**Міністерство освіти та науки України**

**Національний університет «Києво-Могилянська академія»**

**Факультет правничих наук**

*Кафедра приватного права*

**МАГІСТЕРСЬКА РОБОТА**

освітній ступінь – магістр

на тему:

**«Правове регулювання технологій розпізнавання обличчя в ЄС, США та Україні: приватно- та публічно-правовий аспекти»**

(«Legal regulation of facial recognition technologies in the EU, the USA and Ukraine: private and public law aspects»)

***Виконала:***

Гуменюк Вероніка Іванівна,

студентка 2 року навчання магістерської програми

e-mail: veronika.humeniuk@ukma.edu.ua

***Науковий керівник:***

Смирнова Тетяна Сергіївна,

к.ю.н., доцент кафедри приватного права

Рецензент_____

Магістерська робота захищена з оцінкою_____

Секретар ЕК_____

«__» _____ 2024 р.

**Київ – 2024**

# Декларація академічної доброчесності

Я, Гуменюк Вероніка Іванівна, студентка 2 року навчання магістерської програми за спеціальністю „Право" факультету правничих наук НаУКМА підтверджую таке:

- написана мною магістерська робота на тему „Правове регулювання технологій розпізнавання обличчя в ЄС, США та Україні: приватно- та публічно-правовий аспекти" („Legal regulation of facial recognition technologies in the EU, the USA and Ukraine: private and public law aspects") відповідає вимогам академічної доброчесності та не містить порушень, передбачених п. 3.1. Положення про академічну доброчесність здобувачів освіти у НаУКМА, зі змістом якого я ознайомлена.

01.05.2024 р. В. І. Гуменюк

**ЗМІСТ**

# ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

| | | |
|---|---|---|
| AI Act | - | Artificial Intelligence Act |
| CCPA | - | California Consumer Privacy Act |
| EDPB | - | European Data Protection Board |
| EDPS | - | European Data Protection Supervisor |
| FRT | - | Facial Recognition Technology |
| GDPR | - | General Data Protection Regulation |
| LED | - | Law Enforcement Directive |
| КПК України | - | Кримінально-процесуальний кодекс України |
| ЄС | - | Європейський Союз |
| ЄСПЛ | - | Європейський суд з прав людини |
| США | - | Сполучені Штати Америки |
| ШІ | - | штучний інтелект |

# ВСТУП

Останнім часом набирає обертів розвиток таких сучасних технологій як розпізнавання обличчя (або ж facial recognition). Фахівці інформаційних технологій досягають успіхів у збільшенні результативності розпізнавання при розробленні цих технологій, що дає підґрунтя для їх все більшого використання.

Саме у зв'язку з цим зауважимо, що наше дослідження буде релевантним, зокрема, *актуальність* проявляється у тому, що в Україні та у світі ці технології використовуються активно, що наслідком має проблематику захисту прав людини при використанні технологій розпізнавання обличчя. Також актуальність дослідження правового регулювання саме в Європейському Союзі (далі – ЄС), Сполучених Штатах Америки (далі – США) та Україні проявляється у тому, що:

1) в ЄС зараз нормативне регулювання охоплює найбільше коло правовідносин, пов'язаних з використанням технологій розпізнавання обличчя;
2) в США знаходяться головні офіси найбільших технологічних гігантів світу (наприклад, «Google», «Meta» (колишній «Facebook»), «Microsoft», «Amazon», «Apple» тощо), які рухають технологічний розвиток і можуть впливати на регулювання технологій розпізнавання обличчя;
3) в Україні правове регулювання цих технологій є обмеженим попри широке застосування.

У межах цієї роботи ми виокремили *дослідницьке питання,* яке сформулювали так: чи існує (та яким є) нормативне регулювання використання технологій розпізнавання обличчя та чи є воно достатнім в ЄС та США, а також в Україні?

Відповідно, *об'єктом нашого дослідження* є сфера правового регулювання інформаційних технологій, зокрема у контексті технологій розпізнавання обличчя. *Предметом* же є правотворча та правозастосовна практика в ЄС, США та Україні щодо використання технологій розпізнавання обличчя, зокрема, у

сферах цивільного права, захисту персональних даних, кримінального процесуального права, адміністративного права та прав людини.

*Мета* роботи проявляється у дослідженні нормативно-правових актів цієї сфери на сучасному етапі та аналізі проблемних аспектів правового регулювання використання згаданих технологій у приватній та публічній сферах в ЄС, США та Україні.

Успішне досягнення цієї мети полягає у виконанні таких *завдань*:

1) З'ясувати, яким чином створюються та функціонують технології розпізнавання обличчя.
2) Виокремити галузі, сфера регулювання яких поширюється на вказані технології, щоб визначити напрямок для аналізу актів.
3) Дослідити та віднайти особливості правотворчої та правозастосовної практики при використанні технологій розпізнавання обличчя у цивільно-правовому аспекті в ЄС, США та Україні.
4) Дослідити та віднайти особливості правотворчої та правозастосовної практики при використанні технологій розпізнавання обличчя у публічно-правовому аспекті в ЄС, США та Україні.
5) Зрозуміти, чи наявне зараз правове регулювання застосування цих технологій є достатнім для правовідносин в ЄС, США та Україні та які перспективи для його розвитку.

З упевненістю можемо сказати, що *ступінь наукової розробки проблеми* є порівняно значним, оскільки проблематику цієї теми описали багато дослідників. Ними, зокрема, є Т. Авдєєва [61, 63], Г. Аніуліс [3], Б. Баклі [9], Р. Косерару [30], А. Людва [61], Т. Мадієга [2], Г. Мілдебрат [2], В. Рапосо [44], Е. Роу [32], М. Хантер [9] та інші. Проте зауважимо, що наукові розробки щодо правотворчості та правозастосування в Україні з питань штучного інтелекту, який використовується у технологіях розпізнавання обличчя, потребують доопрацювання.

Для виконання поставлених завдань ми використали низку загальних та спеціальних методів.

Серед *загально-наукових методів* ми використали аксіологічний – при оцінці відповідності технологій розпізнавання обличчя загальнолюдським цінностям; антропологічний – при дослідженні відповідності таких технологій базовим правам людини; аналітичний – при конструюванні аналізу нормативного та правозастосовного регулювання цих технологій; експеримент – при використанні генеративного штучного інтелекту, щоб дослідити у межах, які б не порушували права інших людей, емпіричним шляхом, як може здійснюватися розпізнавання обличчя; системно-структурний – для дослідження місця цих технологій у системі правових явищ; феноменологічний – при відокремленні елементів цих технологій для фокусування на важливих аспектах та досягнення якомога ефективнішого дослідження предмета; синергетичний – при дослідженні цього питання у взаємозв'язку права зі сферою інформаційних технологій, а також емпіричний метод експерименту – при дослідження функціонування генеративного штучного інтелекту при запиті розпізнати обличчя та емоції особи, зображеної на фото.

Серед *спеціально-наукових методів* правових досліджень ми використали формально-юридичний – для відображення регулювання сфери технологій розпізнавання обличчя в ЄС, США та Україні на рівні нормативно-правових актів; порівняльно-правовий – для ілюстрації у нашому дослідженні порівняльної характеристики підходів до розуміння проблематики правового регулювання цих технологій у різних галузях права; логіко-юридичний – при виокремленні проблем правового регулювання та при побудові пропозицій для подолання потенційних прогалин та порушень з метою відповідності позитивного права підходу природного права.

# РОЗДІЛ 1. ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ ТЕХНОЛОГІЙ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ

## *1.1. Технологічні особливості*

У сучасному світі технології розпізнавання обличчя (далі – FRT) набули досить широкого вжитку і в майбутньому потенційно будуть застосовуватися набагато частіше.

FRT тепер не є предметом наукової фантастики або занепокоєнь щодо майбутнього. Вони вже впливають на життя людей щодня [1].

Для розуміння функціонування та потенціалу цих технологій, наведу приклади застосування, які ілюструють поширеність використання FRT.

Зокрема, прикладом є насамперед використання камер спостереження з функцією розпізнавання обличчя для забезпечення громадської безпеки та пришвидшення виявлення правопорушників органами правопорядку. Аналогічно ця технологія використовується на митницях та в аеропортах. Згадане стосується здебільшого сфери публічного порядку.

Щодо приватної сфери, то прикладами можуть бути встановлення захисту через розпізнавання обличчя для обмеження доступу до гаджетів або ж навіть приміщень. Також банки або брокерські компанії можуть використовувати ці технології для ідентифікації та автентифікації клієнта.

Результати використання цих технологій справді можуть бути помічними, проте цікавим є й питання, як саме вони досягаються та реалізуються.

