

конференції (28 лютого – 1 березня 2013 р.)/ Г. К. Авдеева – Тюмень: Тюменський державний університет, 2013. 73 с.

2. Практикум з криміналістики: навч. посібн./кол. авторів: В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін. / за ред. В. Ю. Шепітька – К.: Ін Юре, 2013 . 92 с.

3. Криміналістичний вісник: науково-практичний збірник / редкол.: І. М. Охріменко (голов.ред.) – К.: ДНДЕКЦ МВС України, 2021. 20 с.

Сушко Роман Олександрович,
завідувач відділу судової експертизи
Дніпропетровського науково-дослідного
експертно-криміналістичного центру
МВС України

АСПЕКТИ РОЗВИТКУ СИСТЕМ АВТОМАТИЧНОГО РОЗПІЗНАВАННЯ ОБЛИЧ В УКРАЇНІ

Автоматичне розпізнавання обличчя – це метод ідентифікації або перевірки особистості людини за допомогою унікальних характеристик її обличчя. Ця технологія фіксує, аналізує та порівнює моделі з деталей обличчя кількох людей. Його можна використовувати для перевірки особи на зображеннях, відео або в режимі реального часу [1]. У криміналістиці в нашій державі, на жаль, система автоматичного розпізнавання облич майже не використовується. Відеорежими з системою автоматичного розпізнавання облич встановлено в деяких великих містах, але вони функціонують під патронатом органів місцевого самоврядування і на законодавчому рівні їх використання не врегульовано. Однак в найближчому майбутньому зазначена система має багато перспектив. Як приклад можна відзначити Китай, який є справжнім флагманом у світі по впровадженню систем автоматичного розпізнавання облич. На теперішній час в Китаї крім розшуку злочинців та зниклих осіб вона використовується для посадки в поїзд, оплати покупок, доступу до відеоігор з обмеженням по віку, зняття готівки в банкоматі, ідентифікації громадян, які вчинили дрібні правопорушення та у багатьох інших випадках.

Однак в контексті криміналістики ми розглянемо розпізнавання обличчя що використовується правоохоронними органами для пошуку підозрюваних і зниклих безвісти людей. Це може допомогти знайти людей, які вчинили злочини, і допомогти їх негайно затримати, що в свою чергу допоможе набагато збільшити безпеку у суспільстві, оскільки рецидивна злочинність в нашій державі на даний момент складає близько 30 % [2], і це тільки за офіційною статистикою, не враховуючі латентні злочини. Також наявність таких систем дозволила б оперативно відслідковувати пересування як злочинців так і безвісно зниклих осіб, оперативно реагувати та планувати дії з їх розшуку.

Однак, на жаль, в нашій державі використання таких систем законодавчо не врегульовано, тому ні самих систем, ні способів наповнення їх інформацією та матеріалами для ідентифікації, ні підстав для використання у підрозділах органів внутрішніх справ поки немає.

При впровадженні в практичну діяльність Автоматичних систем ідентифікації обличчя потрібно звертати увагу на наступні аспекти:

1. Точність. Одне з найбільших занепокоєнь щодо технології розпізнавання обличчя – чи вона точна. Якщо це не так, для особи можуть настати несприятливі наслідки. Наприклад, особу можуть помилково ідентифікувати як підозрюваного у злочині та заарештувати. Людину можуть помилково ідентифікувати під час посадки на рейс і затримати охорону аеропорту. Досвід показує, що недопрацьоване програмне забезпечення має труднощі з розпізнаванням певних людей, зокрема афроамериканців, представників етнічних меншин, жінок та молодих людей. Щоб уникнути звинувачень у расовому профілюванні чи інших підступних цілях, важливі високі оцінки точності. Так в ст. 22 Загального регламенту про захист даних [3] забороняється автоматизоване прийняття рішень, тобто будь-яке «рішення, засноване виключно на автоматизованій обробці, включаючи профілювання, яке спричиняє щодо нього юридичні наслідки або подібним чином істотно впливає на нього». Виняток до цієї заборони, якщо це дозволено законодавством Союзу або держави-члена, яке передбачає відповідні гарантії прав і свобод суб'єкта даних, принаймні право на втручання людини з боку контролера. Це означає, що збіги, засновані на технологіях розпізнавання обличчя мають бути підтверджені людьми (наприклад, поліцейським), які оцінять всі наявні ознаки та ситуацію, і на основі цієї оцінки вживають заходів. Багато помилкових спрацьовувань на цьому етапі вже виключено.

2. Прозорість. Системи розпізнавання обличчя часто працюють, завантажуючи базу даних біометричних даних, зображень або відео в комп'ютер і дозволяючи штучному інтелектові встановлювати збіги. Цей процес зазвичай вимагає величезної кількості даних. Загальний регламент про захист даних (GDPR) вимагає, щоб під час збирання та використання публічної інформації їм надавалося пояснення того, як збираються та використовуються їхні дані. Навіть у країнах, які не підпадають під GDPR, усім сторонам, які беруть участь у цій технології, важливо розуміти, кому належать дані, які збираються, і як вони будуть використовуватися.

