УДК 342.9
DOI https://doi.org/10.24144/2788-6018.2024.05.75

ПРАВОВІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ УКРАЇНИ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ З УРАХУВАННЯМ ДОСВІДУ ОЛІМПІЙСЬКИХ ІГОР В ПАРИЖІ 2024 РОКУ

Діордіца І.В.,
доктор юридичних наук, професор,
професор кафедри приватного та публічного права,
Київський національний університет технологій та дизайну

Дараган О.В.,
аспірант кафедри конституційного,
адміністративного та фінансового права,
Академія праці, соціальних відносин і туризму

Соловйов А.С.,
аспірант кафедри конституційного,
адміністративного та фінансового права,
Академія праці, соціальних відносин і туризму

Діордіца І.В., Дараган О.В., Соловйов А.С. Правові аспекти забезпечення державної безпеки України за допомогою штучного інтелекту з урахуванням досвіду Олімпійських ігор в Парижі 2024 року.

У статті автори здійснили дослідження правових аспектів забезпечення державної безпеки України за допомогою штучного інтелекту з урахуванням досвіду Олімпійських ігор в Парижі 2024 року. Актуальність дослідження обумовлена зростанням викликів щодо застосування штучного інтелекту в суспільному житті та необхідністю дотримання права на приватність. Встановлено, що після тривалих обговорень технологію розпізнавання облич за допомогою штучного інтелекту на Олімпійських іграх у Парижі не було впроваджено. Обґрунтовано, що основними напрямками удосконалення чинного в Україні нормативного регулювання щодо використання штучного інтелекту та забезпечення приватності громадян, уникнення можливих порушень прав людини, є такі: у контексті впровадження технології розпізнавання облич важливо мати детальні правила, що регулюють обсяг і застосування заходів, а також надійні гарантії проти ризику зловживань і свавілля (потреба у правових гарантіях є значно більшою, коли йдеться про використання технології розпізнавання облич в реальному часі); обробка персональних даних при застосуванні технології розпізнавання обличчя має бути виправданою та потребує високого рівня обґрунтування; використання технології розпізнавання обличчя для криміналістичної ідентифікації підозрюваного за фотографіями та відео і, відповідно, використання технології розпізнавання обличчя в реальному часі для його розшуку та арешту повинно відповідати «нагальній суспільній потребі» та враховувати характер і тяжкість правопорушення. Доведено, що визначаючи реальні загрози державній безпеці України на сучасному етапі у контексті можливого впровадження технології розпізнавання облич важливо мати детальні правила, що регулюють обсяг і застосування заходів, а також надійні гарантії проти ризику зловживань і свавілля. Невідворотна необхідність у правових гарантіях щодо реалізації та захисту приватності громадян, особливо коли йдеться про використання технології розпізнавання облич в реальному часі, висновується зі змісту Стратегії забезпечення державної безпеки.

Ключові слова: державна безпека, національна безпека, штучний інтелект, інформаційна безпека, кібербезпека, розпізнання обличчя, право на приватність.

Diorditsa I., Daragan O., Soloviov A. Legal aspects of ensuring state Security of Ukraine with the help of artificial intelligence in the light of the experience of the Olympic Games in Paris 2024.

In this article, the authors research the legal aspects of ensuring the State security of Ukraine with the help of artificial intelligence, taking into account the experience of the Olympic Games in Paris in 2024. The relevance of the research is due to the growing challenges to the use of artificial intelligence in public life and the need to respect the right to privacy. It is established that after lengthy discussions, the technology of face

recognition using artificial intelligence was not introduced at the Olympic Games in Paris. It is substantiated that the main areas for improving the current regulatory framework in Ukraine for the use of artificial intelligence and ensuring the privacy of citizens and avoiding possible human rights violations are as follows: in the context of the introduction of face recognition technology, it is important to have detailed rules governing the scope and application of measures, as well as reliable safeguards against the risk of abuse and arbitrariness (the need for legal safeguards is much greater when it comes to the use of real-time face recognition technology); the processing of personal data in the application of face recognition technology must be justified and require a high level of justification; the use of face recognition technology for forensic identification of suspects. It is proved that when identifying real threats to the state security of Ukraine at the present stage in the context of the possible introduction of face recognition technology, it is important to have detailed rules governing the scope and application of measures, as well as reliable guarantees against the risk of abuse and arbitrariness. The inevitable need for legal guarantees for the implementation and protection of citizens' privacy, especially when it comes to the use of real-time face recognition technology, is derived from the content of the State Security Strategy.