Найпримітивніше пояснення цих технологій – це програми на основі штучного інтелекту, який здійснює певні операції, щоб досягти визначеної розробником мети. Як вказують Т. Мадієга та Г. Мілдебрат, операції, які може виконувати програма, мають досить широкий спектр: від просто перевірки наявності обличчя на зображенні, до більш складних. Вони виділяють такі:

- верифікація – порівняння двох зразків біометричних даних для з’ясування, чи перший екземпляр відповідає другому;

- ідентифікація – порівняння одного зображення з іншими, які зберігаються у базі даних, щоб визначити, чи це зображення належить до цієї бази; та
- категоризація (або класифікація) – віднесення певних зображень до груп, відсортованих за певною ознакою [2, с. 2].

Загалом, FRT – це біометрична технологія, яка зазвичай використовує три частини:

1) камеру для отримання цифрового зображення;
2) базу даних збережених зображень для порівняння; та
3) алгоритм, який створює відбиток обличчя з отриманого зображення і порівнює його з базою даних зображень [3, с. 1515].

Важливо, що камеру і базу даних можна замінити різними джерелами, зокрема: технологіями громадського спостереження (наприклад, системами відеоспостереження), урядовими базами даних (наприклад, тими, що містять ліцензійну та паспортну інформацію), а також веб-сайтами (наприклад, Facebook). [3, с. 1515-1516].

Програмним кодом описують алгоритм, якому слідує штучний інтелект при машинному навчанні.

Машинне навчання, за своєю суттю, покликане імітувати процес засвоєння інформації, як це робить людський розум [4].

Так-от, ці логічні правила є планом для штучного інтелекту, за яким він аналізує значну кількість інформації у вигляді зображень облич та перетворює проаналізовану інформацію у цифрове вираження, щоб таким чином він міг порівнювати їх [5].

У цьому цифровому вираженні, як правило, відображається сукупність певних параметрів, які залежать від побудови алгоритму.

Проблема в тому, що зображення облич створюються за різного освітлення, обстановки, кута до об’єктива тощо. Саме тому штучному інтелекту слід проаналізувати кілька фото, щоб на їхній основі створити 3D модель обличчя та використовувати при FRT саме її для досягнення якомога точнішого результату [6].

Створення 3D моделі обличчя є одним із видів алгоритмів, за яким функціонують FRT.

FRT можуть поділятися на декілька видів залежно від методів, за якими вони аналізують зображення: такі, що аналізують лише деякі риси, а не все обличчя (здебільшого концентруються на таких основних рисах як ніс, очі та губи); такі, які аналізують все обличчя, не виокремлюючи певні риси; гібридні, які використовують характеристики попередніх двох методів [7].

Машинне навчання допомагає штучному інтелекту вивчити стільки параметрів, що стає можливим з досить високою точністю ідентифікувати людину, навіть якщо та в сонячних окулярах, головному уборі або захисній масці [8].

З огляду на особливості функціонування, система за результатами аналізу дає певну оцінку за встановленою шкалою.

Остаточна відповідь в алгоритмі досягається за допомогою простої операції встановлення порогу несхожості [6].

Крім того, FRT може використовуватися не лише для ідентифікації особи, а й для визначення певних характеристик особи таких як, наприклад, статі, віку, емоційного стану [9, с. 638].

Загалом, ці технології є досить ефективними. Проте цікавим та неймовірно важливим є питання захисту прав особи при використанні цих технологій, оскільки слушною є думка, що зображення людини з її лицем може бути отримано набагато легше, ніж відбитки пальців [10, с. 4].

### *1.2. Сфера правового регулювання*

Варто також зосередитися на питанні, якою галуззю регулюється використання FRT.

Вважаю, що для належного дослідження, варто розглянути окремо нормативне регулювання щодо:

а) суб’єкта, який застосовує FRT; та

б) об’єкта, до якого застосовується FRT.

*Щодо суб’єкта, який застосовує FRT*

З огляду на різні цілі використання технологій розпізнавання обличчя, їх можуть застосовувати як суб’єкти приватного, так і публічного права.

У приватно-правовій сфері часто суб’єкт та об’єкт застосування FRT є однією особою. Як правило, користувачі програмного забезпечення самостійно погоджуються на обробку зображень, до прикладу, при обробці зображень відповідними фільтрами у застосунках, сканування обличчя для розблокування доступу до гаджету або приміщення, для ідентифікації особи при використанні банківських застосунків або застосунку «ДіЯ». У приватній сфері FRT має широке коло випадків застосування. Зазвичай таке застосування базується на активній або пасивній згоді об’єкта щодо якого застосовується FRT.

У публічно-правовій сфері суб’єктами, що застосовують FRT є, як правило, державні або муніципальні органи. Ледь не найпоширенішим є застосування цих технологій для слідкування за дотриманням публічного правопорядку та правил перетину держаного кордону. Тому такі технології застосовуються органами правопорядку, митними органами, військовими тощо. Є деякі випадки, за яких приватні компанії та організації також застосовують FRT для дотримання публічно-правових положень, зокрема, норм адміністративного права, про що детальніше згадуємо у Розділі 3.

*Щодо об’єкта, до якого застосовується FRT*

Як було описано вище, обличчя людини – це об’єкт, який аналізується цими технологіями. Цілком зрозуміло, що обличчя – персональні дані певного індивіда. Нижче розглянемо, чому це твердження є раціональним.

Під персональними даними відповідно до ЗУ «Про захист персональних даних» [11] розуміються відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. На нашу думку, це досить широка дефініція, що не забезпечує визначеності.

Як відомо, найбільшого рівня регулювання у сфері захисту персональних даних було досягнуто в ЄС. Зокрема, прийнятий регламент про захист

персональних даних – General Data Protection Regulation (далі – GDPR) [12] – має більш ґрунтовні норми, які регулюють вказане питання. У ньому надано розширену дефініцію, зокрема, під персональними даними розуміється інформація, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати. Проте вказується, що саме може вважатися такими ідентифікаторами: ім'я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор або ж один чи сукупність факторів, характерних для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної ідентичності такої особи.

Тож, з буквального тлумачення цих норм можемо стверджувати, що обличчя людини є персональними даними, бо воно дає змогу ідентифікувати особу.

Більш того, цей акт у статті 9, а також Закон України «Про захист персональних даних» у статті 7, виділяють так звані особливі категорії даних, до яких належать дані про расову або етнічну приналежність, релігійні, політичні погляди, членство у професійних спілках, а також генетичні та біометричні дані, дані про здоров'я, сексуальне життя або сексуальну орієнтацію.

Аналогічно, до прикладу, і в Каліфорнії, США (один із небагатьох штатів, який має власне правове регулювання питання захисту персональних даних) у California Consumer Privacy Act, який був змінений California Privacy Rights Act (далі – CCPA) [13], виділяють також подібний вид персональних даних – чутлива персональна інформація. До неї подібним чином відносять генетичні та біометричні дані, а також ще й геолокацію особи, реєстраційні соціальні номери, паспортні дані тощо.

Зауважимо, що важливість виокремлення спеціальних, або ж чутливих, даних є необхідним задля привернення уваги до потреби у забезпеченні більш надійного захисту таких даних та впровадженні складніших механізмів доступу, передачі, обробки та знищення.

Акцентуємо увагу саме на біометричних даних як частині особливої категорії даних.

Е. Устаран вказує, що прикладами біометричних даних можуть бути ДНК, відбитки пальців, долоні, візерунки судин, сітківка та райдужна оболонка ока, запах, голос, почерк, техніка натискання клавіш, хода та, звісно ж, обличчя [14, с. 360]. Такий підхід прийнятий також за GDPR та CCPA.

З цього випливає, що об'єктом використання FRT є саме обличчя людини. Ба більше, не кожне обличчя людини за замовчуванням є об'єктом, до якого застосовуються FRT. Звісно ж, дослідження об'єкта за допомогою FRT залежить від контексту використання таких технологій, що розкриємо у наступних розділах.

Хочемо також наголосити, що враховуючи різні цілі, на які може бути спрямоване використання FRT, можна виокремити різні особливості правового регулювання. До прикладу, для функціонування FRT створюють певні бази з даними про осіб, тому є й важливим, відповідно до чого такі бази даних були сформовані. Ми розуміємо, що FRT залежні від баз даних, але все ж таки намагаємося орієнтувати своє дослідження суто на правове регулювання використання FRT, без концентрування на формуванні баз даних, оскільки вважаємо, що це питання трохи виходить за межі предмета цього дослідження, залишаючи простір для подальших наукових розробок.

Зі згаданого стає зрозуміло, що використання FRT здебільшого регулюється законодавством про захист персональних даних, що забезпечує охорону права на приватне життя. Проте таке регулювання перебуває у тісному зв'язку з процедурними нормами щодо застосування спостереження за особами і правами на мирні зібрання, на свободу вираження поглядів та забороною дискримінації, що проявляється у контексті адміністративного та кримінально-процесуального права.

