ЦИВІЛІСТИЧНІ ПРОБЛЕМИ ІТ-ПРАВА

УДК 340.5
DOI https://doi.org/10.32837/chc.v0i41.423

Гончаренко Владислава Олександрівна,
кандидат юридичних наук, доцент,
доцент кафедри цивільного права
Національного університету «Одеська юридична академія»
ORCID ID: 0000-0001-9114-0276

ПРАВОВЕ РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ

Постановка проблеми. Технологія розпізнавання обличчя в режимі реального часу є системою автоматизованої обробки цифрових зображень, які містять біометричні дані фізичної особи у момент їх фіксації з метою ідентифікації, автентифікації, верифікації або категоризації цих осіб. Система проводить ідентифікацію особи через набір даних, що зберігаються у базі даних у форматі фото та відео.

У процесі аналізу біометричних даних особи відбувається фіксація зображення обличчя, яке за допомогою алгоритму перетворюється у цифрові дані з метою порівняння їх із цифровими даними, що зберігаються у базі даних зображень осіб. Перевірка особи відбувається у режимі реального часу за декілька секунд шляхом зіставлення нейропсихологічних, фізіологічних та інших характерних рис обличчя людини (відстані між очима, форми губ, носа тощо).

Системи розпізнавання обличчя сьогодні широко використовуються у світі та в Україні. Зазначені системи наявні у смартфонах, турнікетах, датчиках руху, камерах відеонагляду тощо. Комплексні системи відеоспостереження встановлюються в Україні у громадських місцях, що викликає питання стосовно дотримання вимог законодавства України про захист персональних даних під час побудови, впровадження та функціонування комплексних систем відеоспостереження в містах України.

Стан дослідження теми. Сьогодні проблемні питання правового регулювання використання технологій розпізнавання обличчя майже не досліджені. Окремі питання захисту персональних даних висвітлювалися у наукових роботах Є.О. Харитонова й О.І. Харотонової [1, с. 169–177], К.Г. Некіт [2, с. 57-65], О.В. Кохановської [3, с. 28–33], С.В. Гуцу [4, с. 123–129]. Постійне оновлення законодавства Європейського Союзу щодо захисту персональних даних, а також справедливості та прозорості систем штучного інтелекту (далі – ШІ) вимагає відповідного теоретичного опрацювання запроваджених змін із метою приведення законодавства України у цій сфері до вимог Європейського Союзу.

Метою дослідження є аналіз правового регулювання використання технологій розпізнавання обличчя за законодавством України та Європейського Союзу.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Відповідно до Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» [5] від 20 листопада 2012 р. № 5492-VI біометричними даними є сукупність даних про особу, зібраних на основі фіксації її характеристик, що мають достатню стабільність та істотно відрізняються від аналогічних параметрів інших осіб (біометричні дані, параметри – відцифрований підпис особи, відцифрований образ обличчя особи, відцифровані відбитки пальців рук).

Обробка біометричних даних забороняється, за загальним правилом, відповідно до ч. 1 ст. 7 Закону України «Про захист персональних даних» [6], проте ці дані можуть оброблятися, як виняток, лише в окремих випадках за згодою осіб для захисту життєво важливих інтересів суб'єкта персональних даних або на основі значного суспільного інтересу (ч. 2 ст. 7 Закону України «Про захист персональних даних»). Таким чином,

обробка біометричних даних, включаючи розпізнавання обличчя особи, повинна здійснюватися відповідно до закону, що відповідає вимогам Європейського Союзу у цій сфері.

Відповідно до Загального регламенту захисту даних (GDPR) [7] біометричні дані є особливим видом персональних даних, отриманих внаслідок спеціального технічного опрацювання, що стосується фізичних, фізіологічних чи поведінкових ознак фізичної особи, таких як зображення обличчя чи дактилоскопічні дані, які дозволяють однозначно ідентифікувати або підтверджують однозначну ідентифікацію фізичної особи. GDPR, за загальним принципом, забороняє обробку біометричних даних у режимі реального часу. GDPR класифікує зображення обличчя та іншу біометричну інформацію як особливу категорію даних із додатковими обмеженнями на їх використання.

