоскопічна інформація» або «дактилоскопічні дані» пояснений як «відомості про особливості візерунків шкіри людини у графічному або іншому вигляді» [15]). Окремо варто згадати про працю «Біометричні технології в ХХІ столітті та їх використання правоохоронними органами» співавторів В. Захарова та В. Рудешка [16].

Ми також помітили окремий інтерес до поняття біометричного паспорту, який безумовно поживається знову внаслідок впровадження біометричної ідентифікації у прикордонному контролі при в'їзді на територію Шенгенської зони та виїзді з неї (І. Білоус, Д. Диська, В. Литовченко, В. Сезонов, І. Темник, Г. Тітаренко, І. Усатюк, І. Штульман, Х. Ярмакі та ін.). Біометричні технології можуть застосовуватись у фінансово-банківській сфері (А. Альохіна, Н. Волченко, В. Дяченко, А. Ключко, І. Сохань).

Біометричні системи та технології є популярним напрямом досліджень серед представників технічних наук (П. Бідюк, В. Бондарчук, І. Галелюка, П. Ключан, В. Романов, А. Фесенко, В. Швець тощо).

Слід підкреслити, що порушена проблема також частково висвітлювалась у працях, присвячених захисту персональних даних. Одним із прикладів є дисертаційне дослідження А. Михайлик, в якому розглянуто питання щодо використання відбитків пальців для допуску працівників на підприємство як «особливо чутливих» даних та виокремлено категорію «біометричних персональних даних» у класифікації персональних даних працівників [17].

У зарубіжній літературі біометричні системи та технології у правовому контексті розглядали такі автори, як К. Джассеренд, А. Кохемс, Е. Кіндт,

Ф. Нгуєн, К. Прінс, П. Розенцвайг, Р. Томас, П. де Херт, А. Шварц та ін. Серед опублікованих книг, присвячених порушеній проблемі, – «Приватність та проблеми захисту даних під час застосування біометричних технологій» [18], «Біометричне розпізнавання: виклики та можливості» [19], «Біометрія другого покоління: етичний, правовий та соціальний контекст» [20], Довідник з біометрії [21] тощо.

Матеріали та методи

Методологічну основу дослідження становлять такі методи, як: класифікації для того, щоб пояснити наявні можливості біометрії; порівняння – для зіставлення біометричної ідентифікації (визначення особи) та верифікації (перевірки особи) як ключових функцій біометричних систем та технологій; систематизації – для формування переліку найважливіших актів законодавства ЄС щодо біометрії як орієнтирів для українського законодавця, а також аналізу – для вивчення правозастосовної практики.

Джерельна база дослідження містить ключові нормативно-правові акти ЄС, які пов'язані з використанням біометричних систем та технологій, зокрема: у сфері захисту персональних даних (Директива 95/46/ЄС та Загальний регламент про захист даних 2016 р., Директива (ЄС) 2016/680), про штучний інтелект (Регламент (ЄС) 2024/1689), щодо паспортів та посвідчень особи для громадян ЄС (Регламент Ради (ЄС) № 2252/2004, Регламент (ЄС) № 444/2009, Регламент (ЄС) 2019/1157), про впровадження системи EES та нових правил в'їзду на територію Шенгенської зони та виїзду з неї (Регламент (ЄС) 2017/2226, Регламент (ЄС) 2025/1534), а також – застосування бази біометричних даних EURODAC для реалізації міграційної політики (Регламент Ради (ЄС) № 2725/2000, Регламент (ЄС) № 603/2013 та Регламент (ЄС) 2024/1358). Крім того, були опрацьовані рішення Європейського суду справедливості (C-291/12 - Michael Schwarz v Stadt Bochum 2013 р., C-205/21 - Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police) 2023 р., Case C-61/22 - RL v Landeshauptstadt Wiesbaden 2024 р., C-80/23 - Ministerstvo na vatreshnite raboti () and génétiques II 2024 р.) та наглядових органів держав-учасниць – Швеції, Голландії, Литви, Бельгії, Франції – стосовно оцінки правомірності обробки біометричних даних.

Результати та обговорення

Прикметник «біометричний» походить із грецької мови від слів: *bio* – життя, *metrikos* – вимірювати; в українській мові – його значення стосується біометрії [22]. Водночас сам термін «біометрія» може вживатися в різних розуміннях (англ. *biometrics*), насамперед:

- біологічної статистики («розділу біології, змістом якого є планування і обробка результатів кількісних експериментів та спостережень методами математичної статистики» [23]);
- сфери знань про використання біологічних даних для розпізнавання осіб («науки про розпізнавання особи завдяки її фізичним або поведінковим характеристикам, таким як обличчя, відбитки пальців, голос та райдужна оболонка ока» [21]) або методики розпізнавання, в основі якої лежить застосування спеціальних засобів – біометричних технологій (за Кембриджським словником – «використання детальної інформації про тіло людини, наприклад, про особливості кольору її очей, для підтвердження її особи» [24]).

Ми також відзначаємо доволі рідкісне вживання слова «біометрії» – як множинної форми – для позначення самих біометричних даних («біометрії – це біологічні характеристики особи, такі як, обличчя або відбитки пальців, які можуть використовуватися для підтвердження її особи» [25]).

Поняття біометричних систем та технологій

Визнаючи те, що поняття технологій та систем як складові термінів «біометричні технології» та «біометричні системи» відповідно, залишається предметом наукових дискусій, ми пропонуємо під біометричними технологіями розуміти вид технологій, які обробляють біометричні дані для розпізнавання особи. Водночас під розпізнаванням маємо на увазі не тільки визначення, ким є особа, а й виконання інших подібних завдань, що стосуються встановлення певної відповідності між біометричними даними – тими, які вже були раніше збереженими в біометричній системі, та тими, які щойно були введені для розпізнавання. Крім того, біометричні технології можуть у поєднанні зі штучним інтелектом визначати належність особи до певної категорії за окремою характеристикою, у такому разі – зіставлення не відбувається.

Вважаємо ключовою ознакою біометричних систем і технологій зв'язок із біометричними даними – сталими та унікальними характеристиками людини як біологічної істоти, добре відомими прикладами яких є відбитки пальців та зображення обличчя.

Серед визначень біометричних технологій, які існують у світовій науці, – можемо запропонувати такі: «автоматизовані методи розпізнавання або перевірки особи живої людини на базі фізіологічних або поведінкових характеристик» [26], «технології, які вимірюють та накопичують дані, а також можуть аналізувати фізіологічні або поведінкові характеристики людини» [27]. При цьому помічаємо, що здебільшого для наявних розумінь біометричних технологій характерний наголос на розпізнавальному аспекті, тоді як

поза увагою залишається важлива передумова розпізнавання – перетворення біологічної характеристики у дані машиночитаного формату («на відміну від того, як у біометричних науках тіло стає пізнаваним, біометрія генерує тіло, яке можна пізнавати: вона перетворює поверхні та характеристики тіла на цифрові коди та шифри, придатні для машиночитання» [28]).

Зауважимо, що в науковій літературі також дуже часто зустрічаємо термін «біометричні системи», відмінність якого від «біометричних технологій» полягає у співвідношенні понять системи та технології (біометрична система: «система, яка дозволяє розпізнавати певну характеристику особи за допомогою математичних алгоритмів і біометричних даних» [29]; «система, в якій будь-яка частина тіла може бути розпізнана за її біометричними даними, які зберігаються в базі даних і розпізнаються на основі матриць» [30]; «система розпізнавання зразків, яка працює шляхом отримання біометричних даних від особи за допомогою датчика, вилучення набору ознак із отриманих даних та порівняння цього набору ознак із шаблонами, збереженими в базі даних» [31]; «система розпізнавання зразків, яка визначає особу на основі вектора ознак, отриманого з певних фізіологічних або поведінкових характеристик, притаманних цій особі» [32]). На нашу думку, під біометричною системою слід розуміти інформаційну систему, яка завдяки перетворенню біологічних характеристик особи в машиночитану форму та їхнього подальшого аналізу, встановлює відповідність між біометричними даними, тим самим сприяючи розпізнаванню особи, а також визначає належність особи до певної категорії.