Відповідно, зауважимо, що у наступних розділах ми розглянемо застосування FRT у приватно- та публічно-правових сферах. Ми виокремлюємо приватно-правове і публічно-правове регулювання, ґрунтуючись на різниці у методах, зокрема, для приватно-правового це – диспозитивний, а для публічно-правового – імперативний. Відповідно, у частині щодо приватно-правового

аспекту ми з’ясуємо, наскільки використання цих технологій є зарегульованим у площині приватного права, а у публічно-правовому аспекті – розглянемо застосування FRT органами державної та муніципальної влади, розкриємо застосування FRT у контексті адміністративного та кримінально-процесуального права, а також узагальнимо проблеми, з якими наразі зіткнулася спільнота у зв’язку з такими технологіями.

*  *  *

Тож, у цьому розділі розглянули засади функціонування FRT у технічному сенсі та у правовому полі.

Під час дослідження з’ясували, що суть цих технологій зводиться до слідування певному алгоритму для досягнення заздалегідь встановленої мети: верифікувати, ідентифікувати або категорізувати особу, провівши аналіз її зображення (або зображень).

Враховуючи природу цих технологій, для них слід використовувати персональні дані фізичних осіб. Відповідно, ми дослідили, що для їхнього функціонування збираються та обробляються дані про обличчя особи, які вважають біометричними даними. Біометричні дані належать до категорії особливих (чутливих) персональних даних, що підкреслює необхідність їхньої охорони складнішими правовими заходами.

З огляду на досліджене, ми дійшли висновку, що використання зображення обличчя фізичної особи при FRT регулюється здебільшого нормативними положеннями зі сфери захисту особливих (чутливих) персональних даних, проте оскільки окрім приватних суб’єктів, органи державної та муніципальної влади також застосовують FRT, норми адміністративного, кримінально-процесуального права та загальні засади прав людини також мають бути дотримані.

# РОЗДІЛ 2. ПРАВОВЕ РЕГУЛЮВАННЯ ТЕХНОЛОГІЙ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ У ПРИВАТНО-ПРАВОВОМУ АСПЕКТІ В ЄС, США ТА УКРАЇНІ

## *2.1. Приклади застосування FRT у приватно-правовому аспекті*

У цьому розділі ми розглянемо, як функціонує FRT у приватно-правовому аспекті, тобто з позиції забезпечення приватно-правових інтересів. На наш погляд, виокремлення дослідження тематики у контексті цивільно-правової сфери є цікавим та малодослідженим. Тому цим ми прагнемо внести наукову новизну до напрацювань щодо предмета дослідження.

З розвитком розуміння приватності та загроз для неї зростала і потреба в регулюванні як державних, так і приватних організацій. Відповідно, загрози, пов'язані з FRT не обмежуються лише державними установами, але можуть поширюватися і на приватний сектор [3, с. 1518]

FRT у приватно-правовій сфері застосовується у доволі широкому колі випадків, і пересічні користувачі не завжди усвідомлюють, наскільки такі технології є поширеними.

Спершу розглянемо приклади застосування FRT у цій сфері, щоб подальший аналіз був більш зрозумілим та наочним.

Вони можуть бути такими за прямої або непрямої згоди суб'єкта, щодо якого застосовується FRT.

- *регулювання доступу до приміщень*

Зокрема, технологія може застосовуватися для збільшення безпеки за рахунок більш складного доступу до об'єктів нерухомості, студентських кампусів та гуртожитків. Крім того, зображення обличчя, яке сканується FRT, можна використовувати замість квитка на авіаперельот або концерт. Так само ці технології застосовують і для отримання доступу до автомобілів [15].

- *вхід до гаджетів та застосунків*

Через FRT особа може ефективно обмежувати доступ до своїх гаджетів та застосунків, щоб зберігати свою чутливу інформацію надійно, але водночас, зручно до неї отримувати доступ, без необхідності щоразу вводити паролі.

- *запобігання крадіжкам у магазинах* [16, с. 23]
- *оплата товарів та послуг тощо*.

Думаємо, що багато хто зустрічався з можливістю оплати товарів у продуктових супермаркетах в Україні. Програмно така можливість реалізована через FacePay24 – функцію, яку можна активувати через застосунок КБ АТ «Приватбанк» «Privat24» та безконтактно розраховуватися у багатьох магазинах України, де встановлений POS-термінал на Android [17].

Також цікавим прикладом у цьому контексті є верифікація особи при купівлі державних облігацій через застосунок «ДіЯ». У такому випадку застосовується ДіЯ.Підпис, доступ до якого отримується, зокрема, через перевірку за фото [18]. Тобто відбувається обробка обличчя із зробленого у відповідний момент фото, і порівнюється із наявними у базі «ДіЯ» зображеннями власника. До прикладу, фотографією з паспорта, водійського посвідчення, студентського квитка тощо.

Без згоди суб’єкта, щодо якого застосовується FRT, як правило, ці технології можуть використовуватися для досягнення законних інтересів (за GDPR – «legitimate interests») – коли ціль, яку прагнуть досягнути, є пропорційною та виправданою, щоб використовувати персональні дані осіб без їхньої прямої згоди, за умови, що потреби захисту основоположних прав і свобод такої особи не переважають такі законні інтереси.

Яскравим прикладом застосування FRT без згоди суб’єкта є законний інтерес щодо досягнення маркетингових цілей, включно з таргетованою рекламою. Зокрема, через такі технології опрацьовується зібрана інформація, щоб згодом провести її оцінку та виявити певні тенденцій для просування продуктів та/або послуг, оцінити рівень задоволеності клієнтів обслуговуванням тощо. Від цього отримують вигоду як суб’єкти господарювання, так і споживачі. Суб’єкти

підприємницької діяльності отримують змогу збирати, володіти та обробляти ринкову інформацію, яка, за належного застосування, може сприяти покращенню багатьох напрямків ведення бізнесу. Зокрема, обслуговування клієнтів, оцінка успішності маркетингових стратегій, розвиток нових підходів, таргетування рекламних матеріалів лише на конкретну аудиторію, яка найімовірніше зацікавиться продуктом та буде більш схильна придбати його тощо. Споживачі ж отримують більш підходящі за їхніми інтересами рекламні матеріали товарів, робіт або послуг, а також клієнтський сервіс, який підлаштований під їхні конкретні потреби, пріоритети та уподобання.

У своїй думці Офіс Уповноваженого з питань інформації у Великій Британії вказує, що йому відомо, що контролери можуть використовувати FRT в реальному часі для отримання маркетингової інформації або для доставки рекламних продуктів [19, с. 17], проте закликає контролерів забезпечити, щоб обробка біометричних даних була справедивою, необхідною, пропорційною та прозорою [19, с. 20].

Цікавим прикладом цього можна назвати наміри, які були у відомо виробника одягу та взуття Adidas разом з виробником напівпровідникових елементів та пристроїв Intel щодо створення та встановлення цифрових панелей на стіни, які б демонстрували рекламу для особи, яка проходить повз, орієнтуючись, до прикладу, на її стать та вік [20].

Зі згаданих прикладів стає зрозуміло, що застосування FRT у приватно-правовій сфері, як правило, залежить від згоди суб’єкта, щодо якого такі технології застосовуються. Поза волею такого суб’єкта технології можуть застосовувати лише для досягнення так званих «законних інтересів» або «життєвоважливих інтересів».

Вказані приклади чудово демонструють, що використання FRT у приватно-правовій сфері неможливе без дотримання законодавства про захист персональних даних. Це не дарма, бо застосування цих технологій тісно пов’язане з тим, на аналіз чого вони спрямовані, а саме із зображенням обличчя людини. Як з’ясували у Розділі 1, обличчя людини є її персональними даними. Ба більше,

воно належить до категорії чутливих персональних даних, що зобов'язує суб'єктів, які використовують FRT, ставитися до захисту таких даних з більшою обачністю.

Саме ж застосування суто FRT, без прив'язки до зображення особи, не є предметом цього дослідження, бо на практиці технології без зісканованих зображень або зображень з баз даних не мають жодного сенсу. Камера, яка має функцію FRT, без використання зображення людини стає просто звичайною камерою відеоспостереження, яка може аналізувати інші об'єкти, в надії розпізнати обличчя. І вона хоч також обмежує права людини на приватність, проте не так агресивно, як це завдається застосуванням FRT щодо обличчя людини.

Тож, ці приклади застосування дають підстави зрозуміти, що правове регулювання застосування FRT у приватній сфері має бути у відповідності до: (1) прав людини (зокрема, статті 8 Конвенції про захист прав людини та основоположних свобод [21]), чому кореспондує захист персональних даних; (2) цивільно-правових норм та принципів.

Пропонуємо детальніше розглянути засади та проблемні аспекти цих підпунктів.

## *2.2. Особливості захисту персональних даних при використанні FRT у приватно-правовому контексті в ЄС, США та Україні*

У контексті прав людини основоположним правом, яке може обмежуватися FRT у приватно-правовому аспекті є право на повагу до приватного і сімейного життя, закріплене статтею 12 Загальної декларації прав людини [22] та статтею 8 Конвенції про захист прав людини і основоположних свобод.