Заборона на обробку біометричних даних відповідно до GDPR діє лише у разі, якщо фізичну особу ідентифіковано чи можна ідентифікувати. Тому принципи захисту даних не застосовують до анонімної інформації, зокрема інформації, що не стосується фізичної особи, котру ідентифіковано чи можна ідентифікувати, або персональних даних, які стали анонімними у такий спосіб, що суб'єкта даних неможливо чи більше неможливо ідентифікувати. У зв'язку із цим виникає проблемне питання ідентифікації осіб за умов світової пандемії, коли всі зобов'язані носити маски у публічних місцях. З одного боку, збір та обробка зображення особи у масці не є порушенням вимог GDPR щодо обробки біометричних даних, а з іншого – може бути підставою для несанкціонованого збирання інформації, яка не належить до біометричних даних про особу, однак також є персональними даними, як то хода, фігура людини, особливі пошкодження її тіла.

Крім того, незабаром технології 3-D друку дозволять створювати маски на обличчя, що може призвести до заміни однієї особи іншою, тому використовувати дані, зібрані з використанням технологій розпізнавання обличчя, з метою визначення особи правопорушника слід заборонити на законодавчому рівні. Дійсно, технології ШІ сприяють швидкому пошуку ймовірних збігів, однак остаточне рішення про те, чи була знайдена певна особа, має приймати лише людина, а не машина.

Сучасні АТ-технології розпізнавання обличчя поки що не можна назвати неупередженими, оскільки обличчя білих чоловіків розпізнаються більш точно, ніж білих жінок, а загалом розпізнавання білих обличь точніше, ніж із темною шкірою. Проблема упередженості є лише побічною проблемою, оскільки насамперед використання технологій розпізнавання обличчя викликає проблему захисту фундаментальних прав і свобод людини. Як свідчить аналіз судової практики у Російській Федерації, влада знайшла спосіб обійти приписи законодавства щодо збору біометричних даних тільки за згодою осіб, просто зазначаючи, що камери фіксують не зображення людей, а чистоту та кількість транспорту на вулиці.

Не вирішеним лишається сьогодні й питання відповідальності за несанкціоноване одержання інформації з бази біометричних даних, адже такі ситуації вже наявні. Зокрема, у 2020 р. компанію Facebook звинуватили у зборі біометричних даних осіб через Instagram шляхом створення «шаблону обличчя», який необмежений час зберігається у базі даних і використовується в технології розпізнавання обличчя.

Непередбачувані соціальні наслідки використання технологій розпізнавання обличчя та необмежені можливості для зловживання правами людини зумовлюють необхідність розробки відповідної правової бази у стислі строки. Помилки у комп'ютерних методах прийняття рішень щодо ідентифікації осіб можуть дорого коштувати суспільству під час визначення особи правопорушника, порушувати політичні та соціальні права людини у процесі реалізації права на участь у політичних зібраннях. Також порушення прав споживачів може мати місце у разі використання торговими компаніями технологій розпізнавання обличчя з метою автоматичного просування (рекламування) товарів.

Важливою гарантією реалізації права на захист персональних даних є встановлене у ст. 17 GDPR право на стирання (забуття). Зокрема, видалення контролером персональних даних працівника після звільнення є обов'язковим на вимогу суб'єкта даних, якщо немає іншої законної підстави для опрацювання. На жаль, цивільне законодавство України щодо захисту персональних даних не передбачає такого імперативного правила. Строки зберігання персональних даних регламентуються наказом Міністерства юстиції України від 12 квітня 2012 р. № 578/5 «Про затвердження Переліку типових документів, що створюються під час діяльності державних органів та органів місцевого самоврядування, інших установ, підприємств та організацій, із зазначенням строків зберігання документів» [8] (далі – Перелік). Строк зберігання документів від-

ділу кадрів і, відповідно, персональних даних становить 75 років. Згідно з п. 1.7 Переліку строки зберігання документів є мінімальними, їх не можна скорочувати. Таким чином, за законодавством України не допускається стирання персональних даних працівника за його вимогою у разі припинення трудових відносин.

Контроль за додержанням законодавства про захист персональних даних в Україні покладено на Уповноваженого Верховної Ради України з прав людини, однак за відсутності в Україні законодавства, яке регулює використання систем відеоспостереження, здійснення належного контролю за використанням біометричних даних особи сьогодні є неможливим.