Функції біометричних систем та технологій

У технічній літературі як звичайно виокремлюють дві функції, які можуть виконувати технічні засоби щодо біометричних даних: верифікацію (або автентифікацію) та ідентифікацію (режим верифікації: користувач стверджує, що він є тим, за кого себе видає, а система, своєю чергою, «приймає або відхиляє це твердження» в результаті порівняння його характеристик з тими, що зберігаються в базі даних; режим ідентифікації: біометрична система отримує характеристики користувача та порівнює їх із тими, що вже зберігаються в базі даних, щоб визначити, ким він є серед усіх зареєстрованих користувачів [33]).

Отже, біометричні системи та технології можуть виконувати таку функцію, як визначення особи, тобто ідентифікації, коли працівники правоохоронних органів здійснюють пошук імовірного злочинця за наявними біометричними даними, а також перевірку особи – верифікацію (скажімо, при посадці на літак чи зверненні для отримання статусу біженця). Ми також зустрічаємо близьке за значенням до верифікації поняття аутентифікації, що часто

застосовується для позначення процедури доступу до інформаційних систем та технічних засобів серед іншого – на підставі біологічних характеристик (альтернативними є паролі, PIN-коди і т. ін.).

У поясненнях Робочої групи зі статті 29 (попередниці Європейської ради із захисту даних, яка до 2018 р. була незалежним дорадчим органом ЄС із питань приватності та персональних даних) біометрична ідентифікація та біометрична верифікація (або автентифікація) показані як споріднені функції з дещо різними завданнями. У першому випадку біометрична система встановлює, чи є ця біометрична характеристика відомою базі даних, а отже, можна з'ясувати – ким є фізична особа («ідентифікація особи за допомогою біометричної системи зазвичай є процесом порівняння біометричних даних особи (отриманих для ідентифікації) з низкою біометричних шаблонів, що зберігаються в базі даних, тобто відбувається процес зіставлення “один до багатьох”»). У другому випадку – чи є ця характеристика тією самою, яку вже раніше біометрична система запам'ятала («верифікація особи за допомогою біометричної системи, як правило, є процесом порівняння біометричних даних особи (отриманих під час верифікації) з одним біометричним шаблоном, що зберігається на пристрої, – цей процес характеризує зіставлення “один до одного”» [34]).

У результаті зіставлення біометричної ідентифікації та верифікації можемо дійти переконання, що перша з функцій – визначення особи – незважаючи на незрівнянні нові можливості, несе більші ризики та загрози у правовій площині для захисту прав людини, ніж перевірка особи. По-перше, відбувається порівняння біометричних даних великої кількості осіб, а не просто встановлення відповідності того, що біологічні характеристики однієї особи такі самі; по-друге, обробка даних, забезпечувана через інтерактивну інформаційну систему, тобто її застосування не обмежується підприємством, яке контролює допуск працівників за відбитками пальців. З цього випливає, що здійснення біометричної ідентифікації потребує особливого контролю за інформаційною безпекою в контексті правової охорони безпеки баз даних та унеможливлення несанкціонованого втручання у відповідні інформаційні системи. Ми також наголошуємо, що процедура біометричної верифікації, як правило, є наслідком попередньої згоди особи, котра надає свої біометричні характеристики для подальшого використання з певною метою (наприклад, користувач телефону зберігає відбиток пальця для того, щоб надалі отримувати доступ). Натомість, при біометричній ідентифікації часто виникають спірні ситуації, коли особа цілком аргументовано заявляє про неправомірність збору та зберігання її біометричних даних (приклади із правозастосовної практики розглянемо далі).

Ще одна функція, яку виконують біометричні технології та системи, полягає у визначенні належності особи до якоїсь групи за окремою характеристикою, тобто встановленні відповідності того, що вона є такою ж, як й інші відповідно до віку, статі чи етносу (таку біометрію часто називають «м'якою» [35]). Проте значною мірою ця функція забезпечується штучним інтелектом, тоді як роль біометричної системи насамперед у тому, щоб отримати потрібну характеристику та перетворити її у дані машиночитаного формату.

Критерії класифікації та нові можливості біометрії

На нашу думку, класифікувати біометричні системи та технології доцільно відповідно до таких критеріїв.

А. Вид використовуваної біологічної характеристики. Додатково до «традиційних» відбитків пальців застосовують унікальні візерунки райдужної оболонки ока, геометрію руки (довжину пальців і відстань між суглобами), риси обличчя, унікальні голосові ознаки, такі як висота і тон голосу, а також новітні засоби розпізнавання – малюнок вен, ДНК, запах, нігтьове ложе, ходу, форму вуха тощо [36]. Окремі вчення називають розширення біологічних характеристик для розпізнавання біометричними системами та технологіями «другим поколінням» біометрії [20].

Б. Кількість використовуваних характеристик. З одного боку, такі системи та технології можуть базуватися на біометричних даних одного виду – достатньо відбитків пальців для того, щоб визначити особу. Водночас сьогодні дедалі частіше застосовують мультимодальність як поєднання кількох біологічних характеристик (наприклад, сигналу електрокардіограми та відбитків пальців [37]). Такий підхід є цілком виправданим за умов, коли ціна помилки є високою.

В. Необхідність фізичного контакту (та можливість дистанційного розпізнавання). На сучасному етапі новітні розробки роблять можливим визначення особи на відстані, без будь-якого фізичного контакту [38]. З одного боку, такі технології вирішують проблему небажання багатьох людей проходити технічні процедури, з іншого боку, їхнє застосування породжує етично-правові дискусії стосовно відсутності згоди, порушення права на невтручання у приватне життя та відеоспостереження у громадських місцях.

Г. Сфери застосування. Біометричні системи та технології застосовуються як у діяльності органів державної влади (прикордонний контроль, боротьба зі злочинністю, охорона здоров'я), так і приватними компаніями (контроль допуску працівників, фінансові та банківські операції). Слід відзначити, що біометрія є широко використовуваною в Інтернеті речей та управлінні персональними гаджетами.

Біометричні розробки швидко розвиваються та можуть виконувати нові й нові завдання («сфера застосування біометричних технологій розширилась за межі безпекових завдань, все частіше включає комерційні та цивільні цілі» [39]). Так, біометрія, що базується на відстеженні руху очей, лежить в основі моніторингу для виявлення втоми водія для підвищення безпеки дорожнього руху, а також сприяння взаємодії особи з інвалідністю з технічним пристроєм [29].

Основою правового регулювання біометричних систем та технологій є законодавство про захист персональних даних, відповідно до якого біометричним даним як об'єктам обробки гарантована посилена охорона. Вона виявляється в тому, що біометричні дані кваліфікують як «чутливі» персональні дані, а отже, щодо їх збору, зберігання та використання в деяких аспектах законодавець визначає більш жорсткі рамки. Крім Загального регламенту про захист даних, розглянемо й інші акти законодавства для впровадження біометрії на прикладі права ЄС як орієнтиру для українського законодавця.

Використання біометричних технологій у законодавстві ЄС

Директива 95/46/ЄС [40], що визначала правові основи захисту персональних даних в ЄС перед набуттям чинності Загальним регламентом про захист даних, не містить жодних спеціальних положень щодо біометричних даних. Водночас присвячена обробці особливих категорій даних ст. 8 не виокремлює біометричних даних, хоча й у ній згадані дані, що стосуються здоров'я чи статевого життя людини, а також дані, які вказують на расове чи етнічне походження. Важливу роль для обробки біометричних даних згідно з Директивою відігравали: ст. 6 (принципи щодо якості даних), ст. 7 (критерії законності), ст. 17 (права суб'єктів даних).

