

ГОНЧАРЕНКО ВЛАДА ОЛЕКСАНДРІВНА

*Національний університет «Одеська юридична академія»,
доцент кафедри цивільного права,
кандидат юридичних наук, доцент*

ПРАВОВЕ РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ

Технологія розпізнавання обличчя в режимі реального часу (LFR) є системою автоматизованої обробки цифрових зображень, які містять біометричні дані фізичної особи, такі як, обличчя, фігура, хода людини тощо¹, 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.

Системи розпізнавання обличчя на сьогодні широко використовуються у світі та, зокрема, в Україні. Комплексні системи відеоспостереження встановлюються в Україні в 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.

Як визначається у ч. 5 ст. 6 Закон України «Про захист персональних даних», обробка персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством.

Обробка біометричних даних забороняється за загальним правилом, відповідно до ч.1 ст. 7 Закону України «Про захист персональних даних».

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

Загальний регламент захисту даних (GDPR) за загальним принципом забороняє таку обробку біометричних даних. GDPR класифікує зображення обличчя та іншу біометричну інформацію як особливую категорію даних з додатковими обмеженнями на їх використання. Проте, ці дані (так само, як визначає Закон України «Про захист персональних даних») 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»).

¹ Відповідно до Закону України "Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус" від 20.11.2012 N 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).

Контроль за дотриманням 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 на сьогодні є неможливим.

У Євросоюзі випадки притягнення до відповідальності за порушення вимог GDPR вже є дуже розповсюдженими. Зокрема, ще у 2018 році 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 вистежування місцезнаходження учнів цієї школи за допомогою тегів, додатків для смартфонів і технології розпізнавання осіб. За допомогою камери відеоспостереження система ідентифікувала учня і робила помітку у системі про наявність його у певному класі. При цьому 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 році міська рада Сан-Франциско ухвалила постанову, яка забороняє владі міста використовувати технологію розпізнавання облич. 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.

У лютому 2020 року Європейською Комісією було оприлюднено «Білу книгу з штучного інтелекту. Європейський підхід до досконалості і довіри» («A White paper on Artificial Intelligence – A European approach to excellence and trust»). Відповідно до цього документу 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 широкую дискусію про те, які можливі обставини можуть виправдати такі винятки, і чи слід і на яких умовах дозволяти використання розпізнавання облич у громадських місцях.

Внаслідок ґрунтовного вивчення цього питання Європейська Комісія у травні 2021 року оприлюднила пропозиції до регуляторних правил, які мають створити умови для безпечного та етичного використання штучного інтелекту (ШІ) в інтересах громадян Євросоюзу. 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 та тестування

допоможуть переконатись, 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 та недискримінації. Тому це заборонено в 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; або виявлення та встановлення осіб, які вчинили тяжкі злочини. Нарешті, до всіх систем розпізнавання емоцій та біометричної категоризації завжди будуть застосовуватися конкретні вимоги щодо прозорості.

Таким чином, у Європейському Союзі вже розроблені чіткі правила використання систем біометричної ідентифікації осіб в режимі реального часу. Зазначене свідчить про необхідність приведення законодавства України про захист персональних даних до високих стандартів Євросоюзу.

Ключові слова: штучний інтелект, персональні дані, біометричні дані, інформаційні технології.

Ключевые слова: искусственный интеллект, персональные данные, биометрические данные, информационные технологии.

Key words: artificial intelligence, personal data, biometric data, information technology.

ОМЕЛЬЧУК ОЛЕКСАНДР СЕРГІЙОВИЧ

*Національний університет «Одеська юридична академія»,
доцент кафедри цивільного права,
кандидат юридичних наук, доцент*

ДО ПИТАННЯ РОЗМЕЖУВАННЯ КАТЕГОРІЙ «ЦИВІЛЬНИЙ ОБОВ'ЯЗОК» ТА «ЦИВІЛЬНЕ ЗОБОВ'ЯЗАННЯ»

Цивільне законодавство та юридична наука широко використовують схожі за змістом категорії «цивільний обов'язок», «цивільне зобов'язання», а також похідні від них «обов'язок особи», «зобов'язана особа».

Суб'єктивний цивільний обов'язок зазвичай розглядається у контексті змісту цивільних правовідносин у безпосередньому зв'язку з суб'єктивними цивільними правами. Як зазначає С.О. Погрібний, суб'єктивний цивільний обов'язок необхідно розглядати як вид і міру належної поведінки суб'єкта цивільних правовідносин. Обов'язок, наряду з цивільним правом, виникає на підставі норми об'єктивного цивільного права (статутного або договірної), у зв'язку з виникненням