Цілком зрозуміло, що користуючись такими технологіями суб'єкти приватного права повинні зважати, щоб таке використання відповідало засадам захисту прав людини. Як згадували у Розділі 1, застосування FRT може відбуватися як за прямою або непрямою згодою особи, щодо якої їх застосовують,

так і без згоди такої особи, але з метою переслідування законних інтересів. У контексті застосування без згоди власника персональних даних постає доволі дискусійна конфронтація приватних інтересів індивіда – об'єкта застосування FRT, та інтересів (переважно) суб'єктів господарювання – суб'єктів застосування FRT.

Балансування вказаних інтересів є дуже важливим, оскільки, з одного боку, права людини є віхою розвитку праворозуміння країн західного світу і вважаються тим демократичним благом, яке слід належним чином захищати, але з іншого боку, є інтереси бізнесу, які частково переплетені з публічними інтересами, бо підприємці реалізовують власні права на свободу підприємницької діяльності, а держава у цей час отримує блага у вигляді робочих місць, податків та інших платежів.

У цьому контексті ми вбачаємо дві конфронтації – (1) право людини на приватне життя та (2) право людини на свободу підприємницької діяльності. Складність полягає в тому, що використання FRT хоч і може забезпечувати право людини на свободу підприємницької діяльності, є водночас значною загрозою для права на приватне життя. І, як відомо, права людини не мають заздалегідь встановленої сили або ієрархії.

Як слушно зауважує Жозеп Боррель, Високий представник Європейського Союзу з питань закордонних справ і політики безпеки, світ погодився з універсальністю, взаємозалежністю та неподільністю прав людини. Це означає, що не існує ієрархії прав, де одні мають перевагу над іншими, або що існують культурні чи географічні винятки. Всі люди, де б вони не жили, мають ці права і мають право на їх захист [23].

Логічним є прагнення забезпечити та захистити обидва права, проте з огляду на специфіку FRT, це близьке до неможливого. Об'єкт, до якого застосовується FRT, як правило, перебуває у слабшій позиції, ніж суб'єкт, який застосовує ці технології. Проте нормотворці знайшли важелі впливу, які сприяють збалансуванню. Ними є норми щодо захисту персональних даних та обмеження процедурних аспектів застосування FRT.

Пропонуємо у цій частині розділу розглянути особливості захисту персональних даних осіб при використанні FRT та особливості застосування цих технологій, враховуючи, що в основі FRT лежить застосування штучного інтелекту.

Використання FRT приватними суб'єктами господарювання є предметом занепокоєння органів захисту персональних даних у всьому світі.

У ЄС до обробки персональних даних приватними компаніями, в тому числі за допомогою FRT, застосовується GDPR. Цей акт вимагає, щоб обробка персональних даних була законною, справедливою та прозорою, а також щоб особи були проінформовані про обробку їхніх даних. GDPR також надає особам певні права, такі як право на доступ до своїх персональних даних, їхнє виправлення та видалення. Використання FRT приватними суб'єктами господарювання повинно відповідати цим вимогам і поважати право на приватне життя.

У США немає прийнятого федерального закону, який би регулював FRT по всій країні. Проте відповідні акти останнім часом активно приймаються на рівні штатів. Наприклад, у Каліфорнії прийняли CCPA, який є чи не єдиним базовим масштабним актом щодо захисту персональних даних. Цей акт регулює лише частину відносин, де використовується FRT. Це викликано тим, що CCPA (зі змінами, внесеними California Privacy Rights Act) поширює свою дію здебільшого на суб'єктів, які отримують прибуток [24]. Підкреслюємо, що він прийнятий на рівні штату, тобто його дія обмежується територією штату та його населенням. Також у Вірджинії прийняли Virginia Consumer Data Protection Act, який має багато спільного із CCPA та аналогічно поширюється також і на суб'єктів господарювання [25].

Варто згадати і штат Іллінойс. Тут у 2008 році прийняли більш деталізований закон щодо захисту саме біометричних даних – Biometric Information Privacy Act [26]. За ним заборонено використовувати такий вид даних без прямої згоди особи. Більш того, за цим актом до біометричних даних аналогічно включають геометрію обличчя.

Щодо України, то законодавство не містить спеціальних норм, спрямованих на регулювання використання FRT у приватно-правовому аспекті. Безперечно, у будь-якому випадку, у разі відсутності спеціальних норм, таке використання має відповідати загальним нормам, зокрема, Конституції України та ЗУ «Про захист персональних даних».

На ньому наголошує й Уповноважений Верховної Ради України з прав людини, вказуючи, що українське законодавство про захист персональних даних не містить заборони встановлювати у торговельних приміщеннях або на їхніх фасадах камери відеоспостереження, проте воно зобов'язує знайти баланс між інтересами закладу встановити відповідні технології та правом на приватність. Водночас, суб'єкти персональних даних мають право знати про механізм автоматичної обробки їхніх персональних даних через FRT [27, с. 6-7]. Уповноважений Верховної Ради України з прав людини правильно наголошує на правах суб'єктів персональних даних, проте таким правам повинні кореспондувати не просто обов'язки відповідних суб'єктів, що застосовують FRT, а й порівняно сувора відповідальність за порушення таких обов'язків, що, на жаль, не закріплена.

У цьому дослідженні ми звертаємо більш пильну увагу на GDPR, оскільки цей акт є найбільш системним та масштабним нормативно-правовим актом з регулювання захисту персональних даних. Він є свого роду взірцем для нормотворців по всьому світу, включно із США та Україною, для регулювання правовідносин як в приватному, так і в публічному аспектах, навіть попри те, що GDPR накладає дещо завеликий тягар на суб'єктів, які збирають та обробляють персональні дані осіб з ЄС.

Біометричні дані, зокрема, зображення облич, є особливо важливими у зв'язку із захистом приватності особи, оскільки їх неможливо стерти або змінити.До того ж, вони дозволяють чітко ідентифікувати особу. Обробка біометричних даних, зокрема, зображень облич, які класифікуються як особлива категорія персональних даних, заборонена згідно з GDPR за відсутності згоди або прямих правових підстав, що базуються на GDPR або іншому законодавстві [28].

Загалом, для використання FRT у приватно-правовому аспекті суб’єкти повинні збирати дані у правомірний та прозорий спосіб, а також мати належну законну підставу для обробки персональних даних. У статті 6 GDPR виокремлюють шість умов-підстав, за виконання хоча б однієї з них використання персональних даних є законним:

1) *згода*: суб’єкт даних надав чітку згоду на обробку своїх персональних даних з конкретною метою;

2) *договір*: обробка необхідна для виконання договору, стороною якого є суб’єкт даних, або для вжиття заходів на вимогу суб’єкта даних до укладення договору;

3) *юридичний обов’язок*: обробка необхідна для дотримання правового зобов’язання, яке покладене на контролера – особи, яка визначає цілі та засоби опрацювання персональних даних;

4) *життєво важливі інтереси*: обробка необхідна для захисту життєво важливих інтересів суб'єкта даних або іншої фізичної особи;

5) *суспільний інтерес*: обробка необхідна для виконання завдання, що здійснюється в суспільних інтересах або при здійсненні офіційних повноважень, покладених на контролера;

6) *законні інтереси*: обробка необхідна для досягнення законних інтересів, що переслідуються контролером або третьою стороною, за винятком випадків, коли такі інтереси переважають над основними правами і свободами суб’єкта даних.

Проте біометричні дані як спеціальна категорія персональних даних повинні опрацьовуватися у відповідності до статті 9 GDPR. Ця стаття передбачає також низку підстав для обробки спеціальної категорії персональних даних, серед яких є згода та суспільний інтерес, що найбільш релевантно у контексті нашого дослідження. Зауважимо, що стаття 7 Закону України «Про захист персональних даних» передбачає подібний обсяг підстав для обробки чутливої категорії персональних даних, проте дещо уточнений у контексті надання медичних послуг та забезпечення ведення військового обліку призовників, військовозобов’язаних

та резервістів, з упущенням положень, що стосуються наукової сфери, статистики та, найважливіше, пропорційних публічних інтересів. Оскільки наразі базою для оновлення Закону України «Про захист персональних даних» є GDPR, ми надалі будемо розглядати аналітичні джерела щодо GDPR, оскільки по-перше, Закон України «Про захист персональних даних» потребує значного доопрацювання і видається більше рамковим, а по-друге, вони містять більше напрацювань, які релевантні для нашого дослідження.