Важливою частиною права ЄС у середині 2000-х рр. стали правила, які стосуються використання біометрії для паспортів та проїзних документів, насамперед Регламенту Ради (ЄС) № 2252/2004 про стандарти для захисних елементів і біометричних даних у паспортах і проїзних документах, які видають держави – учасниці ЄС [41]. З одного боку, його положення конкретизують мету обробки біометричних даних у вигляді перевірки справжності документа та верифікації особи пред'явника. Суб'єкт даних може вивірити персональні дані та вимагати їхнього виправлення або навіть видалення. З іншого боку, встановлені високі стандарти захисту від підробки та безпеки даних (надійний чіп для збереження зображення обличчя та двох відбитків пальців). У Регламенті використаний термін «біометричний ідентифікатор» (його пояснюють так: «персональні дані, отримані в результаті спеціальної технічної обробки, що стосуються фізичних, фізіологічних або поведінкових

характеристик особи, які дозволяють або підтверджують унікальну ідентифікацію цієї особи, наприклад, зображення обличчя або дані відбитків пальців» [42]). Регламент (ЄС) № 444/2009 удосконалив попередні положення, які скасовують загальне зобов'язання щодо збору та зберігання відбитків пальців дітей до 6 років, а також установив правило: «одна людина – один паспорт» для неповнолітніх [43].

Регламент (ЄС) № 2019/1157 спрямований на стандартизацію посвідчень особи (ID-карток) для громадян ЄС з метою захисту від підробок та шахрайства через запровадження біометричних ідентифікаторів [44]. У багатьох аспектах положення Регламенту (ЄС) № 2019/1157 перегукуються з Регламентом Ради (ЄС) № 2252/2004, адже в обидвох випадках ідеться про забезпечення підтвердження особи, проте дещо різними засобами [45]. В основі виданих державами-членами посвідчень особи повинен лежати добре захищений носій інформації, який містить біометричні дані, у вигляді зображення обличчя та відбитків пальців, збір яких здійснює кваліфікований та уповноважений персонал (ст. 10). Підкреслена необхідність збору, зберігання та використання біометричних даних відповідно до законодавства про захист персональних даних, гарантуючи безпеку, цілісність, автентичність та конфіденційність даних (ст. 11).

Порядок впровадження у 2025–2026 рр. – період з 12 жовтня 2025 р. до 10 квітня 2026 р. – прикордонного контролю за допомогою біометричних технологій для громадян України та інших держав, які не є членами ЄС, при в'їзді на територію Шенгенської зони та виїзді з неї, визначається Регламентом (ЄС) № 2017/2226 про Систему в'їзду/виїзду (далі – EES) для реєстрації відповідних даних та умови доступу правоохоронних органів до EES [46]. Регламент (ЄС) № 2025/1534 [47] дає можливість державам застосувати гнучкий підхід та реалізовувати визначені нововведення поступово.

EES призначена для виконання низки завдань:

- 1) модернізувати управління кордонами в державах ЄС (шляхом електронної реєстрації в'їзду та виїзду громадян держав, що не входять до ЄС, або відмов у в'їзді);
- 2) підвищувати ефективність прикордонних перевірок, унаслідок чого в осіб, які подорожують, враження від прикордонного контролю будуть кращими;
- 3) сприяти ефективній боротьбі зі шахрайством стосовно персональних даних внаслідок збирання біометричних даних;
- 4) сприяти зміцненню безпеки в ЄС через протидію тероризму та організованих злочинності [42].

Нова біометрична система прикордонного контролю має низку особливостей, узагальнених нами на основі опрацювання [48–50]:

- база даних складається з біометричних ідентифікаторів відбитків пальців та фотографій обличчя;
- для реєстрації в базі перед першим перетином кордону особою, яка подорожує, потрібно пройти комплексну процедуру, водночас у подальшому щодо неї буде здійснюватися швидке автоматизоване розпізнавання;
- біометрична ідентифікація запроваджується для тих осіб, які перебуватимуть на території Шенгенської зони короткостроково (до 90 днів протягом 180-денного періоду);
- процедура поки не має альтернатив (у вигляді, наприклад, ручного проставлення штампів у паспортах), тобто відмова від біометричної ідентифікації має своїм наслідком заборону в'їзду;
- біометрична ідентифікація застосовується на зовнішніх кордонах держав – учасниць ЄС, зокрема при виїзді осіб, яким надано тимчасовий захист (запроваджений для українців Імплементативним рішенням Ради 2022/382, див. [51, с. 166–170]), та які не є громадянами держав-учасниць;
- біометричні дані збираються в осіб віком від 12 років, крім того, визначені строки їх зберігання, що свідчить про відповідність положенням Загального регламенту про захист даних;
- у певних випадках, визначених Регламентом 2017/2226, доступ до EES мають правоохоронні органи.

Тривалий час ЄС використовує інформаційну систему EURODAC, введenu на початку 2000-х Регламентом Ради (ЄС) № 2725/2000 [52]. Ідея EURODAC полягала в тому, щоб з метою виконання положень Дублінської конвенції сформувати єдину базу з відбитками пальців шукачів притулку, завдяки якій можна було визначати ту державу, яка повинна розглядати конкретну заявку. У Регламенті Ради вказано, яка саме інформація підлягала збору, а також обмежено строк зберігання даних до 10 років (або до моменту набуття шукачем притулку громадянства держави – учасниці ЄС), після чого дані мали бути негайно знищені (ст. 5-7). Варто зауважити, що Регламент (ЄС) № 603/2013 [53] вдосконалив попередній та розширив можливості EURODAC за рахунок використання для потреб правоохоронної діяльності як помічного засобу у запобіганні, виявленні та розслідуванні тероризму та інших найбільш небезпечних кримінальних правопорушень. Сьогодні держави, взявши відбитки пальців у шукачів притулку та нелегальних мігрантів (віком від 14 років), повинні впродовж 72 год передати

їх у EURODAC. Своєю чергою, завдяки системі встановлюється відповідність нового зразка біометричних даних та вже наявних, а далі – приймається аргументоване рішення про долю особи. Використання EURODAC правоохоронними органами допустиме лише за наявності достатніх підстав вважати, що це істотно сприятиме забезпеченню потреб правоохоронної діяльності, а також – за умови, що не існує інших можливих засобів з меншим рівнем втручання. Наступного року має набути чинності Регламент (ЄС) № 2024/1358 [54], який істотно змінить положення Регламенту (ЄС) № 603/2013 (серед іншого – EURODAC буде застосовуватися ширше – не тільки для справ біженців, а й реалізації інших складових міграційної політики, так само визначені додаткові біометричні ідентифікатори для застосування).

Загальний регламент про захист даних (Регламент (ЄС) № 2016/679 [55]) – ст. 9 – у цілому забороняє обробку «спеціальних категорій» персональних даних, до яких, на відміну від положень попередньої Директиви – 95/46/ЄС – прямо включені й біометричні (а також генетичні) дані. Водночас наведено декілька випадків, коли така обробка можлива як виняток (насамперед – виразна згода, крім неї – виконання юридичних зобов'язань, захист життєво важливих інтересів, забезпечення суспільного інтересу та ін.). Ми відзначаємо те, що збір, зберігання та використання біометричних даних будь-яким способом, з одного боку, підпорядковується загальним положенням про захист персональних даних, зокрема визначеним у ст. 32 обов'язком контролера та оператора даних вживати необхідні технічні та організаційні заходи для безпеки даних, а також не допускати несанкціонованого доступу. З іншого боку, законодавство ЄС посилює правову охорону біометричних даних як «чутливих», порівнюючи з персональними даними, які не належать до «чутливих». Зауважимо, що в Директиві (ЄС) № 2016/680 [56], що відома як Директива про правоохоронну діяльність, загальна підстава для обробки біометричних даних з метою однозначної ідентифікації особи визначена як «сувора необхідність» (ст. 10).