Key words: state security, national security, artificial intelligence, information security, cybersecurity, face recognition, right to privacy.

Постановка проблеми. У квітні 2024 року Міжнародний олімпійський комітет (МОК) запустив свою комплексну стратегію щодо штучного інтелекту та спорту під назвою «The Olympic AI Agenda». Основна ідея полягає у тому, що штучний інтелект потрібно використовувати для підтримки, а не заміни продуктивності спортсмена [1].

Розробкою даного документа займалася група, яка була сформована із новаторів у сегменті ШІ, науковців, спортсменів і безпосередньо технологічних компаній.

Звертаємо увагу, що одним із ключових напрямів став захист спортсменів від булінгу та насильства в інтернеті, особливо спрямованого проти жінок у спорті.

Одночасно із реалізацією зазначеної вище стратегії МОК, із метою гарантування безпеки під час проведення Олімпійських ігор в Парижі, французький уряд уклав контракти з чотирма компаніями – Videtics, Orange Business, ChapsVision та Wintics.

Наріжним каменем впровадження технологій ШІ задля забезпечення безпеки Олімпійських ігор стала позиція низки правозахисних організацій щодо використання системи розпізнавання облич.

Так, 23 листопада 2022 року у французькій газеті Le Parisien було опубліковано статтю, в якій інформувалося про те, що уряд Франції відмовився від проєкту впровадження системи розпізнавання облич для підтримки заходів безпеки на Олімпійських іграх 2024 року в Парижі [2]. Однак, дебати про можливе впровадження систем розпізнавання облич під час Олімпійських ігор набули широкої дискусії, яка розділила політичних лідерів, науковців, новаторів сегменту ШІ щодо того, чи необхідно використовувати біометричні системи, керовані штучним інтелектом, для моніторингу громадських місць.

Стан опрацювання проблематики. В Україні чимало вчених займалися дослідженням окремих аспектів правового регулювання штучного інтелекту. Саме проблематика запровадження та використання штучного інтелекту як об'єкта правовідносин, його соціалізації та основоположних принципів його співвідношення щодо дотримання прав і свобод людини останнім часом ставали предметом дослідження правників із різних галузей юридичної науки. Так на рівні наукових робіт можемо відмітити праці К. Токаревої та Н Савлівої [3], Ю. Тюрі [4], О. Задихайла [5], О. Карпенка [6] та ін. Однак безпосередньо проблематика правових аспектів забезпечення державної безпеки України за допомогою штучного інтелекту з урахуванням досвіду Олімпійських ігор в Парижі 2024 року українськими науковцями не вивчалася.

Метою статті є системне дослідження правових аспектів забезпечення державної безпеки України за допомогою штучного інтелекту з урахуванням досвіду Олімпійських ігор в Парижі 2024 року та вироблення практичних рекомендацій щодо удосконалення законодавства у даному сегменті.

Виклад основного матеріалу. Перш ніж заглиблюватися в деталі, необхідно з'ясувати сутність поняття технології розпізнавання облич за законодавством Франції. Національна комісія з інформатики та свободи (CNIL) визначає цю технологію як «імовірнісний додаток для розпізнавання обличчя, який може автоматично розпізнавати особу на основі атрибутів її обличчя з метою її автентифікації або ідентифікації» [7].

