ЦИВІЛЬНЕ ПРАВО І ЦИВІЛЬНИЙ ПРОЦЕС; СІМЕЙНЕ ПРАВО

Токарева В.О.,
кандидат юридичних наук, доцент,
доцент кафедри цивільного права
Національного університету «Одеська юридична академія»

УДК 347.15/18
DOI 10.32782/2663-5666.2023.2.1

ПРАВОВЕ РЕГУЛЮВАННЯ ЗАСТОСУВАННЯ СИСТЕМ ВІДДАЛЕНОЇ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ В ЄС

Вступ. Застосування автоматизованих технології відеоспостереження із дистанційним біометричним розпізнаванням обличчя актуалізує питання впливу технологій та приватне життя та встановлення правових гарантій захисту прав особи на недоторканність приватного життя, адже наразі, існуючі технології дозволяють створити диктатуру на зразок Дж. Орвелла та авторів інших антиутопій. Поширення використання даних систем державними органами обумовлюється метою забезпечення національної безпеки: запобігання, розкриття та розслідування злочинів, предикативної аналітики вчинення правопорушень, оплати громадського транспорту, державних послуг тощо. У діяльності комерційних організацій технологія (транспортних організацій, банків, супермаркетів, кафе), використовується для гарантування безпеки, полегшення доступу до фінансових продуктів і підвищуватимуть продажі.

Метою статті є дослідження доктринальних та нормативних джерел ЄС в області застосування автоматизованих технологій відеоспостереження із дистанційним біометричним розпізнаванням обличчя та розробка пропозиція для правового регулювання українського законодавства.

Виклад основного матеріалу. Наразі, лідером використання технології відеоспостереження із дистанційним біометричним розпізнаванням є КНР, де системи відеоспостереження із функцією розпізнавання обличчя не лише активно застосовуються, а й експортується до різних держав світу [1]. Технологія передбачає присвоєння особі рейтингу в соціальній системі та може відправляти необхідні данні правоохоронним органам про те, що особа має неоплачені штрафи, ухиляється від сплати аліментів або перебуває в розшуку [2]. Технологія дозволяє уряду КНР збирати великі обсяги даних про громадян.

Наразі, дослідницькі проекти, що фінансуються в межах програми «Горизонт 2020», використовують штучний інтелект на зовнішніх кордонах ЄС, в межах проекту iBorderCtrl система штучного інтелекту детекції брехні складає профіль мандрівників на основі комп'ютерного автоматичного інтерв'ю, знятого відео камерою мандрівника напередодні мандрівки та аналізу штучним інтелектом 38 мікрожестів. Наразі, проект пройшов тестування в Угорщині, Латвії та Греції [3]. Технологія відеоспостереження із дистанційним біометричним розпізнаванням допомагає правозахисним організаціям виявляти жертв работоргівлі, визначати їхнє місцезнаходження, заощаджуючи час фахівців, як, наприклад, компанія Marinus Analytics використовує програм у сервісі Amazon Rekognition [4].

У зв'язку із повномасштабною російською агресією, Україна отримала доступ до приватної бази даних розпізнавання обличчя – Clearview AI, яка містить майже десять мільярдів фотографій, що має надати можливість перевіряти фізичних осіб при перетині кордону [5]. Правоохоронні органи США використовували технологію Clearview AI для встановлення учасників масових заворушень під час протестів Black Lives Matter та штурму Капітолію у Вашингтоні [6]. Clearview AI, відома тим, що свої послуги надає державним органам та його представникам, а база фотографій зібрана із відкритих джерел в Інтернеті та соціальних мережах, зокрема громадян ЄС, порушує європейське законодавство, законний збір та обробку персональних даних про фізичних осіб.

Відтак, використання технології покликано нести позитивний вплив, разом з цим, на конфе-

ренції під назвою «Орвеллівське передбачення: обговорення небезпек біометричного спостереження» проведеного Європейською Радою з питань захисту персональних даних (European Data Protection Board, EDPB) зазначається, що шкода від застосування технологій розпізнавання обличчя може значно перевищувати потенційні переваги [7]. Адже не можна нехтувати впливом повсюдного відеоспостереження на добробут та психіку людей, та потребу дотримання вимог законодавства при захист персональних даних під час оброки. Поширення застосування технології ставить питання етико правових засад її розповсюдження.