Оскільки для здійснення біометричної ідентифікації та реалізації інших функцій біометрії дедалі частіше застосовують технології штучного інтелекту, зокрема, для виявлення приналежності, то основи правового регулювання біометричних технологій також формує законодавство у сфері штучного інтелекту, яке в загальному масштабі перебуває на стадії зародження. Закон ЄС про штучний інтелект (Регламент (ЄС) 2024/1689 [57]), в якому, окрім вже згаданих нами функцій ідентифікації, верифікації, категоризації, названо ще одну – розпізнавання емоцій, здійснювану системами штучного інтелекту, призначеними для ідентифікації або визначення емоцій

чи намірів особи на основі її біометричних даних, розмежовує системи штучного інтелекту, які обробляють біометричні дані, за критерієм безпеки. Через неприйнятний ризик забороняється застосування штучного інтелекту для таких завдань (ст. 5): біометричної категоризації, в результаті якої відбувається автоматизоване виведення висновків, що стосуються «чутливих» даних про особу (наприклад, завдяки аналізу зображення обличчя штучний інтелект відносить особу до етнічної групи), розпізнавання емоцій у сфері праці та освіти, створення або розширення баз даних для розпізнавання обличчя шляхом необмеженого скрейпінгу в Інтернеті, а також – дистанційної біометричної ідентифікації у режимі реального часу, що здійснюється у громадських місцях для потреб правоохоронної діяльності (щодо останнього випадку Закон допускає винятки за наявності чітко визначених умов). Слід додати, що велика кількість застосувань біометричних технологій належать до тих, що становлять високий ризик, їхнє впровадження дозволено, якщо будуть вжиті необхідні заходи для недопущення можливого негативного впливу (ст. 16).

Правозастосовна практика наглядових органів із захисту даних та Європейського суду справедливості

Однією з найвідоміших справ останніх років щодо біометрії у правозастосовній практиці Європейського суду справедливості є запит про попереднє рішення (*RL v Landeshauptstadt Wiesbaden*, 2024 р. [58]) стосовно оскарження відмови у видачі посвідчення особи громадянину Німеччини через те, що той не надав відбитків пальців (як це передбачено згаданим вище Регламентом (ЄС) 2019/1157). Серед аргументації – невідповідність правилам щодо захисту персональних даних. Водночас Суд, підтверджуючи те, що Регламент (ЄС) 2019/1157 був прийнятний із порушенням процедури відповідно до Договору про функціонування Європейського Союзу, а через те – за деякий час його дію потрібно припинити, не виявив порушень у сфері захисту персональних даних. Обмеження принципу поваги до приватного та сімейного життя (ст. 7 Хартії основних прав Європейського Союзу) та на захист персональних даних (ст. 8) було цілком виправданим, за оцінками Суду, положеннями ст. 52, в яких ідеться про принцип пропорційності та міркування громадської безпеки як загальносупільного інтересу. Крім того, у рішенні наголошено, що біометричні дані підлягають обробці як необхідний захід боротьби з шахрайством (підrobкою документів та крадіжкою особистих даних).

Схожі питання порушувались при вивченні Європейським судом справи за іншим запитом про попереднє рішення – від Адміністративного суду

Гельзенкірхена – *Michael Schwarz v Stadt Bochum* (2013) [59]. Німецькому громадянину було відмовлено у видачі паспорта без збору його біометричних даних – відбитків пальців, виходячи з дії Регламенту Ради (ЄС) № 2252/2004. Крім апелювання до порушень загальновизнаних принципів у сфері прав людини, а також недотримання вже згаданої нами Директиви 95/46/ЄС про захист персональних даних, як і вимоги пропорційності, на думку скажника, сам Регламент не має під собою належного правового обґрунтування. Водночас, згідно з судовою оцінкою, положення Регламенту схарактеризовані як цілком правомірні: з одного боку, збір персональних даних у вигляді відбитків пальців кваліфікований як обробка персональних даних, з іншого боку, він проводиться для того, щоб запобігти підробці та не може бути заміненим іншими заходами.

Ще дві справи стосуються болгарської правозастосовної практики [60; 61]. У справі С-118/22 щодо керівника Головного управління Національної поліції Міністерства внутрішніх справ Болгарії Суд дійшов висновку, що безстрокове та невибіркове зберігання біометричних (та генетичних) даних осіб – відбитків пальців, фотографій та зразків ДНК – не відповідає праву ЄС. Як виявилось, за болгарським законодавством дані засуджених не підлягають видаленню з бази даних навіть після погашення судимості. Таку практику, за оцінками Суду, слід вдосконалити – правило щодо збору та зберігання даних абсолютно усіх засуджених до їхньої смерті є не виправданим, так само недоречним є те, що суб'єкт даних не наділений правом вимагати знищення своїх біометричних даних [61].

У справі С-205/21 Суд розглядав заперечення проти збору біометричних даних, обов'язкового для усіх осіб, котрі обвинувачуються у вчиненні навмисних кримінальних правопорушень. Предметом особливого вивчення, як і в попередньому випадку, стали положення Директиви (ЄС) 2016/68. Встановлено, що вимоги болгарського законодавства не враховують правило пропорційності – наскільки всезагальний збір біометричних даних необхідний для досягнення поставлених цілей правоохоронної діяльності, та чи не є він надмірним у кожному можливому випадку [60].

На завершення огляду правозастосовної практики наводимо окремі рішення наглядових органів держав – учасниць ЄС зі захисту даних, які стосуються теми нашого дослідження та були прийняті у період 2019–2024 рр.

Шведський орган із захисту даних у 2019 р. оштрафував на 20 тис. євро муніципалітет за встановлення в рамках експериментального проєкту системи розпізнавання облич у школі з метою контролю відвідування. Хоча біометрична верифікація здійснювалась за згоди батьків учнів, наглядо-

вий орган відзначив те, що існували методи з меншим рівнем втручання у приватне життя, а також підкреслив, що надана згода була певною мірою вимушеною, а оцінка можливого впливу не була проведена заздалегідь [62].

Нідерландський орган оштрафував підприємство на 750 тис. євро за незаконну обробку персональних даних співробітників – їхніх відбитків пальців – при контролі за перебуванням на робочому місці та обліком робочого часу. У рішенні 2020 р. вказано, що безпекові міркування не обґрунтовують таку обробку та відзначений їй непропорційний характер. Крім того, згода, надана працівниками, схарактеризована наглядовим органом як така, що не була вільною, зокрема через те, що суб'єкти даних не були належним чином поінформовані [63].

Литовський орган, за результатами розслідування скарги щодо обов'язкового сканування відбитків пальців клієнтів спортивного клубу як єдиного можливого методу ідентифікації, прийняв рішення про порушення низки положень Загального регламенту, включаючи те, що згода не була надана вільно, а компанія не провела попередньої оцінки можливого впливу. Розмір накладеного штрафу – 20 тис. євро (2021 р.) [64].

Питання інформованої та вільної згоди стало ключових при прийнятті рішення Бельгійським органом із захисту даних у 2024 р. Збір відбитків пальців для системи обліку робочого часу, який проводився без належних правових підстав, а також їхня подальша обробка як біометричних даних на порушення принципів мінімізації даних та обмеження цілей були визнані порушенням у сфері захисту персональних даних, штраф – 45 тис. євро [65].

Останніми роками відразу в декількох державах органи із захисту даних розглядали скарги проти компанії Clearview AI, відомої своїм програмним забезпеченням на базі штучного інтелекту, яке дозволяє розпізнавати особу завдяки фотографії. В європейській практиці такі скарги були подані у Греції, Італії, Голландії, Франції та ін. Практично в усіх випадках наглядовий орган встановлював факт правопорушення та призначав штраф. За незаконну обробку персональних даних у супереч ст. 6 Загального регламенту, а також недотримання прав суб'єктів даних та відсутність співпраці Французький орган у 2022 р. оштрафував компанію на 20 млн євро [66].