У Євросоюзі випадки притягнення до відповідальності за порушення вимог GDPR вже є дуже розповсюдженими. *Зокрема, ще у 2018 р.* перший штраф у розмірі 200 000 шведських крон за порушення регламенту GDPR отримала Швеція. Муніципальна школа міста Шеллефтео використовувала відеокамеру та систему розпізнавання осіб для відстежування місцезнаходження учнів цієї школи за допомогою тегів, додатків для смартфонів і технології розпізнавання осіб. За допомогою камери відеоспостереження система ідентифікувала учня та робила помітку у системі про наявність його у певному класі. Слід зауважити, що учні та батьки надали письмову згоду на застосування системи відеоспостереження, однак, на думку Шведського управління із захисту даних (DPA), рада школи не могла використовувати їхню згоду, оскільки учні залежать від правління школи, а така залежність не може визнаватися юридично адекватною причиною для обробки конфіденційних персональних даних.

У 2019 р. міська рада Сан-Франциско ухвалила постанову, яка забороняє поліції міста використовувати технологію розпізнавання обличь. У Портленді у 2020 р. вперше у США повністю заборонили використовувати технології розпізнавання осіб у громадських місцях. Також штрафи за порушення регламенту вже отримали корпорація Google (50 млн євро), авіакомпанія British Airways (204 млн євро), мережа готелів Marriott (110 млн євро), італійський оператор зв'язку Wind Tre (16,7 млн євро) тощо.

На вирішення означених проблем у лютому 2020 р. Європейською Комісією було оприлюднено «Білу книгу зі штучного інтелекту. Європейський підхід до досконалості і довіри» ("A White paper on Artificial Intelligence – A European approach to excellence and trust" [9]). Відповідно до цього документа системи відеоспостереження з метою обробки біометричних даних можуть використовуватися тільки у виняткових, належним чином обґрунтованих і адекватних випадках на підставі законодавства ЄС або національного законодавства. Європейська Комісія таким чином почала дискусію про те, які можливі обставини можуть виправдати такі винятки та чи слід і на яких умовах дозволяти використання розпізнавання обличь у громадських місцях.

Внаслідок ґрунтовного вивчення цього питання Європейська Комісія у квітні 2021 р. оприлюднила пропозиції до регуляторних правил, які мають створити умови для безпечного й етичного використання ШІ в інтересах громадян Євросоюзу. З метою регулювання систем ШІ у Європейському Союзі планується створити спеціалізований орган – European Artificial Intelligence Board, який буде формувати переліки продуктів із високим ступенем ризику, вводити штрафи за використання ризикованих систем ШІ, проводити періодичні перевірки додержання регуляторних норм.

У цих правилах передбачаються критерії з оцінки ризиків використання технологій ШІ. Згідно з новими правилами всі системи ШІ, призначені для використання для віддаленої біометричної ідентифікації осіб, вважатимуться ризикованими та підлягатимуть попередній оцінці відповідності регулятором. Високоякісні набори даних і тестування допоможуть переконатися, що такі системи є точними та відсутній дискримінаційний вплив на особу. Використання віддаленої біометричної ідентифікації в режимі реального часу в загальнодоступних приміщеннях для цілей правопорядку створює особливі ризики для основних прав, зокрема гідності людини, поваги до приватного та сімейного життя, захисту персональних даних і недискримінації. Це заборонено у принципі, за кількома вузькими винятками, які суворо визначені, обмежені та регламентовані. Вони включають використання для правоохоронних цілей цілеспрямованого пошуку конкретних потенційних жертв злочинів, включаючи зниклих дітей; відповідь на безпосередню загрозу теракту; виявлення та встановлення осіб, котрі вчинили тяжкі злочини.

Використання технологій для віддаленої біометричної ідентифікації осіб у режимі реального часу в загальнодоступних місцях для правоохоронних органів для будь-якої із зазначених цілей має враховувати такі елементи:

1) характер ситуації, що породжує можливе використання, зокрема серйозність, імовірність

і масштаби шкоди, заподіяної за відсутності використання системи;

2) наслідки використання системи для прав і свобод усіх зацікавлених осіб, зокрема їх серйозність, імовірність і масштаби наслідків.

До всіх систем розпізнавання емоцій і біометричної категоризації завжди будуть застосовуватися конкретні вимоги щодо прозорості.