Ця технологія може бути використана для двох основних функцій – верифікації та ідентифікації. Функція верифікації в основному передбачає порівняння 1:1 між окремим зображенням обличчя користувача (наприклад, зробленим електронною рамкою на кордоні) та біометричною фотографією, що зберігається в біометричному токені (наприклад, в паспорті). Верифікація найчастіше розглядається як синонім до «автентифікація» .

З іншого боку, методи ідентифікації передбачають порівняння одного зображення обличчя з безліччю зображень, що містяться в базі даних. Ці методи використовуються, наприклад, правоохоронними органами для ідентифікації підозрюваного.

Французьке агентство DPA у своєму звіті зазначило, що дана технологія, відома як «комп'ютерний зір», яка є однією з гілок «штучного інтелекту», що полягає в оснащенні систем можливостями цифрового аналізу зображень шляхом вилучення такої інформації, як розпізнавання образів, аналіз рухів, виявлення об'єктів [8].

Такі технології на основі штучного інтелекту дедалі частіше застосовуються для найрізноманітніших цілей, зокрема для моніторингу спортивних об'єктів. Наприклад, уряд Нідерландів профінансував план впровадження інтелектуального відеоспостереження на трьох стадіонах у Нідерландах з метою боротьби з дискримінацією під час футбольних матчів Ередивізії. Зокрема, на арені «Де Кюїп», домашньому стадіоні ФК «Феєнорд», використовується технологія для визначення причин дискримінаційної поведінки, способів її виявлення та припинення в зародку. Технологія також може визначати настрій інших уболівальників, які перебувають поруч з таким проявом дискримінації [9].

Незважаючи на те, що ця технологія все частіше впроваджується на спортивних об'єктах, існує дуже мало оцінок щодо того, чи було її застосування успішним у забезпеченні ефективної безпеки на заходах. Незважаючи на нестачу інформації, системи, керовані штучним інтелектом, часто сприймаються або представляються як панацея для забезпечення безпеки великих масових заходів.

Технології розпізнавання облич в основному дозволяють автоматизовано обробляти зображення обличчя з метою ідентифікації або автентифікації особи, саме тому вони використовувалися на великих громадських заходах по всьому світу, таких як Олімпійські ігри в Токіо (з метою автентифікації) і Чемпіонат світу з футболу, що проходив в Катарі. Зокрема, в Катарі під час проведення Чемпіонату світу з футболу, що проходив на 8 стадіонах, застосовувалися 15 000 камер відеоспостереження, підключених до систем розпізнавання облич. З цієї точки зору розпізнавання облич сприймається як потужний інструмент безпеки, що дозволяє правоохоронним органам контролювати громадські місця.

Мабуть, легко зрозуміти, чому французька влада була зацікавлена у впровадженні розпізнавання облич для підтримки заходів безпеки на Олімпійських іграх 2024 року в Парижі.

Зрештою, від систем авторизації та ідентифікації відмовилися як від засобу підтримки заходів безпеки на Олімпійських іграх. Так, міністр внутрішніх справ Франції заявив, що «я не є прихильником розпізнавання облич, інструменту, який є суспільним вибором і який пов'язаний з певним ризиком – тому що я вважаю, що у нас немає засобів гарантувати, що цей інструмент не буде використаний проти громадян за іншого режиму» [10].

Незважаючи на те, що французький уряд для забезпечення безпеки спортивних заходів під час Олімпійських ігор 2024 року в Парижі зрештою відмовився від свого проекту з розпізнавання облич, він вирішив дозволити впровадження інших відеопристроїв, керованих штучним інтелектом.

Тобто, замість розгортання технологій розпізнавання облич французький уряд обрав іншу технологію, яка є менш інвазійною, а саме використання смарт-камер. Основна відмінність між смарт-камерами і розпізнаванням облич полягає в тому, що в той час як метою розпізнавання облич є ідентифікація або автентифікація особи, смарт-камери можуть мати кілька цілей, починаючи від аналізу і закінчуючи категоризацією об'єктів або осіб.

