

Розвиток систем автоматичного розпізнавання облич: деякі аспекти розвитку в Україні

Роман Сушко

головний судовий експерт, Дніпропетровський НДЕКЦ МВС України,
м. Дніпро, Україна, e-mail: ronboss@ukr.net

Розглянуто таке явище, як автоматичне розпізнавання обличчя, його переваги та недоліки, а також перспективи його розвитку в Україні.

Ключові слова: обличчя; ідентифікація; автоматичні системи; біометрія; бази даних; особиста інформація; безпека.

Development of Automatic Face Recognition Systems: Certain Development Aspects in Ukraine

Roman Sushko

The paper deals with such a phenomenon as automatic face recognition, its advantages and disadvantages, as well as prospects for its development in Ukraine.

Keywords: face; identification; automatic systems; biometrics; databases; personal information; security.

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. Її можна застосовувати 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 застосовується. Відеокамери із 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 із впровадження систем автоматичного розпізнавання облич. Нині в Китаї, крім розшуку злочинців та зниклих осіб, вона застосовується для посадки в поїзд, оплати покупок, доступу до відеоігор із обмеженням за віком, зняття готівки в банкоматі, ідентифікації громадян, які вчинили дрібні правопорушення та в багатьох інших випадках.

Однак в контексті криміналістики ми розглянемо розпізнавання обличчя, що застосовується правоохоронними органами для пошуку підозрюваних і зниклих безвісти людей. Це може допомогти знайти людей, які вчинили злочини, і негайно затримати, що, в свою чергу, допоможе набагато покращити безпеку суспільства, оскільки рецидивна злочинність у нашій державі нині складає близько 30 % [2], і це тільки за офіційною статистикою, не враховуючи латентні злочини. Також наявність таких систем дозволила б оперативно відслідковувати пересування як злочинців, так і безвісти зниклих осіб, оперативно реагувати та планувати дії з їх розшуку. Однак, на жаль, в нашій державі застосування таких систем законодавчо не врегульовано, тому ні систем, ні способів наповнення їх інформацією та матеріалами для ідентифікації, ні підстав для використання в підрозділах органів внутрішніх справ поки немає.

Під час впровадження в практичну діяльність автоматичних систем ідентифікації облич потрібно звертати увагу на такі аспекти:

1. Точність. Одне з найбільших занепокоєнь щодо технології розпізнавання облич — 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 охороною аеропорту. Досвід свідчить, 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 або інших підступних цілях, важливі високі оцінки точності. У ст. 22 Загального регламенту про захист даних [3] заборонено 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 ЄС або держави-члена ЄС, яке передбачає відповідні гарантії прав і свобод суб'єкта даних, принаймні, право на втручання з боку контролера. Це означає, що збіги, засновані на технологіях розпізнавання обличчя мають бути підтверджені людьми (наприклад, поліцейським), які оцінять усі наявні ознаки та ситуацію і на підставі цієї оцінки вживатимуть 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 даючи змогу штучному інтелектові встановлювати збіги. Цей процес зазвичай вимагає величезної кількості даних. Загальний регламент про захист даних (GDPR) вимагає, щоб під час збирання публічної інформації та

користування нею їм надавалося пояснення того, як збираються 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 ними будуть користуватися.

3. Безпека. Оскільки програми розпізнавання обличчя можуть зберігати великі обсяги даних, важливо, щоб ці програми мали найвищий рівень безпеки. Також важливо, щоб постачальники, які співпрацюють із 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 до захисту 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 унаслідок 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 із зображенням (що вже трапилося

у практиці Сполучених Штатів Америки [4]);

- проблема статусу такої інформації як доказу в суді (зокрема, через відсутність правового регулювання);
- імовірність порушення права на свободу вираження поглядів у частині захисту журналістських та адвокатських джерел;
- загрози для належної реалізації права на мирні зібрання (зокрема, створення «охладжуючого ефекту» для активістів через страх притягнення до відповідальності внаслідок участі в мітингах, демонстраціях, протестах);
- можливість зловживань і застосування систем для політичних переслідувань із боку держави, утисків вразливих та маргіналізованих груп тощо [5].

У 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 розробляти 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 регулювального законодавства та якісного підходу до роботи з такими технологіями. Зако-

ни про захист персональних даних прийняті в більшості країн Європи та дають змогу частково розв'язувати дану проблему. Нашій країні ніщо не заважає застосовувати їх позитивний досвід. Ще одним із чинників забезпечення безпеки запровадження таких систем є грамотний підхід до їх розгортання. Для страхування від перехвату інформації зловмисниками передавання цих даних має здійснюватися із застосуванням технологій шифрування протягом усього процесу, а персональні дані мають бути знеособлені. Це дасть змогу здійснювати точне звіряння біометричних та персональних даних тільки на захищених серверах.

Перелік джерел посилання

1. Hartwig B. The Benefits and Drawbacks of Automated Facial Recognition in Forensic Science. URL: <https://bit.ly/3NVKD8w> (дата звернення: 10.09.2024).
2. Статистичні данні Генеральної прокуратури України. URL: <https://bit.ly/3aT6fDS> (дата звернення: 10.09.2024).
3. URL: <https://gdpr-text.com/uk/> (дата звернення: 11.09.2024).
4. URL: <https://nyti.ms/3HqmZ1H> (дата звернення: 11.09.2024).
5. Центр демократії та верховенства права: Чи легально встановлювати на міських вулицях камери із системою розпізнавання облич? URL: <https://bit.ly/3xVfE6X> (дата звернення: 12.09.2024).