Висновки з дослідження та перспективи подальших розвідок у цьому напрямі. Таким чином, у Європейському Союзі вже розроблені чіткі правила використання систем біометричної ідентифікації осіб у режимі реального часу. Зазначене свідчить про необхідність приведення законодавства України про захист персональних даних до високих стандартів Євросоюзу. Серед питань, які насамперед мають бути визначені у цивільному законодавстві України, слід відзначити такі:

– використання технологій розпізнавання обличчя правоохоронними органами має відбуватися у чіткій відповідності до вимог законодавства України про захист персональних даних. Рішення про ідентифікацію особи, прийняте на підставі використання технологій розпізнавання обличчя, не може використовуватися як доказ вини особи;

– обов'язкове доведення до відома осіб інформації про використання технологій розпізнавання обличчя;

– вирішення на законодавчому рівні питання про обов'язкове одержання згоди осіб на використання технологій розпізнавання обличчя у комерційних цілях (у разі розміщення реклами, пропонування кредитів тощо)

– введення системи контролю за законністю використання технологій розпізнавання обличчя з боку громадськості;

– розробка юридичних механізмів забезпечення заборони опрацювання персональних даних, що розкривають расову чи етнічну належність, політичні переконання, релігійні чи філософські вірування, членство у професійних спілках, опрацювання генетичних даних, біометричних даних для цілі єдиної ідентифікації фізичної особи, даних стосовно стану здоров'я чи даних про статеве життя фізичної особи чи її сексуальної орієнтації;

– встановлення мінімальної вірогідності у роботі технологій розпізнавання обличчя та граничного строку зберігання біометричних даних.

ЛІТЕРАТУРА:

1. Харитонов Є.О., Харитонова О.І. Категорія «Інтернет речей» та цивільні правовідносини. *Наукові праці Національного університету «Одеська юридична академія».* Т. 20. 2017. С. 169–177.
2. Некіт К.Г. Персональні дані та індустріальні дані як об'єкти права власності: оцінка можливостей. *Часопис цивілістики*. 2020. № 36. С. 57–65.
3. Кохановська О.В. До питання про захист персональних даних в Україні. *Вісник Верховного Суду України*. 2011. № 6. С. 28–33. URL: http://nbuv.gov.ua/UJRN/vvsu_2011_6_8.
4. Гуцу С.Ф. Захист персональних даних працівників на підприємствах, установах та організаціях. *Гуманітарний часопис.* 2012. № 4. С. 123–129.
5. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус : Закон України від 20 листопада 2012 р. № 5492-VI. URL: https://zakon.rada.gov.ua/laws/show/5492-17#Text.
6. Про захист персональних даних : Закон України від 01 червня 2010 р. № 2297-VI. Відомості Верховної Ради. 2010. № 34. Ст. 481.
7. Загальний регламент про захист даних Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 р. *Офіційний вісник Європейського Союзу.* 2016. L 119. С. 1.
8. Про затвердження Переліку типових документів, що створюються під час діяльності державних органів та органів місцевого самоврядування, інших установ, підприємств та організацій, із зазначенням строків зберігання документів : наказ Міністерства юстиції України від 12 квітня 2012 р. № 578/5. URL: https://zakon.rada.gov.ua/laws/show/z0571-12#Text.
9. White Paper on Artificial Intelligence: a European approach to excellence and trust. URL: https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.

Гончаренко Владислава Олександрівна

ПРАВОВЕ РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ

У статті досліджуються проблемні питання правового регулювання систем розпізнавання обличчя, які сьогодні широко використовуються у світі та в Україні. Проаналізовано досвід регулювання захисту персональних даних у законодавстві ЄС, де розроблені чіткі правила використання систем біометричної ідентифікації осіб у режимі реального часу.

Відповідно до Загального регламенту захисту даних (GDPR) біометричні дані є особливим видом персональних даних, отриманих внаслідок спеціального технічного опрацювання, що стосується фізичних, фізіологічних чи поведінкових ознак фізичної особи, таких як зображення обличчя чи дактилоскопічні дані, що дозволяють однозначно ідентифікувати або підтверджують однозначну ідентифікацію фізичної особи. GDPR, за загальним прин-

ципом, забороняє обробку біометричних даних у режимі реального часу. GDPR класифікує зображення обличчя та іншу біометричну інформацію як особливу категорію даних із додатковими обмеженнями на їх використання.

