DOI https://doi.org/10.36059/978-966-397-318-0-14

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

ДО ПИТАННЯ ДИСТАНЦІЙНОЇ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

Застосування автоматизованих технології системи ШІ відеоспостереження із дистанційним біометричним розпізнаванням або віддаленої біометричної ідентифікації особи 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.

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. Дослідницькі проекти, що фінансуються в межах програми «Горизонт 2020», використовують штучний інтелект на зовнішніх кордонах ЄС, в межах проекту iBorderCtrl, «розумна система детекції брехні», який складає профіль мандрівників на основі комп'ютерного автоматичного інтерв'ю, знятого відео камерою мандрівника перед пригодою, та аналізу 38 мікрожестів на основі аналізу штучним інтелектом, нараз пройшло тестування в Угорщині, Латвії та Греції [3].

Наразі, 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 конференції 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 транспорті у Лондоні, 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 [8].

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 [9].

Традиційно найбільш послідовну позицію у питанні застосування даної технології 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) [10].

Верховний комісар ООН з прав людини Мішель Башле у доповіді від 13 вересня 2021 р. «Право на недоторканність приватного життя в цифрову епоху» зазначив, що 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, а також дискримінації, у межах своєї юрисдикції, зокрема, встановити належні правові гарантії та інструменти для їхньої ефективної реалізації (п. 10 Доповіді) [11]. Дистанційне біометричне розпізнавання обличчя, згідно із Доповіддю Верховного комісара пов'язане з глибоким втручанням у приватне життя. Біометричні данні є одним з ключових ідентифікаторів особи, які дозволяють відрізнити від інших осіб. За твердженням Верховного комісара, дистанційна біометрична ідентифікація значно підвищує можливість державних органів систематично провадити ідентифікацію та спостереження за людьми в громадських місцях, підриваючи право людей на власне життя без стороннього нагляду та справляючи прямий

негативний ефект на такі права, як свобода висловлювань, свобода мирних зібрань і об'єднань та свобода пересування (п. 27 Доповіді). 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 мають бути введена заборонена не лише систем розпізнавання обличчя, а й розпізнавання за будь-якими іншими ознаками та віднесення будь-яких технологій віддаленої біометричної ідентифікації людей у режимі реального часу, соціальних рейтингів (проведених приватними та державними структурами), автоматичного правозастосування (як і будь-якого автоматичного ухвалення рішень, які торкаються прав та свобод людини) і технологій, що розпізнають емоції, за загальним правилом, до технологій із неприйнятним рівнем ризику [12].

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 приватним компаніями у громадських місцях; заборона на невибіркове розпізнавання осіб та обмеження лише особами, яких розшукують, встановлення підстав і процедури внесення людей до переліків розшукуваних.

Список використаних джерел:

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 Листопада 2018. URL: https://hromadske.ua/posts/yes-viprobuye-detektori-brehni-zi-shtuchnim-intelektom-na-kordonah-krayin

4. Kaiser Larsen Marinus Analytics fights human trafficking using Amazon Rekognition09 AUG 2018 URL: https://aws.amazon.com/blogs/machine-learning/marinus-analytics-fights-human-trafficking-using-amazon-rekognition/

5. Десять 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. Veliz C. The Power of BigTech and Ethics, GRC World Forums1 April 2021. URL: https://www.grcworldforums.com/on-demand-content/the-power-of-bigtech-and-ethics-carissa-veliz/1185.article

9. 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

10. 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

11. Bachelet. 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

12. 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