Слід зазначити, що використання систем відеоспостереження вимагає дотримання принципу законності та ставить питання щодо ефективності застосування таких систем, оскільки відеоспостереження не запобігло вчиненню терористичних актів у громадському транспорті у Лондоні [8], терористичних актів 2001 року в США. К. Веліз підтверджує, що використання систем відеоспостереження не ефективне в попередженні терористичних актів, оскільки є не закономірними вчинками, а умисними порушенням законодавства. До того, ж втручання у приватне життя яке справляє відеоспостереження також призводить до смерті людей [9]. Крім того, залишаються ризики пов'язані із можливістю вторинного використання даних зібраних системами відеоспостереження із дистанційним біометричним розпізнаванням з порушенням мети, для якої вони були отримані та зібрані. Тому використання технології відеоспостереження із біометричною ідентифікацією потребує суворої регламентації.

Тому, поряд із позитивним ефектом використання технології, наразі, відзначається тенденція у правовому регулювання на обмеження повсюдного використання систем відеоспостереження із дистанційним біометричним розпізнаванням та розробка чітких правових засад використання технології. Навіть, в КНР поступово запроваджуються законодавчі обмеження використання технології. Згідно зі ст. 26 Закону КНР Про захист персональної інформації, що набрав чинності 1 листопада 2021 р., передбачено, що встановлення обладнання для збору зображень або розпізнавання обличчя у громадських місцях повинно здійснюватися у випадках, коли це вимагається засадами національної та громадської безпеки та згідно із законодавством про, що має бути чітко зазначено. Збір зображень та відмінних ідентифікаційних ознак може здійснюватися тільки з метою національної безпеки, та не може здійснюватися для іншої мети, за виключенням окремої згоди суб'єкта даних [10].

Традиційно досить послідовну позицію у питанні правового регулювання прав та свобод фізичних осіб, та функціонування новітніх інформаційно комунікаційних технологій, в тому числі технологій дистанційного біометричної ідентифікації займає ЄС. Відповідно до Резолюції Європейського парламенту від 6 жовтня 2021 р. людина не лише має право на правильну ідентифікацію, а й право взагалі не бути ідентифікованою, за виключенням випадків, коли це вимагається законодавством у зв'язку із суспільними інтересами відповідно до закону (п. 8) [11].

За твердженням Верховного комісара ООН з прав людини М. Башле у доповіді від 13 вересня 2021 р. «Право на недоторканність приватного життя в цифрову епоху» відповідно до ст. ст. 2 і 17 Міжнародного Пакту про Громадянські та Політичні Права, на держави покладається не лише обов'язок не порушувати фундаментальне право людини на недоторканність приватного життя («негативний обов'язок»), а й «позитивний обов'язок» захищати осіб від подібних посягань, та дискримінації, у межах своєї юрисдикції, зокрема, встановити належні правові гарантії та інструменти для їхньої ефективної реалізації (п. 10 Доповіді) [12]. Дистанційне біометричне розпізнавання обличчя, згідно із Доповідю Верховного комісара пов'язане з глибоким втручанням у приватне життя. Біометричні данні є одним з ключових ідентифікаторів особи, які дозволяють відрізнити особу від інших суб'єктів даних. За твердженням Верховного комісара, дистанційна біометрична ідентифікація значно підвищує можливість державних органів систематично провадити ідентифікацію та спостереження за людьми в громадських місцях, підриваючи право людина на недоторканність приватного життя без стороннього нагляду та справляючи прямий негативний ефект на такі права, як свобода думки, свобода мирних зібрань і об'єднань та свобода пересування (п. 27 Доповіді).

Резолюція Європарламенту Про штучний інтелект у кримінальному провадженні та його використанні поліцією та судовими органами у кримінальних справах від 6 жовтня 2021 р. також наголошує, що використання біометричних даних у ширшому сенсі пов'язане з принципом права на людську гідність, що становить осно-

ву всіх основних прав, гарантованих Хартією фундаментальних прав ЄС. Використання і збір будь-яких біометричних даних для цілей віддаленої ідентифікації, наприклад, шляхом розпізнавання обличчя у громадських місцях, а також на автоматичних контрольно-пропускних пунктах, які використовуються для прикордонного контролю в аеропортах, може становити особливі ризики для основоположних прав, наслідки яких можуть значно варіюватися залежно від мети, контексту і сфери використання [13]. В Резолюції Європарламент дотримується позиції про те, що впровадження систем ШІ в правоохоронній і судовій сферах має розглядатися не як проста технічна можливість, а як політичне рішення, що стосується цілей правоохоронних органів і систем кримінального правосуддя.