Важливою гарантією реалізації права на захист персональних даних є встановлене у ст. 17 GDPR право на стирання (забуття). Зокрема, видалення контролером персональних даних працівника після звільнення є обов'язковим на вимогу суб'єкта даних, якщо немає іншої законної підстави для опрацювання. На жаль, цивільне законодавство України щодо захисту персональних даних не передбачає такого імперативного правила.

У Євросоюзі випадки притягнення до відповідальності за порушення вимог GDPR вже є дуже розповсюдженими. В Україні контроль за додержанням законодавства про захист персональних даних покладено на Уповноваженого Верховної Ради України з прав людини, однак за відсутності в Україні законодавства, котре регулює використання систем відеоспостереження, здійснення належного контролю за використанням біометричних даних, одержаних за їх допомогою, сьогодні є неможливим.

Відповідно до Білої книги зі штучного інтелекту системи відеоспостереження з метою обробки біометричних даних можуть використовуватися тільки у виняткових, належним чином обґрунтованих і адекватних випадках на підставі законодавства ЄС або національного законодавства.

Згідно з регуляторними правилами Європейської Комісії всі системи штучного інтелекту, призначені для використання для віддаленої біометричної ідентифікації осіб, вважаються ризикованими та підлягають попередній оцінці відповідності регулятором. Використання віддаленої біометричної ідентифікації у режимі реального часу в загальнодоступних приміщеннях для цілей правопорядку забороняється у принципі, за кількома вузькими винятками, які суворо визначені, обмежені та регламентовані. Вони включають використання для правоохоронних цілей цілеспрямованого пошуку конкретних потенційних жертв злочинів, включаючи зниклих дітей; відповідь на безпосередню загрозу теракту; виявлення та встановлення осіб, котрі вчинили тяжкі злочини.

Зроблено висновок про необхідність приведення законодавства України про захист персональних даних до високих стандартів Євросоюзу.

Ключові слова: технологія розпізнавання обличчя в режимі реального часу, біометричні дані, правове регулювання, захист персональних даних, штучний інтелект.

Goncharenko Vladyslava

LEGAL REGULATION OF THE USE OF FACE RECOGNITION TECHNOLOGIES

The article examines the problematic issues of legal regulation of facial recognition systems, which are now widely used in the world and, in particular, in Ukraine. The experience of regulation of protection of personal data in the EU legislation is analyzed, in which clear rules for the use of biometric identification systems in real time are developed.

According to the General Data Protection Regulation (GDPR), "biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. The GDPR, as a general principle, prohibits the processing of biometric data in real time. The GDPR classifies facial images and other biometric information as a special category of data with additional restrictions on their use.

An important guarantee of the realization of the right on protection of personal data is established in Art. 17 GDPR right to erasure (forgetting). In particular, the controller's removal of an employee's personal data after dismissal is mandatory at the request of the data subject, unless there is another legal basis for processing. Unfortunately, the civil legislation of Ukraine on personal data protection does not provide for such an imperative rule.

In the European Union, prosecutions for breaches of GDPR are already very common. In Ukraine, the Commissioner for Human Rights of Ukraine is responsible for monitoring compliance with the legislation on personal data protection. However, in the absence of legislation in Ukraine regulating the use of video surveillance systems, proper control over the use of biometric data obtained with their help is currently impossible.

According to the White Paper on Artificial Intelligence, video surveillance systems for the processing of biometric data may be used only in exceptional, duly justified and adequate cases on the basis of EU or national legislation.

According to the regulatory rules of the European Commission, all artificial intelligence systems intended for use for remote biometric identification of persons are considered risky and are subject to prior assessment of compliance by the regulator. The use of real-time remote biometric identification in public premises for law enforcement purposes is prohibited in principle, with a few narrow exceptions that are strictly defined, limited and regulated. These include the use for law enforcement purposes of a targeted search for specific potential victims of crime, including missing children; response to the immediate threat of a terrorist attack; or identifying of a person commited serious crime.

It is concluded that the legislation of Ukraine on personal data protection have to be harmonized with high standards of the European Union.

Key words: real-time remote biometric identification technology, biometric data, legal regulation, personal data protection, artificial intelligence.