Смарт-камери не обробляють біометричні дані і не призначені для ідентифікації осіб. Однак, навіть якщо смарт-камери не обробляють біометричні дані, це не означає, що вони не становлять ризиків для прав і свобод людини, оскільки вони можуть обробляти інші типи персональних даних. Це також означає, що їх слід вважати більш інтрузивними, ніж «традиційні» системи відеоспостереження, оскільки, як пояснює CNIL, смарт-камери за своєю природою дуже відрізняються від традиційних систем відеоспостереження, оскільки «людей більше не просто знімають, а аналізують в автоматизованому режимі, в реальному часі, щоб зібрати певну інформацію про них» [11].

Ризики, які становлять системи розумних камер, залежать від мети і способу їх використання. Наприклад, система, яка впливає або приймає рішення, що індивідуально впливає на людину, не становить такого ж ризику, як система, спрямована на невизначену групу людей або розгорнута в статистичних цілях.

У Франції немає спеціального закону, який би регулював використання розумних камер, однак це не означає, що ці системи не підлягають регулюванню або що вони де-факто дозволені чи заборонені.

Загалом, якщо системи розумних камер обробляють персональні дані, їх використання повинно відповідати принципам і правилам захисту даних: французькому Закону про обробку даних і свободи (loi informatique et libertés), а також Загальному регламенту про захист даних або Директиві про правоохоронні органи, якщо

обробка здійснюється правоохоронними органами. Крім того, CNIL зазначає, що оцінка впливу на захист даних повинна проводитися «через інноваційний характер технології». Крім того, в деяких конкретних випадках законодавство про захист даних передбачає необхідність прийняття внутрішніх положень, наприклад, коли технологія використовується правоохоронними органами для запобігання злочинам. У таких випадках розгортання «розумного» відео вимагає наявності законодавчого або іншого нормативного документа, який би дозволяв або контролював їх законне застосування [12].

Отже, необхідно зазначити, що наразі немає чітких доказів чи ефективні такі розумні відеосистеми. Існує дуже мало інформації про минулі експерименти та їх результати. Наприклад, низка територіальних громад у Франції використовує штучний інтелект у поєднанні із зображеннями відеоспостереження для виявлення кинутих сумок, стеження за громадським транспортом, управління світлофорами і т. ін. Так, муніципалітет Тулуза експериментував із програмним забезпеченням, яке виявляє підозрілі ситуації. Однак після оскарження цієї діяльності до суду, заступник міського голови заявив, що експерименти з розумними камерами не були «повністю задовільними» [12].

Узагальнюючи окреслену проблематику та проектуючи її на національну правову систему, не можемо оминути увагою той факт, що Конституція України забороняє втручання в особисте і сімейне життя людини крім випадків, безпосередньо зазначених у самому Основному Законі (наприклад, якщо таке втручання передбачено законом та здійснюється в інтересах національної безпеки).

Щодо практики застосування в Україні системи розпізнавання облич та наявне нормативне регулювання, можна констатувати про існування суттєвих недоліків у національному законодавстві, а саме: відсутність правового режиму захисту зображення обличчя людини, законодавчих підстав для встановлення та застосування вуличних відеокамер із технологіями розпізнавання облич, відсутність запобіжників від зловживань такими технологіями, а також недотримання принципу пропорційності втручання у права людини. Це створює ризики порушень Україною міжнародно-правових зобов'язань, зокрема статті 8 ЄКПЛ (право на повагу до приватного і сімейного життя) [13].

Основними напрямками удосконалення чинного в Україні нормативного регулювання щодо використання штучного інтелекту та забезпечення приватності громадян, уникнення можливих порушень прав людини, є такі:

1) у контексті впровадження технології розпізнавання облич важливо мати детальні правила, що регулюють обсяг і застосування заходів, а також надійні гарантії проти ризику зловживань і свавілля; потреба у правових гарантіях є значно більшою, коли йдеться про використання технології розпізнавання облич в реальному часі;

2) обробка персональних даних при застосуванні технології розпізнавання обличчя має бути виправданою та потребує високого рівня обґрунтування;

3) використання технології розпізнавання обличчя для криміналістичної ідентифікації підозрюваного за фотографіями та відео і, відповідно, використання технології розпізнавання обличчя в реальному часі для його розшуку та арешту повинно відповідати «нагальній суспільній потребі» та враховувати характер і тяжкість правопорушення [14].