Висновки

Виконуючи важливі для органів державної влади та приватних компаній функції, пов'язані з розпізнаванням осіб – завдяки перетворенню біологічних характеристик особи у машиночитаний формат та їх подальшому аналізу щодо встановлення певної відповідності, біометричні системи та технології

викликають етично-правові дилеми з приводу того, наскільки обґрунтованим є обмеження права на невтручання у приватне життя внаслідок збору, зберігання та використання біометричних даних задля забезпечення інтересів публічного характеру або й в інших випадках, коли суб'єкт даних не надав виразної згоди. Як показують результати дослідження, для вирішення цих дилем слід урахувувати, що біометричні системи та технології з їхніми незрівнянними можливостями не мають високорезультативних альтернатив у з'ясуванні того, ким є особа. Крім того, ми відзначаємо, що серед них є такі, які обробляють біометричні дані більш-менш узгоджено з волею суб'єкта даних, підтверджуючи особу (управління гаджетами та Інтернет речей); ті, що не сприяють визначенню особи, а лише категоризують наявні біологічні характеристики – вони є відносно безпечними, якщо не виводять «чутливі» дані; а також – призначені для біометричної ідентифікації – найменш прийнятні для населення, особливо коли функціонують віддалено та без зв'язку з потребою охорони суспільної безпеки. На прикладі законодавства ЄС можемо помітити, що правові рамки використання біометричних технологій визначають, по-перше, положення про захист персональних даних, що надають спеціальну охорону біометричним даним як «чутливим»; по-друге, про штучний інтелект, у поєднанні з яким сучасні біометричні системи та технології виходять на новий рівень точності та ефективності, порівняно з так званим «першим поколінням»; по-третє, особливості правового забезпечення галузевого впровадження біометричних технологій. Слід окремо відзначити правову охорону інформаційної безпеки та захищеності не тільки баз даних, а й самих біометричних систем та технологій.

Список використаних джерел

- [1] Бердиченко І. О. Удосконалення правових процедур біометричної ідентифікації та верифікації особи. *VIII Юридичні могилянські читання* : програма та тези Всеукр. наук.-практ. конф. Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2023. С. 9–13. URL: https://chmnu.edu.ua/wp-content/uploads/Mogilyanski_chitannya_-_2023.pdf (дата звернення: 10.10.2025).
- [2] Бойко А. М. Межі правомірного обігу біометричних персональних даних за законодавством України. *Правові новели*. 2020. Вип. 10. С. 142–146. <https://doi.org/10.32847/ln.2020.10.20>.
- [3] Бойко А. Захист біометричних персональних даних Уповноваженим Верховної Ради України з прав людини. *Юридичний науковий електронний журнал*. 2021. № 2. С. 160–163. <https://doi.org/10.32782/2524-0374/2021-2/37>.
- [4] Мартинова А. Адміністративно-правове забезпечення обігу та захисту біометричних персональних даних : дис. ... д-ра філософії : 081. Київ, 2022. 165 с.
- [5] Бригинець С. Біометричні дані: збір і захист у Європі, США та Україні. *Юридична газета*. 2019. № 40(694). URL: <https://yur-gazeta.com/publications/practice/inshe/biometrichni-dani-zbir-i-zahist-u-evropi-ssha-ta-ukrayini.html> (дата звернення: 10.10.2025).

- [6] Бродкевич В., Гуцалюк М. Біометрія та захист основних прав людини. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2010. № 23. С. 293–301.
- [7] Дубонос К. В. Нормативно-правове регулювання використання баз біометричних даних в Україні. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція*. 2019. № 41, т. 2. С. 99–102. <https://doi.org/10.32841/2307-1745.2019.41-2.22>
- [8] Дубонос К. Використання баз біометричних даних підрозділів експертної служби МВС України під час розслідування кримінальних правопорушень : дис. ... д-ра філософії : 081. Київ, 2021. 286 с.
- [9] Романов В., Галелюка І., Галелюка О. На часі – біометрична ідентифікація особи в Україні. *Світогляд*. 2010. № 6. С. 42–45. URL: https://www.mao.kiev.ua/biblio/jscans/svitoglyad/svit-2010-26-6/svit-2010-26-6-42-romanov_galelyuka.pdf (дата звернення: 10.10.2025).
- [10] Стефанчук М. Перспективи адаптації законодавства України до стандартів Європейського Союзу у сфері правового регулювання ідентифікації фізичної особи. *Право України*. 2017. № 8. С. 173–181.
- [11] Тарасевич Т. Ю. Правове регулювання біометричної ідентифікації особи: національні тенденції та зарубіжний досвід. *Часопис Київського університету права*. 2021. № 2. С. 281–286. <https://doi.org/10.36695/2219-5521.2.2021.58>.
- [12] Щербак Я., Бзова Л. Зарубіжний досвід правового регулювання біометричної ідентифікації особи. *Наукові читання пам'яті Іанса Гросса* : зб. тез міжнар. наук.-практ. конф. (м. Чернівці, 9 груд. 2021 р.). Чернівці : Технодрук, 2021. С. 274–278.
- [13] Книженко С. О., Шарабан О. І. Дактилоскопічний облік в Україні: правове регулювання та тенденції розвитку. *Науковий вісник Ужгородського Національного Університету. Серія: Право*. 2023. Вип. 79, ч. 2. С. 237–242. <https://doi.org/10.24144/2307-3322.2023.79.2.36>.
- [14] Про ідентифікацію людини шляхом дактилоскопії : проект Закону України від 18.01.2012 р. № 9732. URL: <https://ips.ligazakon.net/document/JF71C00A?an=3>.
- [15] Про ідентифікацію людини шляхом дактилоскопії : проект Постанови про відхилення проекту Закону України від 11.05.2012 р. URL: https://w2.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=43345 (дата звернення: 10.10.2025).
- [16] Захаров В., Рудешко В. Біометричні технології в ХХІ столітті та їх використання правоохоронними органами : посібник. Львів : ЛьвДУВС, 2015. 492 с.
- [17] Михайлик А. Захист персональних даних працівників в умовах цифрової трансформації : дис. ... д-ра філософії : 081. Харків, 2023. 203 с.
- [18] Kindt E. Privacy and Data Protection Issues of Biometric Applications. *Law, Governance and Technology Series*. Vol. 12. Dordrecht : Springer, 2013. 975 p.
- [19] Biometric Recognition: Challenges and Opportunities / ed. by J. Pato, L. Millett. Washington : National Academies Press, 2010. 165 p.
- [20] Second Generation Biometrics : The Ethical, Legal and Social Context / ed. by E. Mordini, D. Tzovaras. Dordrecht : Springer, 2012. 334 p.
- [21] Handbook of Biometrics / ed. by A. Jain, P. Flynn, A. Ross. Boston : Springer, 2007. 556 p.
- [22] Біометричний. СЛОВНИК.ua. URL: <https://slovnyk.ua/index.php?swrd=біометричний> (дата звернення: 10.10.2025).