Методи відеоспостереження, засновані на дистанційній ідентифікації ставлять виклик існуючому підходу у кримінальному праві про реагування на правопорушення після вчинення, не припускаючи, що всі люди потребують постійного спостереження для запобігання потенційних правопорушень. Тому впровадження подібних технологій потребує проведення оцінки наслідків впровадження технологій, які знижують роль людини в правозастосуванні та винесенні судових рішень.

Означена ситуація призводить то того, що внаслідок використання технології розпізнавання обличчя людина жодним чином не впливає на обсяг даних які збираються відносно неї, що посягає на її інформаційне самовизначення, людську гідність та недоторканність приватного життя. За таких умов, розширення застосування технологій відеоспостереження може справляти вплив на прийняття рішення особами не лише у сфері щоденних правочинів, а й політичного вибору. Крім того цілі заради яких розширюється застосування відеоспостереження може так і залишитися недосяжними, а втручання у приватне життя буде невідворотно порушено. Оскільки застосування технології відеоспостереження із дистанційним біометричним розпізнаванням представляє собою обробку персональних даних, то застосування технології вимагає дотримання принципів обробки персональних даних, принципу законної обробку та застосування технології лише за умови якщо це необхідно, для досягнення законної мети обробки.

Згідно із Керівництвом 2/2019 Європейської ради із захисту персональних даних Щодо обробки персональних даних відповідно до статті 6(1)(b) Регламенту зазначено, що в контексті надання онлайн-послуг суб'єктам даних «необхідність» позначає, неможливість досягнення мети іншим способом. Йдеться саме про неможливість досягти мети, а не про вартість або зручність тощо. Необхідність має бути наявною, реально існуючою або вона має виникнути в найближчому майбутньому, а не гіпотетичною. Обробка персональних даних «на випадок» для досягнення гіпотетичної мети, яка вірогідно не настане, не охоплюється категорією «необхідність» [13, 14].

Європейський суд Справедливості у справі Heinz Huber v Bundesrepublik Deutschland зазначив що концепт «необхідності» має власне незалежне значення у праві ЄС, яке має тлумачитися у повній відповідності до цілей законодавства про захист персональних даних [15]. У справі Valsts policijas Rigas regiona parvaldes Kartibas policijas parvalde v Rigas pasvaldibas SIA Rigas satiksme Європейський суд Справедливості застережив, що відступи та обмеження стосовно обробки персональних даних можуть застосовуватися лише, якщо це суворо необхідно [16].

ЄКПЛ у ч. 2 ст. 8 наголошує, що органи державної влади не можуть порушувати недоторканність приватного життя, інакше як: на підставі закону; якщо це необхідно в демократичному суспільстві в інтересах національної безпеки, громадської безпеки та економічного добробуту держави, для запобігання або припинення злочину, захисту здоров'я чи моралі або захисту прав і свобод інших осіб.

У ч. 1 ст. 52 Хартії фундаментальних прав ЄС міститься аналогічне формулювання, однак, його доповнює принцип пропорційності, під яким розуміється пропорційність між характером запроваджуваних обмежень та їхнім впливом на права суб'єктів, з одного боку, і важливістю та масштабом переслідуваних цілей, з іншого.

Європарламент у Резолюції від 6 жовтня 2021 р., визнає певний позитивний вплив від застосування систем віддаленої біометричної ідентифікації в області правозастосування, підвищення якості методів роботи правоохоронних та судових органів, ефективністю боротьби із злочинами у фінансовій сфері, відмиванню доходів отриманих злочинним шляхом, фінансуванню тероризму, насильницькими злочинами та експлуатацією дітей в Інтернеті, окремими видами кіберзлочинів, водночас може призвести до зростання числа випадків використання систем віддаленої ідентифікації для масового

спостереження. Водночас застосування систем з метою масового спостереження буде невідповідним [11].

Законопроект ЄС про штучний інтелект від 18 червня 2021 р. відносить технології розпізнавання обличчя до категорії технологій із високим рівнем ризику для прав і свобод людини та встановлення загальної заборони на використання таких технологій, за виключенням чітко визначених випадків.