У розрізі предмета нашого дослідження констатуємо, що Стратегія забезпечення державної безпеки від 16.02.2022 р. (далі – Стратегія) визначає реальні й потенційні загрози державній безпеці України, напрями та завдання державної політики у сфері державної безпеки, є основою для планування і реалізації політики у сфері державної безпеки [15].

Однак, безпосередньо у самій Стратегії не наводиться поняття «державна безпека». Звертаємо увагу, що поняття «державна безпека» закріплено в п. 1 ст. 1 Закону України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII і визначається як захищеність державного суверенітету, територіальної цілісності і *демократичного конституційного ладу* та інших життєво важливих національних інтересів від реальних і потенційних загроз невоєнного характеру [16].

У п. 3 Стратегії конкретизуються об'єкти забезпечення державної безпеки – державний суверенітет, конституційний лад, територіальна цілісність України, оборонний, економічний і науково-технічний потенціал, кібербезпека, інформаційна безпека, об'єкти критичної інфраструктури, державна таємниця та службова інформація.

Також нормативно інтерпретовано поняття «загрози державній безпеці» – явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити захищеність державного суверенітету, територіальної цілісності та демократичного конституційного ладу й інших життєво важливих національних інтересів.

Зважаючи на те, що до об'єктів забезпечення державної безпеки РНБО віднесла *конституційний лад*, а з-поміж загроз державній безпеці визначено ті можливі явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити, зокрема,

захищеність *демократичного конституційного ладу*, висновуємо прагнення авторів даної Стратегії нормативно гарантувати, зокрема й забезпечення приватності громадян та уникнення можливих порушень прав людини.

Зазначене вище корелюється зі змістом структурних складових поняття «інформаційна безпека» (визначеного у п. 3 Стратегії) – стан захищеності національних інтересів людини, суспільства і держави в інформаційній сфері, за якого унеможливлено завдання шкоди через: неповноту, невчасність та невірогідність інформації, що використовується, негативний інформаційний вплив; витік державної таємниці та службової інформації; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації, у тому числі шляхом проведення іноземними спецслужбами, окремими організаціями, групами, особами спеціальних інформаційних операцій та деструктивних інформаційних впливів, а також забезпечується своєчасне виявлення, запобігання та нейтралізація реальних і потенційних загроз національним інтересам та національній безпеці України.

Висновки. Отже, визначаючи реальні загрози державній безпеці України на сучасному етапі у контексті можливого впровадження технології розпізнавання облич важливо мати детальні правила, що регулюють обсяг і застосування заходів, а також надійні гарантії проти ризику зловживань і свавілля.

Невідворотна необхідність у правових гарантіях щодо реалізації та захисту приватності громадян, особливо коли йдеться про використання технології розпізнавання облич в реальному часі, висновується зі змісту Стратегії забезпечення державної безпеки, а саме:

1. До об'єктів забезпечення державної безпеки віднесено *конституційний лад*.

2. З-поміж загроз державній безпеці визначено ті можливі явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити, зокрема, захищеність *демократичного конституційного ладу,* при якому людина, її життя і здоров'я, честь і гідність, *недоторканність і безпека* визнаються найвищою соціальною цінністю.