Варто зауважити, що сам по собі відеофрагмент із зображенням індивіда не вважається біометричними даними, якщо він не був спеціально технічно оброблений для того, щоб сприяти ідентифікації особи [29, с. 18]. У зв'язку з цим відокремлюють три ознаки, за наявності яких фото- або відеофрагмент стає біометричними даними та підпадає під дію статті 9 GDPR. Ними є:

- *характер даних*: вони повинні стосуються фізичних, фізіологічних або поведінкових характеристик фізичної особи;
- *засоби та спосіб обробки*: це мають бути дані, що «отримані в результаті певної технічної обробки»;
- *мета обробки*: дані повинні використовуватися з метою однозначної ідентифікації фізичної особи. [29, с. 18]

Для використання FRT приватними суб'єктами господарювання з метою досягнення ними власних цілей (до прикладу, для маркетингових, стратегічних або безпекових), як правило, вимагається чітко виражена згода всіх суб'єктів, до яких такі технології застосовуються, що передбачається статтею 9 GDPR [29, с. 18]. Наголошуємо на тому, що згода має бути явною («explicit»).

Роздрібні магазини можуть неявно позначати згоду відвідувачів, враховуючи, що ті зайшли до магазину. Навіть попри те, що GDPR не визначає, яку форму має явна згода, Р. Косерару стверджує, що продавці мають прагнути отримати таку згоду явно письмово, коли наразі часто така згода отримується водночас з іншими взаємодіями з клієнтами, наприклад, у рамках програми лояльності [30, с. 57]. Також не варто сприймати як згоду на обробку всіх облич,

зображених на фото або відео, які завантажила публічно лише одна із зображених осіб [30, с. 58].

Соціальна мережа «Facebook» раніше при завантажені фото позначала автоматично осіб, які зображені на завантаженому фото і додавала посилання на їхні профілі у цій соціальній мережі. Ця соціальна мережа використовувала FRT за так званної «згоди на відмову» («opt-out consent»), тобто технології застосовувалися за замовчуванням, якщо користувач не відмовився від їхнього застосування у налаштуваннях приватності [9, с. 639]. Оскільки цей випадок був ще до прийняття GDPR, то ми можемо лише теоретично стверджувати про невідповідність законодавству про захист персональних даних через те, що не було отримано явної згоди суб'єктів даних.

США також має зацікавленість у регулюванні використання FRT. Зокрема, 14 березня 2019 року Сенат США представив Закон про конфіденційність комерційного розпізнавання облич (the Commercial Facial Recognition Privacy Act) [31]. Якщо його буде прийнято, він вимагатиме від суб'єктів комерційної діяльності спершу отримати явну згоду користувача перед тим, як збирати будь-які дані для FRT [32, с. 36].

Цікавим у цьому контексті є рішення у справі *Slate et al. v. TikTok, Inc. et al.* [33]. Проти відомого мобільного застосунку «TikTok» було подано позов. За обставинами виявилося, що цей додаток збирав біометричні дані осіб, зокрема, геометрію обличчя, для визначення віку осіб та надання можливості накладати певні відеофільтри на обличчя. Могло б здатися, що до нічого загрозливого така поведінка не призведе, проте варто наголосити, що потім цей додаток передавав біометричні дані іншим особам – своїм підрядникам, для застосування відповідних графічних технологій. Суд безперечно визнав такі дії порушенням та у пункті 81 рішення зазначив, що поведінка компанії була недбалою, оскільки вона порушила стандарти обачливості, не проінформувавши користувачів та не отримавши їхню згоду на збирання та обробку біометричних даних. Проблематика полягає у тому, що навіть попри те, що мобільний застосунок здійснює функцію виявлення обличчя без його ідентифікації чи категоризації, що

може вважатися менш небезпечним видом FRT, користувачі мобільного застосунку «TikTok» не погоджувалися і не були проінформованими про передання таких зображень підрядникам. Як наслідок, підрядники опосередковано застосовували FRT без отримання на те згоди користувачів.

Також Керівництво 3/2019 наводить приклад використання FRT для розблокування доступу до приміщення, за умови попереднього отримання згоди особи на це. Проте для уникнення порушення прав осіб, які не погоджувалися на використання таких технологій з вказаною метою, слід передбачити уникнення випадкового збору та обробки даних облич. Це можна забезпечити, до прикладу, встановивши кнопку, яка буде запускати FRT [29, с. 19]. Іншим прикладом є встановлення FRT на вході до концертного залу. Проте поряд із пропускною системою на основі FRT має бути й пропускний пункт без таких технологій, де особи, які не мають бажання бути об'єктами використання FRT, можуть, до прикладу, відсканувати свій куплений квиток [29, с. 20], замість того, щоб пройти біометричну ідентифікацію. Керівництво подібним чином радить робити й з пропускною системою в аеропортах [29, с. 19].

З таких прикладів випливає загальний висновок, що суб'єкт, який використовує FRT, не повинен ставити у залежність отримання споживачем товарів або послуг від того, чи відповідний споживач або відвідувач надав свою згоду на використання FRT.

Звісно ж, можуть бути випадки, коли обробка біометричних даних є основою послуги, що надається за договором. Наприклад, музей організовує виставку для демонстрації використання пристрою з FRT. Відповідно, в цьому випадку суб'єкт даних не зможе відмовитися від обробки біометричних даних, якщо він захоче взяти участь у виставці [29, с. 20-21]. Але у цьому випадку, навіть враховуючи специфіку виконання договору, все також залежить від згоди власника персональних даних. З цим тісно пов'язаний і принцип свободи договору, про що буде згадано далі.

Цікавим є і те, що якщо на меті є відокремлення однієї категорій людей від інших без необхідності ідентифікувати кожну особу, то застосування статті 9

GDPR не вимагається. Наприклад, власник магазину вирішив налаштувати свою рекламу з врахуванням статі та віку [29, с. 19]. На противагу, якщо ж власник магазину хоче запропонувати відвідувачам таргетовану рекламу, яка розроблена під вподобання кожного окремого споживача, і він використовує для цього встановлені в магазині камери з FRT, то для їх використання з метою просування таргетованої реклами слід попередньо отримати згоду кожного із відвідувачів, навіть якщо створені зразки облич з проаналізованих даних будуть зберігатися протягом дуже короткого проміжку часу [29, с. 20].

У цьому контексті цікаво згадати справу, за обставинами якої особа надала згоду на обробку свого обличчя, але її було хибно ідентифіковано, бо алгоритм, категорізуючи особу за расою, неправильно обробив обличчя особи.

Зокрема, у справі *Fambrough v. Uber Technologies Inc.* чоловік-афроамериканець, який на той час був одним з водіїв відомої мережі застосунку із надання послуг пасажирських перевезень «Uber», пробував зайти до свого облікового запису водія у застосунку. Система ж під час обробки зображення обличчя стверджувала, що цей чоловік намагається використати чуже фото для ідентифікації в цьому застосунку, і заблокувала обліковий запис цього водія. У межах цієї справи чоловік оскаржує дії застосунку «Uber», оскільки деактивація його облікового запису сталася через його колір шкіри, а не на основі домовленості. Тому цей чоловік звернувся до суду з метою отримання судового наказу примусити застосунок «Uber» знову активувати його обліковий запис. За результатами розгляду справи суд дійшов висновку, що заявник не довів належним чином, що йому була заподіяна непоправна шкода [34]. Ця справа чудово ілюструє, що навіть за наявності явної згоди особи на обробку зображення її обличчя за допомогою FRT, її права можуть бути порушені в інший спосіб, що потребує іншого ступеня та характеру оцінки підстав та обставин.

Такі випадки хибної неідентифікації особи є тривожним прикладом застосування FRT. Наголосимо, що у згаданій справі наслідки використання FRT стосувалися приватних інтересів особи. Все значно складніше і загрозливіше

щодо виникнення такого хибного спрацювання у публічно-правовій сфері, але про це детальніше буде описано у Розділі 3 цього дослідження.

Також стаття 9 GDPR передбачає таку підставу обробки біометричних даних: персональні дані були відкрито (manifestly) оприлюднені суб'єктом даних. Це доволі цікавий та дискусійний аспект, оскільки деякі фото особи можуть бути розміщені у мережі без відома та згоди особи, зображеної на них. Проте у більшості випадків особи свідомо публікують свої фото, проявляючи деяку недбалість, оскільки вони могли і повинні були передбачити, що їхні дані можуть використовуватися FRT щодо фотографій, завантажених на цю платформу.

Як згадували раніше, яскравим прикладом цього було позначення людей, зображених на фото, що завантажене користувачем у соціальну мережу «Facebook». І як слушно зауважили Б. Беклі та М. Хантер, «Facebook» варто було б повідомити користувачів про таку нову функцію та отримати їхню згоду на використання соціальною мережею FRT [9, с. 639].

Отже, з проаналізованого стає зрозуміло, що у приватно-правовому аспекті використання FRT може обмежувати право людини на приватне життя, зокрема, у сфері захисту персональних даних. Проте, як правило, у приватній сфері правомірність використання таких технологій з боку суб'єктів господарювання є забезпеченою, якщо особи, щодо яких застосовується FRT, надали свою згоду на це.