- [23] Біометрія. СЛОВНИК.ua. URL: <https://slovnkyk.ua/index.php?swrd=біометрія> (дата звернення: 10.10.2025).
- [24] Biometrics. Cambridge Dictionary. URL: <https://dictionary.cambridge.org/dictionary/english/biometrics> (last accessed: 10.10.2025).
- [25] Device security guidance. National Cyber Security Centre. URL: <https://www.ncsc.gov.uk/collection/device-security-guidance/policies-and-settings/using-biometrics> (last accessed: 10.10.2025).
- [26] Mordini E., Petrini C. Ethical and social implications of biometric identification technology. *Annali dell Istituto Superiore di Sanita*. 2007. Vol. 43, No. 1. P. 5–11.
- [27] Wayman J., Jain A., Maltoni D., Maio D. An Introduction to Biometric Authentication Systems. *Biometric Systems* / ed. by J. Wayman, A. Jain, D. Maltoni, D. Maio. London : Springer, 2005. P. 1–20.
- [28] Van der Ploeg I. The illegal body: ‘Eurodac’ and the politics of biometric identification. *Ethics and Information Technology*. 1999. Vol. 1. P. 295–302.
- [29] Guennouni S., Mansouri A., Ahaitouf A. Biometric Systems and Their Applications. *Visual Impairment and Blindness - What We Know and What We Have to Know* (pp. 1–12). London : IntechOpen, 2019. <https://doi.org/10.5772/intechopen.84845>.
- [30] Rajvanshi S., Chauhan S., Kaur S. A New Wave in Biometric System: Systematic Study. *CGC International Journal of Contemporary Technology and Research*. 2022. Vol. 4, issue 2. P. 300–305. <https://doi.org/10.46860/cgcijctr.2022.07.31.300>.
- [31] Pisani P. H., Mhenni A., Giot R., Cherrier E., Poh N., de Carvalho A.C., Rosenberger C., Essoukri Ben Amara N. Adaptive Biometric Systems: Review and Perspectives. *ACM Computing Surveys*. 2019. Vol. 52, issue 5, No. 102. P. 1–38. <https://doi.org/10.1145/3344255>.
- [32] Prabhakar S., Pankanti S., Jain A. Biometric Recognition: Security and Privacy Concerns. *IEEE Security and Privacy Magazine*. 2003. Vol. 1, issue 2. P. 33–42. <https://doi.org/10.1109/MSECP.2003.1193209>.
- [33] Luis-Garcia R., Alberola-Lopez C., Aghzout O., Ruiz-Alzola J. Biometric identification systems. *Signal Processing*. 2003. Vol. 83, issue 12. P. 2539–2557. <https://doi.org/10.1016/j.sigpro.2003.08.001>.
- [34] Opinion 3/2012 on developments in biometric technologies. URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf (last accessed: 10.10.2025).
- [35] Kloppenburg S., van der Ploeg I. Securing Identities: Biometric Technologies and the Enactment of Human Bodily Differences. *Science as Culture*. 2020. Vol. 29, issue 1. P. 57–76. <https://doi.org/10.1080/09505431.2018.1519534>.
- [36] Rosenzweig P., Kochems A., Schwartz A. Biometric Technologies: Security, Legal, and Policy Implications. *Legal Memorandum*. 2004. No. 12. P. 1–10. URL: https://static.heritage.org/2004/pdf/lm_12.pdf (last accessed: 10.10.2025).
- [37] A. El-Rahman S., Alluhaidan A. S. Enhanced multimodal biometric recognition systems based on deep learning and traditional methods in smart environments. *PLoS ONE*. 2024. Vol. 19, issue 2, Article e0291084. <https://doi.org/10.1371/journal.pone.0291084>.
- [38] Handbook of Remote Biometrics for Surveillance and Security / ed. by M. Tistarelli, S. Li, R. Chellappa. London : Springer, 2009.
- [39] North-Samardzic A. Biometric Technology and Ethics: Beyond Security Applications. *Journal of Business Ethics*. 2020. Vol. 167(3). P. 433–450. <https://doi.org/10.1007/s10551-019-04143-6>.

- [40] Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних». URL: https://zakon.rada.gov.ua/laws/show/994_242#Text (дата звернення: 10.10.2025).
- [41] Council Regulation (EC) No. 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States. URL: <https://eur-lex.europa.eu/eli/reg/2004/2252/oj/eng> (last accessed: 10.10.2025).
- [42] Integration of biometric features in passports and travel documents. URL: <https://eur-lex.europa.eu/EN/legal-content/summary/integration-of-biometric-features-in-passports-and-travel-documents.html> (last accessed: 10.10.2025).
- [43] Regulation (EC) No. 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No. 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States. URL: <https://eur-lex.europa.eu/eli/reg/2009/444/oj/eng> (last accessed: 10.10.2025).
- [44] Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement. URL: <https://eur-lex.europa.eu/eli/reg/2019/1157/oj/eng> (last accessed: 10.10.2025).
- [45] Lang A. Of Biometric Documents, Databases and Free Movement of Persons in the EU. *EU and Comparative Law Issues and Challenges Series*. 2023. Vol. 7. P. 119–143. <https://doi.org/10.25234/eclic/28260>.
- [46] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES). URL: <https://eur-lex.europa.eu/eli/reg/2017/2226/oj> (last accessed: 10.10.2025).
- [47] Regulation (EU) 2025/1534 of the European Parliament and of the Council of 18 July 2025 on temporary derogations from certain provisions of Regulations (EU) 2017/2226 and (EU) 2016/399. URL: <http://data.europa.eu/eli/reg/2025/1534/oj> (last accessed: 10.10.2025).
- [48] Entry/Exit System (EES). URL: <https://travel-europe.europa.eu/ees/ltr> (last accessed: 10.10.2025).
- [49] Austin K. How will the EU's new border system work? 2025. URL: <https://www.bbc.com/news/articles/c39rkpe8mj2o> (last accessed: 10.10.2025).
- [50] Buckley J. Traveling to the European Union is about to get more complicated. Here's what you need to know. URL: <https://edition.cnn.com/2025/10/10/travel/eu-entry-exit-system-explained> (last accessed: 10.10.2025).
- [51] Гачкевич А. «Подвійні стандарти» тимчасового захисту втікачів від війни в Україні у міграційній політиці ЄС. *Медіафорум*. 2022. Т. 11. С. 162–179. <https://doi.org/10.31861/mediaforum.2022.11.162-179>.
- [52] Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention. URL: <https://eur-lex.europa.eu/eli/reg/2000/2725/oj/eng> (last accessed: 10.10.2025).
- [53] Regulation (EU) No. 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013. URL: <http://data.europa.eu/eli/reg/2013/603/oj> (last accessed: 10.10.2025).

- [54] Regulation (EU) 2024/1358 of the European Parliament and of the Council of 14 May 2024 on the establishment of ‘Eurodac’. URL: <https://eur-lex.europa.eu/eli/reg/2024/1358/oj> (last accessed: 10.10.2025).
- [55] 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. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> (last accessed: 10.10.2025).
- [56] Directive (EU) 2016/680 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 by competent authorities. URL: <https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng> (last accessed: 10.10.2025).
- [57] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> (last accessed: 10.10.2025).
- [58] C-61/22 - RL v Landeshauptstadt Wiesbaden. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62022CJ0061> (last accessed: 10.10.2025).
- [59] C-291/12 - Michael Schwarz v Stadt Bochum. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0291> (last accessed: 10.10.2025).
- [60] C-205/21 - Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police). URL: <https://curia.europa.eu/juris/liste.jsf?language=en&num=C-205/21> (last accessed: 10.10.2025).
- [61] C-118/22 - Direktor na Glavna direksia "Natsionalna politsia" pri MVR – Sofia. (2024). URL: <https://curia.europa.eu/juris/liste.jsf?num=C-118/22> (last accessed: 10.10.2025).
- [62] Facial recognition in school renders Sweden’s first GDPR fine. URL: https://www.edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_sv (last accessed: 10.10.2025).
- [63] Dutch DPA imposes fine on company using fingerprint technology for attendance and time registration. URL: <https://www.datenschutz-notizen.de/dutch-dpa-imposes-fine-on-company-using-fingerprint-technology-for-attendance-and-time-registration-4325764/> (last accessed: 10.10.2025).
- [64] Lithuanian DPA: Fine Imposed on a Sports Club for Infringements of the GDPR in Processing of Fingerprints of the Customers and Employees. URL: https://www.edpb.europa.eu/news/national-news/2021/lithuanian-dpa-fine-imposed-sports-club-infringements-gdpr-processing_en (last accessed: 10.10.2025).
- [65] Belgian watchdog ruling on consent sets employee biometrics use against GDPR. URL: <https://www.biometricupdate.com/202411/belgian-watchdog-ruling-on-consent-sets-employee-biometrics-use-against-gdpr> (last accessed: 10.10.2025).
- [66] The French SA fines Clearview AI EUR 20 million. URL: https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en (last accessed: 10.10.2025).