Відповідно до Висновку Європейської Ради із захисту персональних даних та Європейського наглядового органу із захисту персональних даних на Законопроект ЄС про штучний інтелект зазначено, що дистанційна біометрична ідентифікація осіб у загальнодоступних місцях несе високий ризик втручання у приватне життя осіб, а можливість бути визначеною або класифікованою програмою зачіпає людську гідність [17]. У Висновку зазначається, що використання систем штучного інтелекту може створити проблеми із дотриманням пропорційності, оскільки може призвести до обробки даних невибіркової та невідповідної кількості суб'єктів даних для ідентифікації лише декількох осіб (наприклад, пасажирів в аеропортах та вокзалах). Безконтактний характер систем відеоспостереження із дистанційним біометричним розпізнаванням здатний створити проблеми прозорості та дотримання правових підстав для обробки даних відповідно до законодавства ЄС. До того ж постає питання щодо способу належного інформування фізичних осіб про відеоспостереження із застосуванням віддаленої біометричної ідентифікації та обробки, для ефективного здійснення прав фізичних осіб, а саме здійснення свободи вираження поглядів, зібрань, асоціацій, свободи пересування. Адже застосування подібних систем істотно впливає на дотримання засад (розумного) очікування населення на анонімність в громадських місцях та може негативно впливати на реалізацію прав та свобод людини.

Визнаючи, що Законопроект ЄС про штучний інтелект містить значний перелік виключних випадків, коли віддалена біометрична ідентифікація в режимі реального часу в публічних місцях допускається для цілей правозастосування, проте Європейська Рада із захисту персональних даних та Європейського наглядового органу закликають запровадити загальну заборону на будь-яке використання ШІ для автоматичного розпізнавання людських рис у загальнодоступних місцях – як обличчя, хода, відбитки пальців, ДНК, голос, натискання клавіш та інших біометричних або поведінкових сигналів – у будь-якому контексті. Оскільки подібна практика як така не може відповідати вимогам необхідності та пропорційності, що в решті випливає з розуміння допустимого втручання у фундаментальні права, як це тлумачить Європейського суду Справедливості та ЄСПЛ. У Висновку пропонується встановити суворі випадки виключень коли технології можуть використовуватися.

Аналогічна позиція висловлена Європейським парламентом у Резолюції Про штучний інтелект у кримінальному провадженні та його використанні поліцією та судовими органами у кримінальних справах від 6 жовтня 2021 р. де зазначено, що підхід, прийнятий у деяких державах, не членах ЄС, до розробки, впровадження та використання технологій масового спостереження, непропорційно обмежує основні права, і тому має не застосовуватися в ЄС. У Резолюції також зазначено, що Європейський парламент закликає запровадити постійну заборону на використання автоматизованого аналізу та/або розпізнавання в публічно доступних місцях характеристик людини, таких як хода, відбитки пальців, ДНК, голос та інші біометричні та поведінкові сигнали.

За твердженням Європейського парламенту використання правоохоронними органами та спецслужбами приватних баз даних розпізнавання обличчя, таких як Clearview AI викликає занепокоєність, а факт використання технології Clearview AI та еквівалентних технологій має розкриватися правоохоронними органами. Європейський парламент загалом закликає заборонити використання приватних баз даних розпізнавання обличчя правоохоронними органами. Європарламент висловлює стурбованість з приводу проведення дослідницьких проектів таких, як iBorderCtrl. Європарламент також вважає необхідним та закликає Комісію запровадити заборону на будь-яку обробку біометричних даних, включно із зображеннями обличчя, у правоохоронних цілях, що призводить до масового спостереження в загальнодоступних місцях та закликає Комісію припинити подальше фінансування на проведення біометричних досліджень, що можуть призвести до невибіркового масового спостереження в громадських місцях.

Незважаючи на те, що остаточних законодавчих рішень в ЄС з цього питання не прийнято, та окремі поодинокі законодавчі обмеження

використання технології мету використання системи відеоспостереження з дистанційним біометричним розпізнаванням обличчя можна говорити про розробку правового регулювання використання технології та поодиноких випадків запровадження обмежень щодо використання технології масового дистанційного розпізнавання людей у громадських місцях у законодавстві, проте не повної заборони законодавством. Підсумовуючи викладене, слід зазначити, відсутність адекватної правової бази, що відповідає викликам таких технологій, а також проблематичність її формування, призводить до глобального тренду на встановлення певних правових обмежень у цій сфері.