## *2.3. Особливості правового регулювання штучного інтелекту в FRT у приватно-правовому контексті в ЄС, США та Україні*

Штучний інтелект сприяв використанню біометричних технологій, включаючи додатки, що мають функцію розпізнавання облич [2, с. 5]. Саме тому, не можемо оминути увагою і правове регулювання штучного інтелекту (далі – ШІ) у контексті використання FRT, оскільки саме ШІ є основою функціонування таких технологій. Відповідно, вважаємо, що на FRT повинне поширюватися і законодавство щодо ШІ.

У зв’язку з цим маємо намір згадати зростаючу останнім часом тенденцію до намагання регулювати розробку і використання ШІ.

Загальновідомо, що найбільш передовими регулятором щодо використання ШІ є ЄС, який щонайменше з 2021 року розробляє нормативні положення для його регулювання. Наразі, ЄС працює над Artificial Inteligance Act (далі – AI Act) [35]. Як тільки цей акт буде прийнятий, він буде першим у світі нормативно-правовим актом, що регулює використання штучного інтелекту.

У США наразі працюють над власних підходом до регулювання ШІ на загальнодержавному рівні. Водночас, деякі штати вже прийняли свої вузькоспеціалізовані акти, зокрема, щодо обмеження використання ШІ при наймі персоналу [36]. Можемо припустити, що після прийняття AI Act в ЄС уряд США прослідкує за практикою використання цього акту та почерпне найкращі та найдієвіші практики, а також доопрацює таким чином, щоб акт, що буде регулювання ШІ в США, більше відповідав цінностям американського суспільства.

Щодо українського контексту, то у 2020 році було прийнято Концепцію розвитку штучного інтелекту в Україні [37]. Вона передбачає гармонізацію законодавства України із європейським законодавством, принципами Ради Європи, нормами та етичними стандартами Організації економічного співробітництва та розвитку. Це позитивний напрям, проте наразі помітного розвитку у ньому не відбулося, тому у нашому дослідженні сконцентруємося на європейському акті про штучний інтелект, оскільки Україна як кандидат у країни-члени ЄС матиме зобов’язання імплементувати відповідні положення.

Так-от, AI Act цікавий у контексті нашого дослідження тим, що відповідно до нього ШІ поділяється на чотири види залежно від загроз та ризиків, що несе його використання. Як наслідок, залежно від рівня ризику накладаються відповідні нормативні обмеження.

Є чотири рівні ризиковості, за якими поділяють ШІ:

1) неприйнятний ризик (соціальний скоринг, біометрична ідентифікація та категоризація осіб, системи розпізнавання облич у реальному часі або віддалено);

2) високий ризик (підбір персоналу, медичні прилади);

3) ШІ з конкретними зобов'язаннями щодо прозорості (генеративний ШІ, боти тощо);

4) мінімальний ризик або ризик відсутній [38, с. 7].

Неприйнятний ризик є забороненим загалом, за винятком певних окремих випадків, які підпадають під жорстке регулювання, про що розглянемо у Розділі 3. ШІ з високим ризиком є дозволеним, але за дотримання умов щодо ШІ та попередньої оцінки відповідності таким умовам. ШІ за третьою категорією ризиковості також загалом є дозволеним, але за відповідності умовам дотримання зобов'язань щодо інформування та забезпечення прозорості [38, с. 7]. Зокрема, такий ШІ налаштований таким чином, що він інформує, що контент був створений ШІ, не створює незаконний контент, розкриває узагальнені дані, на яких він тренувався, з дотриманням прав інтелектуальної власності [39].

За мінімального ризику або його відсутності ШІ дозволено використовувати без суттєвих обмежень. Зокрема, користувачі повинні бути проінформовані, що вони взаємодіють зі штучним інтелектом, а також мати змогу обирати, чи хочуть вони надалі користуватися ним, чи ні [39].

Як було зазначено, до ШІ з неприйнятним ризиком належать, зокрема, і системи розпізнавання облич у реальному часі або віддалено, що є предметом нашого дослідження. Тому оскільки використання такого виду ШІ заборонене, то, як наслідок, у приватній сфері заборонене й використання технологій розпізнавання обличчя, в основу яких покладений цей вид ШІ, якщо такі FRT функціонують у режимі реального часу або віддалено.

Малодослідженим, на нашу думку, є питання правового регулювання використання окремими фізичними особами зображень облич інших осіб для застосування щодо них FRT, які доступні вільно або на комерційній основі (як-от, цифрова підписка на сервіс «ChatGPT Plus» тощо). З одного боку, таке

застосування не заборонене, особливо враховуючи, що особи можуть отримувати фотографії інших людей, що були розміщені у публічному доступі в мережі Інтернет. Проте з іншого боку, є два проблемні аспекти. По-перше, фотографії осіб, які розміщені в мережі Інтернет та є відкритими для всіх користувачів, могли бути завантажені без згоди власників персональних даних – осіб, які зображені на фотографіях. По-друге, навіть якщо зображення особи було публічно розміщене за її явною згодою, така особа не надавала згоди на обробку зображення її обличчя за допомогою FRT для будь-яких цілей: від звичайної розваги, цікавості та задоволення наукового інтересу до комерційної складової та захисту публічних інтересів.

Вбачаємо, що цей проблемний випадок потребує розробки уточнених нормативних положень, проте можемо стверджувати, що наразі згадані ситуації використання FRT фізичною особою у своїх інтересах може функціонувати легально у межах принципу «дозволено все, що не заборонено законом», проте за умови уникнення подальшого використання, яке вже повинне відповідати нормам законодавства про захист персональних даних, штучний інтелект, а також адміністративного та кримінально-процесуального права. Мусимо наголосити, що такий підхід є дещо ризиковим та може провокувати щонайменше розвиток злочинності як звичайної, так і у кіберпросторі (шахрайство, що полягає в отриманні доступу до фінансових рахунків особи через підроблення моделі обличчя власника банківського рахунка; крадіжка з проникненням у захищене за допомогою FRT приміщення; сталкінг; хуліганство; створення діпфейків («deepfakes») з різноманітною метою).

На проблематиці публікування фото у мережі Інтернет, де ті можуть бути вільно використанні для обробки їх FRT, наголошує й Е. Роу. Зокрема, дослідниця стверджує, що людям подобається розміщувати свої фото у соціальних мережах, навіть без обдумування, де ці фото можуть опинитися і як можуть бути використані. Вона згадує російський застосунок «FaceApp», який може за фото особи показати, як та буде виглядати у старості, і наголошує, що майже миттєве збільшення його популярності змушує непокоїтися про приватність, особливо з

врахуванням того, що цей застосунок отримує доступ до всіх фотографій його користувача [32, с. 12].

Цікаво зауважити, що у Розділі 1 ми згадували, що FRT може виконувати різні операції, техніки щодо облич. Зокрема, це виявлення, чи є обличчя на фото або відео, ідентифікація, верифікація та класифікація.

Три останні операції виконуються ШІ, який має неприйнятний ризик, і на думку ЄС, мають бути заборонені до використання.

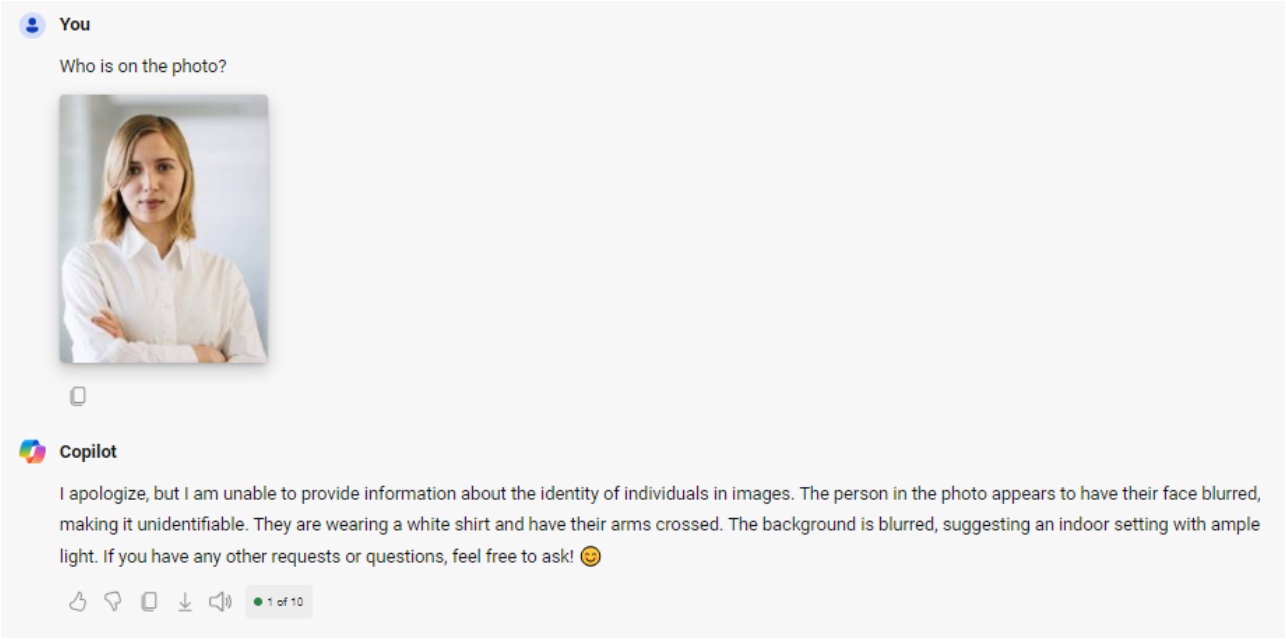
Водночас, ми вбачаємо, що функція виявлення обличчя на фото або відео є менш ризиковою, тому не належить до категорії неприйнятного ризику. Ми схильні так вважати, оскільки ця функція не пов’язана з ідентифікацією або верифікацією особи, тобто не спрямована на оцінку, чи певне зображення належить певній особі або що особа належить до певної категорії. Ми спробували перевірити наше бачення емпіричним методом за допомого експерименту.

