Запаранюк Андрій Васильович,
начальник сектору кримінального аналізу
ГУНП в Чернівецькій області

АКТУАЛЬНІ ПИТАННЯ ВПРОВАДЖЕННЯ ЄВРОПЕЙСЬКИХ СТАНДАРТІВ ЩОДО РОЗПІЗНАВАННЯ ОБ'ЄКТІВ ТА ОБЛИЧ У КРИМІНАЛЬНОМУ РОЗСЛІДУВАННІ (НА ПРИКЛАДІ НАУКОВИХ РОЗРОБОК ПРАВОЗАХИСНИХ ОРГАНІЗАЦІЙ ПРОВІДНИХ КРАЇН)

Штучний інтелект забезпечує використання біометричних технологій, зокрема програми розпізнавання об'єктів та обличь, які використовуються для верифікації, ідентифікації та категоризації приватними чи державними суб'єктами.

Сьогодні регулювання штучного інтелекту є актуальною темою. У 2020 році Рада ООН з прав людини прийняла резолюцію, яка конкретно засуджує використання технологій з розпізнавання обличь у контекст мирних протестів, оскільки ці технології створюють стримуючий вплив на реалізацію права на протест, розширюючи можливості урядів ідентифікувати, контролювати, переслідувати та залякувати протестувальників. Рада закликала держави утримуватися від використання технології розпізнавання обличь для моніторингу осіб, які беруть участь у мирних протестах. Рада Європи, європейська правозахисна організація зі штаб-квартирою в Страсбурзі, у січні 2021 року прийняла Рекомендації щодо розпізнавання обличь [4]. Ці рекомендації встановлюють заходи, яких уряди, розробники систем розпізнавання обличь, виробники, постачальники послуг та організації, що використовують FRT, мають дотримуватися та застосовувати, щоб гарантувати, що вони не порушують права людини та основні свободи будь-якої особи, включаючи право на людську гідність і на захист персональних даних. Рекомендації мають загальний обсяг і охоплюють використання FRT у приватному та державному секторах. Вони закликають до заборони використання особливо нав'язливих FRT і пропонують ввести запобіжні заходи. Майбутня робота Ради Європи над розробкою законодавчої бази для штучного інтелекту також, ймовірно, стосуватиметься норм, застосовних до розпізнавання обличчя. Крім того, існує двостороння співпраця, наприклад, з Радою з торгівлі та технологій, ЄС і США вирішили створити як платформу для трансатлантичного співробітництва та встановлення стандартів для нових технологій, таких як штучний інтелект [5].

Хоча існують реальні переваги використання систем розпізнавання обличь (об'єктів) для громадської безпеки, їх поширеність нав'язливість, а також схильність до помилок, викликають низку занепокоєнь щодо фундаментальних прав, наприклад, дискримінації певних сегментів населення та порушення права на захист даних та приватність.

Розвиток біометричного спостереження, зокрема технології розпізнавання обличчя (об'єктів), можна спостерігати в різних частина земної кулі. Згідно зі звітом Фонду Карнегі «За міжнародний мир» [1] станом на 2020 рік щонайменше 64 країни світу активно використовували системи розпізнавання обличь (об'єктів). Китай є одним із основних користувачів цієї технології. Наприклад, китайські школи використовують розпізнавання обличь, щоб контролювати бібліотечні позики та складати щорічні звіти про харчування кожного учня. Збільшення використання камер розпізнавання обличчя (об'єктів) в громадських місцях було задокументовано в ряді країн по всьому світу, наприклад у Киргизстані, Індії, Латинській Америці, Ізраїлі, США, Австралії, та РФ [3]. Також повідомлялось про те, що в РФ засоби стеження за допомогою штучного інтелекту, все частіше використовуються проти політичних дисидентів, правозахисників, а також осіб, що перебувають під карантинними обмеженнями в зв'язку з пандемією [3].

Дослідивши впровадження штучного інтелекту для розпізнавання обличь (об'єктів) в ряді провідних країн, виявлено наступні заходи вжиті для врегулювання використання вказаної технології:

ЄС запровадив суворі правила відповідно до Хартії основних прав, Загального регламенту захисту даних, Директиви про правоохоронну діяльність та рамок ЄС щодо недискримінації, як також застосовуються до процесів діяльності, пов'язаних з технологіями розпізнавання обличь (об'єктів). Однак різні фактори поставити під сумнів ефективність поточної системи ЄС у належному вирішенні проблем з фундаментальними правами, спричинених технологіями розпізнавання обличь. Навіть якби суди спробували усунути прогалини в захист шляхом розширеного тлумачення існуючої правової бази, правові невизначеності та складності залишалися.