3. У структурі елементів *інформаційної безпеки* чітко виокремлено стан захищеності національних інтересів людини, суспільства і держави в інформаційній сфері, за якого унеможливлено завдання шкоди, зокрема, через: неповноту, невчасність та невірогідність інформації, що використовується, негативний інформаційний вплив; *негативні наслідки застосування інформаційних технологій*; *несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації* і т. ін.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Тартачний О. Штучний інтелект використовуватимуть на Олімпіаді у Парижі. *Speka.media*. 2024. URL: https://speka.media/stucnii-intelekt-na-olimpiadi-p063q6.
2. Wesfreid M. Paris 2024 : pas de reconnaissance faciale aux JO. *Le Parisien*. November 23rd, 2022. URL: https://www.leparisien.fr/politique/paris-2024-pas-de-reconnaissance-faciale-aux-jo-23-11-2022-4E3FP2XBWZC4LBY3B4UMPA3QPE.php?ts=1669200293918.
3. Tokarieva, K., & Savliva, N. (2021). PECULIARITIES OF LEGAL REGULATION OF ARTIFICIAL INTELLIGENCE IN UKRAINE. *Scientific Works of National Aviation University. Series: Law Journal «Air and Space Law»*, *3*(60), 148–153. https://doi.org/10.18372/2307-9061.60.15967.
4. Тюря Ю.І. Правове регулювання використання штучного інтелекту на основі європейського підходу. *Знання Європейського права*. № 2. 2022. С. 141–145. DOI: https://doi.org/10.32837/chern.v0i2.360.
5. Задихайло О. Адміністративно-правове регулювання штучного інтелекту в Україні: сучасний стан та тенденції розвитку. *Збірник наукових праць Харківського національного педагогічного університету імені Г. С. Сковороди «ПРАВО».* Випуск 37, 2023. С. 9–14. https://doi.org/10.34142/ 23121661.2023.37.01.
6. Карпенко О. Штучний інтелект як інструмент публічного управління соціально-економічним розвитком: смарт-інфраструктура, цифрові системи бізнес-аналітики та трансферти. URL: http://www.dy.nayka.com.ua/pdf/ 10_2021/4.pdf.
7. Facial Recognition: For a debate living up to the challenges. *CNIL.* November 15th, 2019. p. 3. URL: https://www.cnil.fr/sites/default/files/atoms/files/facial-recognition.pdf.
8. Image Recognition vs Computer Vision: Key Differences Explained. *Deepomatic.* January 15th, 2024. URL: https://deepomatic.com/blog/difference-between-computer-vision-and-image-recognition.
9. Dutch clubs to deploy «smart technology» to fight fan racism. *France 24*. June 8th, 2022. URL: https://www.france24.com/en/live-news/20220608-dutch-clubs-to-deploy-smart-technology-to-fight-fan-racism.

10. Sécurité des jeux Olympiques et Paralympiques de 2024 – Audition de M. Gérald Darmanin, ministre de l'intérieur et des outre-mer, Commission des lois. *French Senate*. October 25th, 2022. URL: https://www.senat.fr/compte-rendu-commissions/20221024/lois.html.
11. Caméras dit «augmentées» dans les espaces publics: la position de la CNIL. *CNIL.* July 19th, 2022. URL: https://www.cnil.fr/fr/cameras-dites-augmentees-dans-les-espaces-publics-la-position-de-la-cnil.
12. Emery P. Toulouse : le pouvoir des caméras de vidéosurveillance. *La Dépêche*. January 3, 2019. URL: https://www.ladepeche.fr/article/2019/01/ 03/2934369-toulouse-le-pouvoir-des-cameras.html.
13. Воюта Д. Технологія розпізнавання облич: позиція ЄСПЛ у справі Glukhin v. Russia. 6 жовтня, 2023. *Центр демократії та верховенства права.* URL: https://cedem.org.ua/news/glukhin-v-russia/.
14. European Court of Human Rights. Case of Glukhin v. Russia (Application no. 11519/20). URL: https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-225655%22]}.
15. Указ Президента України від 16 лютого 2022 року № 56/2022 «Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки». *Президент України*. URL: https://www.president.gov.ua/documents/562022-41377.
16. Закон України «Про національну безпеку України» від 21.06.2018 р. № 2469-VIII. *Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.