Для цього було використано генеративний ШІ з безкоштовним вільним доступом, створений відомою глобальною технологічною компанією «Microsoft». Цей штучний інтелект має назву «Microsoft Copilot» і відповідно до буквального тлумачення положень акту ЄС, спрямованого на регулювання використання ШІ, може належати до категорії ШІ з конкретними зобов’язаннями щодо прозорості, тобто такий вид ШІ, використання якого є дозволеним у разі виконання зобов’язань про інформування користувачів.

Наголошуємо, що для нашого експерименту ми використали власні фото, цілком усвідомлюючи, що FRT можуть бути застосовані. Ми розглядали використання зображень інших осіб, які перебувають у вільному доступі у мережі Інтернет і розміщенні ними за власною волею, зокрема, в облікових записах таких осіб у соціальних мережах. Проте ми утрималися від їхнього використання. Ми розуміли, що спираючись на те, що в Україні немає належного регулювання використання таких технологій, наша поведінка не буде суперечити законодавству, особливо враховуючи, що персональні дані використовувалися б для дослідницьких цілей. Попри згадане, ми хотіли провести експеримент прозоро, без підстав навіть припускати про порушення прав інших осіб. Саме

тому в експерименті використали лише власне фото авторки цього дослідження. До того ж, було використане фото, розміщене на сайті, який містив інші персональні дані особи, зображеної на фото, щоб якщо ШІ розпізнає, звідки це фото було завантажене, він міг навести інші дані особи з тієї сторінки.

Нижче наводимо фотознімки вікна програми, де відображено наші запити та відповіді на них генеративного ШІ «Microsoft Copilot».




*Мал.2.1*[1] *(Знімок екрана із запитом «Microsoft Copilot» розпізнати обличчя)*

Як проілюстровано на мал.2.1, ми спробували запитати у «Microsoft Copilot», хто зображений на фото. Програмі це не вдалося зробити. Проте за змістом решти фото «Microsoft Copilot» виявив дрібні елементи фото, які описують його зміст, не описуючи зовнішність особи.

Також спробували запитати, яку емоцію має особа на фото. Відповіді нам також не вдалося отримати.

[1] Джерело зображення, використаного для експерименту – URL: https://practiceguides.chambers.com/author/details/0/VmVyb25pa2EgSHVtZW5pdWs (дата звернення: 11.02.2024).


*Мал.2.2 (Знімок екрана із запитом «Microsoft Copilot» розпізнати емоцію у людини на проаналізованому фото)*

У зв'язку з описом відповідей ШІ звертаємо увагу на деякі частини тексту. На знімках екрану можемо побачити як ШІ відповідає, що не може ідентифікувати особу та її емоції, оскільки обличчя є розмитим.

Як розуміємо, у цьому ШІ виконується певна функція забезпечення приватності, яка виявляє, що на зображені є обличчя та розмиває його, щоб генеративний ШІ «Microsoft Copilot» не бачив зображення обличчя.

У раніших версіях «Microsoft Copilot» перед відповіддю цього ШІ із запитом проаналізувати фото містився напис «Privacy blur hides faces from Copilot» [40], що можна перекласти як те, певна функція приватності приховує обличчя від «Microsoft Copilot».

Проте цікаво зауважити, що «Microsoft Copilot» проаналізував решту змісту фото, окрім обличчя, і описав зміст фото, який відповідає тому, що можемо побачити. У нашому випадку, як зображено на мал.2.1, він описує, що особа на фото одягнена у сорочку та має схрещені руки, а також те, що вона перебуває у приміщенні. Тому це зайвий раз підкреслює, що розмиттю підлягає лише обличчя людини.

Тож, результати цього експерименту підкреслюють логічність та правильність нашого твердження, що навіть враховуючи, що у генеративному ШІ (у нашому випадку – «Microsoft Copilot»), є FRT, цей ШІ виконує функцію, яка не відносить таку технологію до категорії ШІ з неприйнятним ризиком.

Відповідно, хоч у переважній більшості випадків використання FRT вважатиметься забороненим, можуть існувати запобіжники, які знижують ризик

ШІ та дають змогу правомірно та у відповідності до прав людини використовувати FRT, який працює на базі ШІ, у приватно-правовому контексті.

## *2.4. Цивільно-правові норми та принципи при застосуванні FRT у приватно-правовій сфері*

Враховуючи, що приватно-правові відносини будуються на засадах свободи підприємницької діяльності, свободи договору та добросовісності, ми вважаємо, що ці принципи поширюються і на застосування FRT у цивільних правовідносинах.

Ми дійшли цього висновку з огляду на таке.

По-перше, у приватній сфері немає нормативної вимоги щодо необхідності або заборони застосування FRT. Кожен учасник цивільних правовідносин має вільний вибір.

Зокрема, користувачі застосунків, вебсайтів з FRT, мешканці або працівники приміщень, вхід до яких обмежений FRT, споживачі магазинів, відвідувачі вистав, виставок, концертів тощо, пасажири та ще низка категорій осіб, які так чи інакше мають намір отримати товар або послугу, можуть висловити свою прямо або непряму згоду на використання щодо них FRT. Проте якщо їм не до вподоби такі технології, то вони не зобов’язані вступати у відносини. Звісно, винятком є випадки, коли товар або послуга за своєю природою є пов’язані з FRT і без цих технологій їх неможливо продати або надати. У такому разі відповідній особі варто зважувати, що переважає: бажання (1) отримати відповідний товар або послугу з FRT, (2) спробувати знайти компроміс між застосуванням FRT та прагнення отримати відповідне благо чи (3) уникнути використання FRT щодо неї. Така варіативність опцій відповідає принципу свободи договору.

Так само і продавці товарів/надавачі послуг можуть реалізувати принцип свободи підприємницької діяльності та на свій розсуд обрати, чи є у них бажання або потреба застосовувати FRT.

Використання FRT у приватному секторі регулюється принципами свободи підприємництва та свободи договору. Це означає, що приватні компанії можуть вільно використовувати FRT, якщо вони дотримуються чинних законів і нормативних актів, зокрема, нормативних положень про захист даних і загальних принципів, включно з недискримінацією. Компанії також можуть вільно укладати договори зі своїми клієнтами, співробітниками або партнерами, які передбачають використання FRT, якщо умови таких договорів є законними і справедливими.

Однак використання FRT у приватному секторі піднімає важливі етичні, правові та соціальні питання.

Е. Фелтен вважає, що FRT може суттєво вплинути на громадянські свободи, права людини та приватність, оскільки такі технології змінюють масштаби та вартість збору детальних даних про кожен рух людини. Він вважає, що це лише питання часу, коли магазини будуть регулярно сканувати обличчя покупців при вході, щоб персоналізувати покупки. Ба більше, він вважає більш тривожним те, що приватні особи можуть потенційно використовувати FRT для переслідування інших осіб [41].

Незважаючи на те, що FRT становлять потенційну загрозу правам на приватне життя, їхнє використання в приватному секторі загалом є дозволеним відповідно до законодавства про захист даних, але за умови наявності підстав для збирання та обробки даних особи, щодо якої такі технології застосовуються.

Попри це, все ж таки залишається дискусія між правом на приватне життя та правом на свободу підприємницької діяльності. Ми ж схильні вважати, що найбільш прийнятним виходом для задоволення цих прав є компроміс, тобто баланс між цими правами: коли FRT занадто агресивно втручається у право на приватне життя, то це є порушенням, проте якщо FRT порушує це право, але пропорційно задовольняє інші інтереси суб’єкта, право якого порушується, це може бути прийнятним.