В США, наразі немає федерального законодавства, яке б регулювало використання розпізнавання обличчя приватними компаніями або в контексті правоохоронних органів, окрім загально прийнятих правил конфіденційності. Разом з тим, Федеральна торгова комісія США відповідно до своєї місії із захисту споживачів випустила деякі рекомендації, в яких зазначено, що компаніям не слід вводити своїх споживачів в оману щодо того, як вони використовують алгоритми розпізнавання обличь [6]. Крім того, потенційні заборони, обмеження або мораторії на використання технології обговорюються по всій країні на рівні штатів і на місцевому рівні. Деякі міста США, такі як Сан-Франциско, Бостон і Портленд, заборонили технологію розпізнавання обличчя в громадських місцях і Штат Каліфорнія прийняв закон, який встановлює трирічний мораторій на будь-яку технологію розпізнавання обличчя, яка використовується в поліцейських натільних камерах з 1 січня 2020 р. Тим не менш, існуюча ланцюжок державних і місцевих законів і постанов не забезпечує правової визначеності для органів державної влади, промисловості та громадян. Крім того, відсутність послідовного

федерального підходу є відповідальністю для органів національної безпеки (таких як Центральне розвідувальне управління), які все частіше використовують технології з розпізнавання обличь. На цьому тлі лунають заклики регулювати використання технології розпізнавання обличчя в США за допомогою федерального законодавства, особливо в контексті стеження правоохоронних органів і, зокрема, для забезпечення єдиного вирішення проблем конфіденційності, що виникають через використання реальних технологія розпізнавання обличчя за часом. З цього приводу було зроблено ряд пропозицій, включаючи пропозицію прийняти Закон про конфіденційність комерційного розпізнавання обличчя від березня 2019 року, який загалом забороняє організаціям використовувати технологію розпізнавання обличчя для збору даних розпізнавання обличчя без надання сповіщення та отримання їхньої згоди. Кілька інших федеральних законопроектів, які регулюють використання технології розпізнавання обличчя, були запропоновані та все ще обговорюються.

У Китаї на сьогоднішній день немає чинних законів чи постанов, які чітко регулюють FRT. Розпізнавання обличь опосередковано регулюється Законом про кібербезпеку, який визначає деякі вимоги щодо збору, використання та захисту особистої інформації, включаючи біометричні дані. Однак у квітні 2021 року Національний технічний комітет із стандартизації інформаційної безпеки Китаю опублікував проект стандарту щодо вимог до безпеки даних розпізнавання обличь, метою якого є встановлення необов'язкових вимог щодо збору, обробки, обміну та передачі даних, які використовуються для розпізнавання обличь у Китаї. 249 Крім того, повідомляється, що китайські законодавці працюють над прийняттям нового закону про конфіденційність даних із сильним акцентом на біометрії, і що приватний сектор Китаю намагається вирішити проблеми конфіденційності, які виникають у зв'язку з використанням систем розпізнавання обличь, шляхом саморегулювання, зокрема з виданням керівництва та галузевих стандартів.

Науковці, зацікавлені сторони та політики в основному поділяють занепокоєння щодо дотримання основних прав, особливо щодо захисту даних і недискримінації, що випливає з дедалі більшого використання технологій розпізнавання обличь (об'єктів). Однак незаперечними є переваги такої технології, які можуть фактично покращити безпеку завдяки точнішій автентифікації та підвищеній безпеці.

Список використаних джерел

1. URL: https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf.

2. URL: https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

3. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653636/EXPO_STU(2021)653636_EN.pdf.

4. URL: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_264.

5. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2279.
6. URL: https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.
7. В роботі використано матеріали Європейської парламентської дослідницької служби «Регулювання розпізнавання обличь в ЄС» від вересня 2021 року.

Іванчук Наталія Віталіївна,
старший науковий співробітник відділу організації наукової діяльності та захисту прав інтелектуальної власності Національної академії внутрішніх справ, кандидат юридичних наук

КЛАСИФІКАЦІЯ ОЗНАК ПОТЕНЦІЙНО НЕБЕЗПЕЧНИХ ОСІБ В УМОВАХ ВОЄННОГО СТАНУ

Позитивні ознаки свідчать з великою ступеню вірогідності про відсутності зв'язку особистості з терористичною діяльністю. До них можна віднести: належність суб'єкта до роботи у правоохоронних органах; широку відомість людини у соціальному контурі; статус офіційного гостя, дипломата тощо.

Наявність негативних ознак є індикатором потенційного зв'язку між пасажиром та терористичним актом, що планується. Вони диференціюються на підозрілі та критичні.

Підозрілі ознаки вказують на значну вірогідність існування факту злочинного наміру у пасажира чи відвідувача чи його можливого використання кримінально-терористичними структурами для здійснення протиправних дій.

Привидами для підозри працівника правоохоронних органів чи служби безпеки повинні стати окремі ознаки у поведінці, зовнішньому вигляді пасажира та його документах. Якщо пасажир з'являється наприкінці огляду, коли працівник втомлений (його увага втрачає певну стійкість, обсяг, концентрацію), чи проявляє особливу невідповідну адекватній ситуації нервозність, наголошує на необхідності прискорення процедур огляду – це маркер, що зазначений суб'єкт може потенційно бути небезпечним та потребує особливої уваги з боку осіб, які забезпечують безпеку авіаперельотів.

Перевіряючи документи, які посвідчують особу, перевізні документи науковці вважають, що акцентувати увагу необхідно на наступних фактах:

невідповідність даних у паспорті, білетах, візі (наприклад, різні імена);

відсутність орієнтування у датах, проставлених у паспорті (чи завчене їх хронологічне відтворення);

явна нелогічність маршруту перельоту;