3. Безпека. Оскільки програми розпізнавання обличчя можуть зберігати великі обсяги даних, важливо, щоб ці програми мали найвищий доступний рівень безпеки. Також важливо, щоб постачальники, які співпрацюють з замовниками послуг адміністрування систем, мали відповідні заходи безпеки, щоб уникнути будь-яких загроз кібербезпеки. Однак на даний час українське законодавство прямо не відносить зображення обличчя до персональних даних, які є захищеними на законодавчому рівні. Тому, на відміну від адміністрування паспортних даних, адміністратори систем відеоспостереження не мають значного

інтересу у захисті такої інформації. Зазначена ситуація підлягає корегуванню як на законодавчому рівні, так і на рівні розробників систем.

Проте, крім питання захисту персональних даних, слід звернути увагу і на численні інші проблеми, які виникають внаслідок застосування відеокамер з функцією розпізнавання обличчя.

Ключовими серед них є:

- можливість незаконного комерційного використання даних (як-от, рекламний таргетинг, зокрема, і політичний);

- ризики дискримінації осіб через позитивні/негативні хиби системи, наявність інституційної дискримінації в суспільстві та подальшу її конвертацію в алгоритми системи;

- ризики неправомірного притягнення осіб до відповідальності, коли система неправильно співвідносить людину з зображенням (що вже трапилося у практиці Сполучених Штатів [4]);

- проблема статусу такої інформації як доказу у суді (зокрема, через відсутність правового регулювання);

- ймовірність порушення права на свободу вираження поглядів у частині захисту журналістських та адвокатських джерел;

- загрози для належної реалізації права на мирні зібрання (в тому числі створення «охолоджуючого ефекту» для активістів через страх притягнення до відповідальності внаслідок участі у мітингах, демонстраціях, протестах);

- можливість зловживань і використання систем для політичних переслідувань з боку держави, утисків вразливих та маргіналізованих груп тощо [5].

Найближчі 15–20 років наша держава може повністю перейти на біометричні паспорти та використання біометричних даних для ідентифікації особи. Звичайно під швидкий розвиток технологій потрібно буде розроблювати законодавчу та нормативно-правову базу для їх застосування, дотримання прав і безпеки громадян. Якраз більшість побоювань що до використання систем автоматичної ідентифікації облич пов'язано лише з відсутністю належного регулюючого законодавства та якісного підходу до роботи з такими технологіями. Закони про захист персональних даних прийняті вже в більшості країн Європи та дозволяють вже частково вирішувати дану проблему. Нашій країні ніщо не заважає застосовувати їх позитивний досвід у себе. Ще одним з факторів забезпечення безпеки запровадження таких систем є грамотний підхід до їх розгортання. Для страхування від перехвату цієї інформації зловмисниками, передача цих даних повинна здійснюватися з використанням технологій шифрування протягом усього процесу, а персональні дані мають бути знеособлені. Це дозволить здійснювати точну звірку біометричних та персональних даних тільки на захищених серверах.

Список використаних джерел

1. Hartwig B. The Benefits and Drawbacks of Automated Facial Recognition in Forensic Science / Ben Hartwig – URL:

<https://www.technologynetworks.com/applied-sciences/articles/the-benefits-and-drawbacks-of-automated-facial-recognition-in-forensic-science-341401>;

2. Статистичні данні Генеральної прокуратури України URL: https://old.gp.gov.ua/ua/stst2011.html?dir_id=114141&libid=100820&c=edit&_c=fo#.

3. URL: <https://gdpr-text.com/uk/>

4. URL: <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>

5. Центр демократії та верховенства права: Чи легально встановлювати на міських вулицях камери із системою розпізнавання облич? URL: <https://cedem.org.ua/analytics/kamery-rozpoznavannya-oblych/>.

Ткач Павло Ігорович,

старший судовий експерт сектору будівельних, земельних досліджень та оціночної діяльності відділу товарознавчих, гемологічних, економічних, будівельних, земельних досліджень та оціночної діяльності Одеського науково-дослідного експертно-криміналістичного центру МВС України

ВИЗНАЧЕННЯ ТА КЛАСИФІКАЦІЯ НЕРУХОМОСТІ

Нерухомість слугує базою для господарської діяльності та розвитку підприємств і організацій усіх форм власності. Саме через це процес формування ринку нерухомості в Україні характеризується бурхливим розвитком. Нерухомість є головним предметом дискусій та спорів під час приватизації державного і комунального майна, оренди та купівлі-продажу земельних ділянок, приміщень житлового та нежитлового секторів.

З теоретичної точки зору нерухомість трактують як земельну ділянку з усім нерухомим майном, яке є як над нею так і під нею. Таке трактування категорії «нерухомість» є загальним, всеохоплюючим визначенням об'єкта нерухомості.

Згідно законодавства України, зокрема Цивільного кодексу під нерухомістю розуміють земельні ділянки, а також об'єкти, що розташовані на них, переміщення яких є неможливим без їх знецінення та зміни призначення. Таким чином, головною особливістю нерухомості є її зв'язок із земельною ділянкою. Слід зазначити, що згідно вітчизняного законодавства до нерухомості відносять також об'єкти, що за своєю природою є рухомими: повітряні й морські судна, судна внутрішнього плавання, космічні об'єкти. Віднесення вказаних об'єктів до нерухомого майна пояснюється тим, що вони є дорогими і права на них підлягають державній реєстрації.

Розглядатися як нерухоме майно може підприємство у вигляді єдиного майнового комплексу. До останнього включають всі види