References

- [1] Berdychenko, I. (2023). Improving the legal procedures of biometric identification and verification of an individual. In *VIII Mohyla Legal Readings: All-Ukrainian Scien. and Practical Conf. M* (Program and abstracts, pp. 9-13). Mykolaiv: Publishing House of Petro Mohyla National University of Kyiv. Retrieved from https://chmnu.edu.ua/wp-content/uploads/Mogilyanski_chitannya_-_2023.pdf.

- [2] Boiko, A.M. (2020). Boundaries of lawful circulation of biometric personal data under the legislation of Ukraine. *Legal Novels*, 10, 142-146. <https://doi.org/10.32847/ln.2020.10.20>.
- [3] Boiko, A. (2021). Protection of Biometric Personal Data by the Commissioner of the Verkhovna Rada of Ukraine for Human Rights. *Legal Scientific Electronic Journal*, 2, 160-163. <https://doi.org/10.32782/2524-0374/2021-2/37>.
- [4] Martynova, A. (2022). *Administrative and legal support for the circulation and protection of biometric personal data*. Ph.D. Thesis. Kyiv.
- [5] Bryhynets, S. (2019). Biometric data: collection and protection in Europe, the USA and Ukraine. *Legal Newspaper*, 40(694). Retrieved from <https://yur-gazeta.com/publications/practice/inshe/biometrichni-dani-zbir-i-zahist-u-evropi-ssha-ta-ukrayini.html>.
- [6] Brodkevych, V., & Hutsaliuk, M. (2010). Biometrics and protection of fundamental human rights. *Fight against Organized Crime and Corruption (Theory and Practice)*, 23, 293-301.
- [7] Dubonos, K. (2019). Statutory regulation of using biometric database of Ukraine. *Scientific Bulletin of the International Humanitarian University. Jurisprudence*, 41(2), 99-102. <https://doi.org/10.32841/2307-1745.2019.41-2.22>.
- [8] Dubonos, K. (2021). *The use of biometric databases of the expert service units of the Ministry of Internal Affairs of Ukraine during the investigation of criminal offenses*. Ph.D. Thesis. Kyiv.
- [9] Romanov, V., Haleliuka, I., & Haleliuka, O. (2010). Biometric identification of an individual in Ukraine is on time. *Worldview*, 6, 42-45. Retrieved from https://www.mao.kiev.ua/biblio/jscans/svitogliad/svit-2010-26-6/svit-2010-26-6-42-romanov_galelyuka.pdf.
- [10] Stefanchuk, M. (2017). Prospects for adapting Ukrainian legislation to European Union standards in the field of legal regulation of the identification of an individual. *Law of Ukraine*, 8, 173-181.
- [11] Tarasevych, T. (2021). Legal regulation of biometric identification: national trends and foreign experience. *Law Review of Kyiv University of Law*, 2, 281-286. <https://doi.org/10.36695/2219-5521.2.2021.58>.
- [12] Shcherbakova, Ya., & Bzova, L. (December 9, 2021). Foreign experience of legal regulation of biometric identification of a person. In *Scientific Readings in Memory of Hans Gross: Collection of abstracts* (pp. 274-278). Chernivtsi: Tekhnodruk.
- [13] Knizhenko, S.O., & Sharaban, O.I. (2023). Dactyloscopic accounting in Ukraine: legal regulation and development trends. *Scientific Bulletin of the Uzhhorod National University. Series: Law*, 79(2), 237-242. <https://doi.org/10.24144/2307-3322.2023.79.2.36>.
- [14] Draft law of Ukraine "On identification of a person by fingerprinting". (January 18, 2012). Retrieved from <https://ips.ligazakon.net/document/JF7IC00A?an=3>.
- [15] Draft resolution on the rejection of the Draft law of Ukraine "On identification of a person by fingerprinting". (May 11, 2012). Retrieved from https://w2.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=43345.
- [16] Zakharov, V., & Rudeshko, V. (2015) *Biometric technologies in the 21st century and their use by law enforcement agencies*. Lviv: Lviv State University of Internal Affairs.
- [17] Mykhailyk, A. (2023). *Protection of employees' personal data in the context of digital transformation*. Ph.D. Thesis. Kharkiv.
- [18] Kindt, E. (2013). Privacy and Data Protection Issues of Biometric Applications. *Law, Governance and Technology Series*, 12. Dordrecht: Springer.

- [19] Pato, J., & Millett, L. (Eds.). (2010). *Biometric Recognition: Challenges and Opportunities*. Washington: National Academies Press.
- [20] Mordini, E., & Tzovars, D. (Eds.). (2012). *Second Generation Biometrics: The Ethical, Legal and Social Context*. Dordrecht: Springer.
- [21] Jain, A., Flynn, P., & Ross, A. (Eds.). (2007). *Handbook of Biometrics*. Boston: Springer.
- [22] Biometric. In *Dictionary.ua*. Retrieved from <https://slovnyk.ua/index.php?sword=біометричний>.
- [23] Biometrics. In *Dictionary.ua*. Retrieved from <https://slovnyk.ua/index.php?sword=біометрія>.
- [24] Biometrics. In *Cambridge Dictionary*. (2025). Retrieved from <https://dictionary.cambridge.org/dictionary/english/biometrics>.
- [25] Device security guidance. National Cyber Security Centre. (2021). Retrieved from <https://www.ncsc.gov.uk/collection/device-security-guidance/policies-and-settings/using-biometrics>.
- [26] Mordini, E., Petrini, C. (2007). Ethical and social implications of biometric identification technology. *Annali dell Istituto Superiore di Sanita*, 43(1), 5-11.
- [27] Wayman, J., Jain, A., Maltoni, D., & Maio, D. (2005). An Introduction to Biometric Authentication Systems. In Wayman, J., Jain, A., Maltoni, D., Maio, D. (Eds.). *Biometric Systems* (pp. 1-20). London: Springer.
- [28] Van der Ploeg, I. (1999). The illegal body: 'Eurodac' and the politics of biometric identification. *Ethics and Information Technology*, 1, 295-302.
- [29] Guennouni, S., Mansouri, A., & Ahaitouf, A. (2019). Biometric systems and their applications. In *Visual Impairment and Blindness - What We Know and What We Have to Know* (pp. 1-12). London: IntechOpen. <https://doi.org/10.5772/intechopen.84845>.
- [30] Rajvanshi, S., Chauhan, S., & Kaur, S. (2022). A New Wave in Biometric System: Systematic Study. *CGC International Journal of Contemporary Technology and Research*, 4(2), 300-305. <https://doi.org/10.46860/cgcijctr.2022.07.31.300>.
- [31] Pisani, P.H., Mhenni, A., Giot, R., Cherrier, E., Poh, N., de Carvalho, A.C., Rosenberger, C., & Essoukri Ben Amara, N. (2019). Adaptive Biometric Systems: Review and Perspectives. *ACM Computing Surveys*, 52(5(102)), 1-38. <https://doi.org/10.1145/3344255>.
- [32] Prabhakar, S., Pankanti, S., & Jain, A. (2003). Biometric Recognition: Security and Privacy Concerns. *IEEE Security and Privacy Magazine*, 1(2), 33-42. <https://doi.org/10.1109/MSECP.2003.1193209>.
- [33] Luis-Garcia, R., Alberola-Lopez, C., Aghzout, O., & Ruiz-Alzola, J. (2003). Biometric identification systems. *Signal Processing*, 83(12), 2539-2557. <https://doi.org/10.1016/j.sigpro.2003.08.001>.
- [34] Opinion 3/2012 on developments in biometric technologies. (2012). Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.
- [35] Kloppenburg, S., & van der Ploeg, I. (2020). Securing Identities: Biometric Technologies and the Enactment of Human Bodily Differences. *Science as Culture*, 29(1), 57-76. <https://doi.org/10.1080/09505431.2018.1519534>.
- [36] Rosenzweig, P., Kochems, A., & Schwartz, A. (2004). Biometric Technologies: Security, Legal, and Policy Implications. *Legal Memorandum*, 12, 1-10. Retrieved from https://static.heritage.org/2004/pdf/lm_12.pdf.