Висновки. З огляду на потребу боротьби з терористичними діями, злочинністю та з урахуванням позиції Європейського парламенту уявляється, що застосування систем віддаленої біометричної ідентифікації має бути обмеженим та включати такі складові, як: заборона на використання систем розпізнавання обличчя приватним компаніями у громадських місцях; заборона на невибіркове розпізнавання обличчя та обмеження лише особами, які перебувають розшуку, встановлення підстав і процедури внесення осіб до числа розшукуваних; визначення місць розміщення засобів систем розпізнавання; інформування осіб, що ведеться відеоспостереження і механізми реалізації та захисту прав осіб (privacy notice) та заборона прихованого відеоспостереження; встановлення строків зберігання таких даних і механізмів їх захисту; виключно обмежений перелік уповноважених державних органів, на використання систем розпізнавання обличчя.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. У Китаї камера розпізнала підозрюваного серед 60 тисяч людей. 14 Квітня 2018. URL: https://volynonline.com/u-kitayi-kamera-rozpiznala-pidozryuvanogo-sered-60-tisyach-lyudey/
2. Сканування за ходою і формою тіла: у Китаї запускають систему тотального стеження. 11 листопада 2018. URL: https://konkurent.ua/publication/32528/skanuvannya-za-hodou-i-formou-tila-u-kitai-zapuskaut-sistemu-totalnogo-stezhennya/
3. Кікоть С. ЄС випробує детектори брехні зі штучним інтелектом на кордонах країн. 01.11.2018. URL: https://hromadske.ua/posts/yes-viprobuye-detektori-brehni-zi-shtuchnim-intelektom-na-kordonah-krayin?topic=svit
4. Kaiser Larsen Marinus Analytics fights human trafficking using Amazon Rekognition. 09 AUG 2018. URL: https://aws.amazon.com/blogs/machine-learning/marinus-analytics-fights-human-trafficking-using-amazon-rekognition/
5. 10 мільярдів фото і система розпізнавання: Україна отримала доступ до бази Clearview AI 14.03.2022. URL: https://www.ukrinform.ua/rubric-technology/3429032-10-milardiv-foto-i-sistema-rozpiznavanna-ukraina-otrimala-dostup-do-bazi-clearview-ai.html
6. Года М. Clearview AI збирає базу фотографій всіх жителів планети: для чого це потрібно компанії. URL: https://24tv.ua/tech/clearview-ai-zbiraye-bazu-fotografiy-vsih-zhiteliv-novini-tehnologiy_n1870807
7. Trainees Conference Recording – An Orwellian Premonition: a discussion on the perils of biometric surveillance. URL: https://edps.europa.eu/press-publications/press-news/videos/trainees-conference-recording-orwellian-premonition-discussion_en
8. Токарева В.О. Страхування ризику тероризму. Традиції та новації юридичної науки: минуле, сучасність, майбутнє: матеріали Міжнародної науково-практичної конференції (м. Одеса, 19 травня 2017 р.) У 2-х т. Т. 2 / відп. ред. Г.О. Ульянова. – Одеса: Видавничий дім «Гельветика», 2017. С. 530-533.
9. Veliz C. The Power of BigTech and Ethics, GRC World Forums. 1 April 2021. URL: https://www.grcworldforums.com/on-demand-content/the-power-of-bigtech-and-ethics-carissa-veliz/1185.article
10. Personal Information Protection Law of the People's Republic of China, PIPL URL: https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021
11. European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)) 6 October 2021. URL: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html
12. Bachelet M. Artificial intelligence risks to privacy demand urgent action.15 September 2021. URL: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27469&LangID=E
13. Guidelines 2/2019 On the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects
14. WP29. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
15 . CJEU, Case C-524/06, Heinz Huber v Bundesrepublik Deutschland, 18 December 2008, para. 52. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62006CJ0524
16 . CJEU, Case C-13/16, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme', para. 30. URL: https://curia.europa.eu/juris/liste.jsf?num=C-13/16
17 . EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act). URL: https://edps.europa.eu/data-protection/our-work/publications/opinions/joint-opinion-edps-edps-proposal-regulation-european_en

Токарева В.О. ПРАВОВЕ РЕГУЛЮВАННЯ ЗАСТОСУВАННЯ СИСТЕМ ВІДДАЛЕНОЇ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ В ЄС

У статті розглянуті доктринальні та нормативні джерела ЄС в області застосування автоматизованих технологій відеоспостереження із дистанційним біометричним розпізнаванням та розроблені шляхи для правового регулювання українського законодавства у цій сфері.