- [37] A. El-Rahman, S., & Alluhaidan, A.S. (2024). Enhanced multimodal biometric recognition systems based on deep learning and traditional methods in smart environments. *PLoS ONE*, 19(2), e0291084. <https://doi.org/10.1371/journal.pone.0291084>.
- [38] Tistarelli, M., Li, S., & Chellappa, R. (Eds.). (2009). *Handbook of Remote Biometrics for Surveillance and Security*. London: Springer.
- [39] North-Samardzic, A. (2020). Biometric Technology and Ethics: Beyond Security Applications. *Journal of Business Ethics*, 167(3), 433-450. <https://doi.org/10.1007/s10551-019-04143-6>.
- [40] Directive 95/46/EC of the European Parliament and of the Council "On the protection of individuals with regard to the processing of personal data and on the free movement of such data". (October 24, 1995). Retrieved from https://zakon.rada.gov.ua/laws/show/994_242#Text.
- [41] Council Regulation (EC) No. 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States. Retrieved from <https://eur-lex.europa.eu/eli/reg/2004/2252/oj/eng>.
- [42] Integration of biometric features in passports and travel documents. Retrieved from <https://eur-lex.europa.eu/EN/legal-content/summary/integration-of-biometric-features-in-passports-and-travel-documents.html>.
- [43] Regulation (EC) No. 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No. 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States. (2009). Retrieved from <https://eur-lex.europa.eu/eli/reg/2009/444/oj/eng>.
- [44] Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement. (2019). Retrieved from <https://eur-lex.europa.eu/eli/reg/2019/1157/oj/eng>.
- [45] Lang, A. (2023). Of Biometric Documents, Databases and Free Movement of Persons in the EU. *EU and Comparative Law Issues and Challenges Series*, 7, 119-143. <https://doi.org/10.25234/eclic/28260>.
- [46] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES). (2017). Retrieved from <https://eur-lex.europa.eu/eli/reg/2017/2226/oj>.
- [47] Regulation (EU) 2025/1534 of the European Parliament and of the Council of 18 July 2025 on temporary derogations from certain provisions of Regulations (EU) 2017/2226 and (EU) 2016/399. (2025). Retrieved from <http://data.europa.eu/eli/reg/2025/1534/oj>.
- [48] Entry/Exit System (EES). (2025). Retrieved from <https://travel-europe.europa.eu/ees/ltr>.
- [49] Austin, K. (2025). How will the EU's new border system work? Retrieved from <https://www.bbc.com/news/articles/c39rkpe8mj2o>.
- [50] Buckley, J. (2025). Traveling to the European Union is about to get more complicated. Here's what you need to know. Retrieved from <https://edition.cnn.com/2025/10/10/travel/eu-entry-exit-system-explained>.
- [51] Hachkevych, A. (2022). "Double standards" of temporary protection of refugees from the war in Ukraine in EU Migration Policy. *Mediaforum*, 11, 162-179. <https://doi.org/10.31861/mediaforum.2022.11.162-179>.

- [52] Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention. (2020). Retrieved from <https://eur-lex.europa.eu/eli/reg/2000/2725/oj/eng>.
- [53] Regulation (EU) No. 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013. (2013). Retrieved from <http://data.europa.eu/eli/reg/2013/603/oj>.
- [54] Regulation (EU) 2024/1358 of the European Parliament and of the Council of 14 May 2024 on the establishment of 'Eurodac'. (2024). Retrieved from <https://eur-lex.europa.eu/eli/reg/2024/1358/oj>.
- [55] 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. (2016). Retrieved from: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>.
- [56] Directive (EU) 2016/680 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 by competent authorities. (2016). Retrieved from: <https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng>.
- [57] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. (2024). Retrieved from <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>.
- [58] C-61/22-RL v Landeshauptstadt Wiesbaden. (2024). Retrieved from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62022CJ0061>.
- [59] C-291/12 - Michael Schwarz v Stadt Bochum. (2013). Retrieved from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0291>.
- [60] C-205/21 - Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police). (2023). Retrieved from <https://curia.europa.eu/juris/liste.jsf?language=en&num=C-205/21>.
- [61] C-118/22 - Direktor na Glavna direktsia "Natsionalna politsia" pri MVR – Sofia. (2024). Retrieved from <https://curia.europa.eu/juris/liste.jsf?num=C-118/22>.
- [62] Facial recognition in school renders Sweden's first GDPR fine. (2020). Retrieved from https://www.edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_sv.
- [63] Dutch DPA imposes fine on company using fingerprint technology for attendance and time registration. (2020). Retrieved from <https://www.datenschutz-notizen.de/dutch-dpa-imposes-fine-on-company-using-fingerprint-technology-for-attendance-and-time-registration-4325764/>.
- [64] Lithuanian DPA: Fine Imposed on a Sports Club for Infringements of the GDPR in Processing of Fingerprints of the Customers and Employees. (2021). Retrieved from https://www.edpb.europa.eu/news/national-news/2021/lithuanian-dpa-fine-imposed-sports-club-infringements-gdpr-processing_en.
- [65] Belgian watchdog ruling on consent sets employee biometrics use against GDPR. (2024). Retrieved from <https://www.biometricupdate.com/202411/belgian-watchdog-ruling-on-consent-sets-employee-biometrics-use-against-gdpr>.
- [66] The French SA fines Clearview AI EUR 20 million. (2022). Retrieved from https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en.

Андрій Олександрович Гачкевич

кандидат юридичних наук, доцент

доцент кафедри міжнародного та кримінального права

Навчально-науковий інститут права, психології та інноваційної освіти

Національного університету «Львівська політехніка»

79005, вул. Князя Романа, 1/3, Львів, Україна

e-mail: andrii.o.hachkevych@lpnu.ua

ORCID 0000-0002-8494-1937

Andrii O. Hachkevych

Ph.D. in Law, Assistant Professor

Assistant Professor of the Department of International and Criminal Law Institute for Law

Psychology and Innovative Education

Lviv Polytechnic National University

79005, 1/3 Kniazia Romana Str., Lviv, Ukraine

e-mail: andrii.o.hachkevych@lpnu.ua

ORCID 0000-0002-8494-1937

Рекомендоване цитування: Гачкевич А. О. Біометричні системи і технології: поняття, види, функції та основи регулювання у праві ЄС. *Проблеми законності*. 2025. Вип. 171. С. 279–304. <https://doi.org/10.21564/2414-990X.171.342740>.

Suggested Citation: Hachkevych, A.O. (2025). Biometric Systems and Technologies: Concepts, Types, Functions and Legal Fundamentals in EU Law. *Problems of Legality*, 171, 279-304. <https://doi.org/10.21564/2414-990X.171.342740>.

Статтю подано / Submitted: 31.10.2025

Доопрацьовано / Revised: 01.12.2025

Схвалено до друку / Accepted: 18.12.2025

Опубліковано / Published: 29.12.2025