Встановлено, що лідером використання технології відеоспостереження із дистанційним біометричним розпізнаванням є КНР. Технологія використовується для допомоги правоохоронним органам та правозахисним організаціям виявляти жертв работоргівлі, визначати їхнє місцезнаходження та заощаджуючи час. У зв'язку із повномасштабною російською агресією, Україна отримала доступ до приватної бази даних розпізнавання обличчя – Clearview AI, яка має надати можливість перевіряти фізичних осіб при перетині кордону.

Доведено, що застосування систем віддаленої біометричної ідентифікації справляє позитивний вплив в області правозастосування, підвищення якості методів роботи правоохоронних та судових органів, ефективності боротьби із злочинами у фінансовій сфері, відмиванню доходів отриманих злочинним шляхом, фінансуванню тероризму, розкриттю насильницьких злочинів, експлуатацією дітей в Інтернеті та окремими видами кіберзлочинів. Встановлено, що використання таких технологій як Clearview AI приватними компаніями може порушувати законодавство про законний збір та обробку персональних даних про фізичних осіб, оскільки до суб'єкта даних не звертаються за отриманням згоди на обробку. Крім того, залишаються ризики пов'язані із можливістю вторинного використання даних зібраних системами відеоспостереження із дистанційним біометричним розпізнаванням з порушенням мети, для якої вони були отримані та зібрані. Тому використання технології відеоспостереження із біометричною ідентифікацією потребує суворої регламентації.

Встановлено, що поряд із безспірними позитивним ефектом використання технології, наразі, відзначається тенденція у правовому регулюванні на обмеження повсюдного використання систем відеоспостереження із дистанційним біометричним розпізнаванням та розробка чітких правових засад використання технології. Обмеження застосування систем відеоспостереження із дистанційним біометричним розпізнаванням, збір та обробка зображень та відмінних ідентифікаційних ознак виключно з метою національної та громадської безпеки, за виключенням окремої згоди суб'єкта даних запроваджено Законом КНР Про захист персональної інформації у 2021 році.

***Ключові слова*:** фізична особа, особисті немайнові права, права людини, цифрові права, персональні дані, захист персональних даних, цифровізація, штучний інтелект, відеоспостереження, законодавство ЄС.

Tokareva V.O. LEGAL REGULATION OF THE USE OF REMOTE BIOMETRIC IDENTIFICATION SYSTEMS IN THE EU

The article examines the EU doctrinal and regulatory sources in the field of automated video surveillance technologies with remote biometric recognition and develops the ways of legal regulation of Ukrainian legislation in this area.

It is established that China is the leader in the use of video surveillance technologies with remote biometric recognition. The technology helps human rights organisations identify victims of human trafficking and locate and save specialist's time. Due to the full-scale Russian aggression, Ukraine gained access to a private facial recognition database, Clearview AI, which should allow for the verification of individuals at border crossings.

It is proved that the use of remote biometric identification systems has a positive impact on law enforcement, improving the quality of law enforcement and judicial methods, and the effectiveness of combating financial crimes, money laundering, terrorist financing, solving violent crimes, online child exploitation and certain types of cybercrime. It has been established that the use of technologies such as Clearview AI by private companies may violate the law on the lawful collection and processing of personal data on individuals, as the data subject is not asked for consent to processing. In addition, there are still risks associated with the possibility of secondary use of data collected by video surveillance systems with remote biometric recognition in violation of the purpose for which it was obtained and collected. Therefore, the use of video surveillance technology with biometric identification requires strict regulation.

It is established that, along with the undoubted positive effects of the technology, there is currently a trend in legal regulation to limit the widespread use of video surveillance systems with remote biometric recognition and to develop clear legal framework for the use of the technology. Restrictions on the use of video surveillance systems with remote biometric recognition, collection and processing of images and distinctive identification features solely for national and public security purposes, with the exception of the separate consent of the data subject, were introduced by the PRC Personal Information Protection Law in 2021.

It is stipulated that the use of remote biometric identification systems should be limited and include the following components: prohibition of the use of recognition systems by private companies in public places; prohibition of indiscriminate recognition of persons and limitation to wanted persons only, establishment of grounds and procedure for putting people on wanted lists; determination of the location of recognition systems, informing people about surveillance and mechanisms for exercising and protecting their rights (privacy notice) and prohibition of covert video surveillance; establishing storage periods for such data and mechanisms for their protection; clearly identifying state bodies that have the authority to use recognition systems.

Key words: natural person, moral rights, human rights, digital rights, personal data, personal data protection, digitalisation, artificial intelligence, video surveillance, EU legislation.