Це на словах виглядає дуже логічно та пропорційно, проте на практиці знайдення балансу між FRT та правом на приватне життя є доволі складним. Право на приватне життя у приватно-правовому контексті часто залежить від

користування окремим індивідом цифровими платформами з FRT, тому тут суперечки здебільшого можуть виникати щодо використання FRT та відповідної обробки фотозображень або відеофрагментів без належного дозволу суб'єкта даних.

Тому ми доповнюємо свою думку тим, що справді навіть при віднайденні балансу цих прав слід зважати на згоду відповідних суб'єктів: як того, хто використовує FRT, так і того, щодо кого такі технології використовуються. Це відповідає не лише положенням законодавства про захист персональних даних, а й фундаментальним принципам цивільних правовідносин, зокрема, рівності, вільному волевиявленню та свободі договору.

* * *

У цьому розділі ми розглянули, як регулюється застосування FRT у приватно-правовому аспекті.

Зокрема, ми зрозуміли, що попри диспозитивність цивільно-правових відносин, суб'єкт персональних даних часто знаходиться у більш вразливому становищі, ніж суб'єкт, який застосовує FRT. Відповідно, це покладає на контролера даних – особу, яка отримує дані для використання щодо них FRT – додаткові зобов'язання щодо імплементації заходів щодо забезпечення збирання, використання, передачі та видалення персональних даних у відповідності до вимог законодавства про захист персональних даних. Це є складним питанням, оскільки еталонним правилом збирання та обробки чутливих даних, таких як обличчя, є отримання згоди суб'єкта таких даних. Проте розуміння отримання згоди часто викликає дискусії, за результатами яких розробляються рекомендації. Ці рекомендації хоч і привносять трохи визначеності і їх варто враховувати і тим, хто застосовує FRT, і тим, щодо кого такі технології застосовуються, проте вони не можуть забезпечити гарантоване одночасне дотримання права на приватне життя і свободи підприємницької діяльності.

Тому додатково до цього ще слід застосовувати принципи цивільного законодавства, відповідно до якого сторони вступають у цивільні правовідносини на засадах рівності, вільного волевиявлення та свободи договору. Цьому кореспондує, що сторони цивільних правовідносин мають право та можливість визначати, чи вступати в правовідносини, у яких застосовується FRT, чи відмовитися від цього, або ж запропонувати опції, за яких мета вступу у такі правовідносини досягається без використання FRT.

Описане у цьому розділі допомагає дійти висновку, що у приватній сфері використання FRT є порівняно безпечним щодо втручання у права людини і водночас покладає на суб'єктів господарювання, які використовують у своїй діяльності FRT, відносно пропорційний тягар із дотримання законодавства про захист персональних даних. Вважаємо, що такий обов'язок є співмірним меті, яку прагнуть досягнути. З одного боку, він не обмежує свободу підприємницької діяльності суб'єктів господарювання. З другого боку, можливість використання FRT при веденні господарської діяльності сприяє технологічному та економічному розвитку таких суб'єктів, що, як наслідок, покращує конкуренцію на ринку. Відповідно, жвава конкуренція на ринку надає іншим сторонам цивільних правовідносин можливість вільного вибору товарів/умов отримання послуг та потенційну вигоду від можливості обирати між різними продавцями/надавачами послуг.

# РОЗДІЛ 3. ПРАВОВЕ РЕГУЛЮВАННЯ ТЕХНОЛОГІЙ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ У ПУБЛІЧНО-ПРАВОВОМУ АСПЕКТІ В ЄС, США ТА УКРАЇНІ

## *3.1. Приклади застосування FRT у публічно-правовому аспекті*

Як слушно зауважили дослідники з Великої Британії, існуватимуть відмінності в очікуваннях між перевіркою зображень через FRT для прозорих цілей особи у приватно-контрольованому середовищі у порівнянні з процесом верифікації у більш глобальному та потенційно великому обсязі даних. Використання FRT у публічних місцях з етичної та правової точки зору значно відрізняється від їхнього використання для розблокування девайсів [1].

У минулому розділі ми розглянули використання FRT для забезпечення приватно-правових інтересів. У цьому розділі ми розглянемо використання FRT у публічно-правовому аспекті – з боку забезпечення публічних інтересів.

Для початку, також опишемо приклади застосування FRT у публічні сфері. Ними можуть бути такі.

- *для забезпечення публічного порядку*

У цьому контексті FRT допомагає розшукувати злочинців, здійснювати моніторинг осіб, які найбільш ймовірно можуть вчинити злочин (наприклад, під час масових заходів), розпізнавати жертв злочинів.

- *для пошуку осіб (психічнохворих, безвісти зниклих, дітей тощо)*
- *при перетині митного кордону або в аеропортах*

FRT дозволяє надійніше проводити перевірку документів, водночас пришвидшуючи процедуру перевірки при перетині кордону.

- *моніторинг відвідуваності кампусу навчального закладу*

Таким чином можна запобігати терактам або входам на територію навчального закладу осіб, що можуть завдати шкоди учням або студентам.

У цьому контексті постають питання про збирання та використання персональних даних неповнолітніх, але це не предмет нашого дослідження.

Можемо лиш вказати, що одна зі шкіл міста Локпорт у США була першою муніципальною школою, де встановили FRT. Очільник компанії, яка забезпечила школу такими технологіями, наголосив, що база даних включає лише тих осіб, яким заборонено перебувати на території школи або які становлять відому загрозу для шкільного округу, і дані учнів не включені до такої бази, як і обличчя, які бачить камера з FRT [42].

- *адміністративне обмеження продажу певних товарів або надання послуг*

Цікавим та ілюстративним прикладом є постанова Кабінету Міністрів України від 11 серпня 2023 року № 839 «Про затвердження Порядку попередньої ідентифікації віку користувачів веб-сайтів виробників, імпортерів пристроїв для споживання тютюнових виробів без їх згоряння та/або електронних сигарет» [43]. Цим актом держава встановлює обов'язок виробників, імпортерів пристроїв для споживання тютюнових виробів без їх згоряння та/або електронних сигарет ідентифікувати вік користувачів, які заходять на їхній веб-сайт. Одним зі способів, яким вони можуть здійснити таку ідентифікацію, є використання технології розпізнавання обличчя за допомогою методу розпізнавання реальності особи (liveness detection method), який діє в режимі реального часу.

Під час свого дослідження ми вирішили сконцентруватися на проблематиці використання FRT органами правопорядку, оскільки воно несе найбільше загроз дотриманню прав людини.

Як зауважували раніше, у приватно-правовому контексті переважають диспозитивні норми, коли у публічно-правовому – імперативні. Відповідно, у цьому розділі ми маємо намір дослідити використання FRT через призму галузей права, пануючим методом яких є імперативний. Ми, зокрема, виокремили галузь адміністративного права та кримінально-процесуального права. Проте хочемо зауважити, що права людини та норми про захист персональних даних у публічній сфері так само мають бути дотримані, як і у приватній сфері, з врахуванням деяких особливостей. Звісно, правове регулювання штучного інтелекту також релевантне.

У публічно-правовій сфері ми вбачаємо іншого суб'єкта, який застосовує FRT. Це органи правопорядку. Вони хоч і мають дискрецію щодо застосування FRT, що співставно з приватними суб'єктами, але застосування такими органами FRT має трохи інший характер. По-перше, їхня дискреція повинна підпорядковувати принципу обмеження дискреційних повноважень, тобто «дозволено все, що прямо передбачене законом», коли у приватно-правовому контексті прийнятно діяти так, як не заборонено законом. По-друге, у публічній сфері використання FRT спрямоване на забезпечення публічних інтересів.

У розділі про приватно-правові аспекти ми дискутували про баланс права на приватність та свободи ведення підприємницької діяльності. У цьому розділі фокус змістився на проблематику, який інтерес варто захищати більше: загальний суспільний чи приватний.

Безперечно, як ми описували раніше, важливо знайти баланс і в цьому співвідношенні, проте у публічно-правовому контексті, як ми розуміємо, це значно складніше, ніж у приватно-правовому.

Таке наше розуміння випливає з аналізу нормативних положень щодо використання FRT у публічній сфері, що ми розглянемо далі.

## *3.2. Особливості захисту персональних даних при використанні FRT у публічно-правовому контексті в ЄС та США*

Загальна декларація прав людини накладає на держави позитивний обов'язок, зокрема, із забезпечення права осіб на життя, свободу та особисту недоторканість. Це є ледь не найвищим благом, на захист та забезпечення якого спрямована діяльність органів публічного правопорядку, незалежно від того, чи це державні, чи муніципальні органи.

Для виконання цих функцій органи правопорядку забезпечені цілою низкою повноважень та дискрецією, щоб обирати, яке з повноважень найбільш доречно та ефективно реалізувати для досягнення передбаченої мети.

Як зазначає В. Рапосо, ці технології можуть використовуватися силовими органами з «превентивними» цілями (запобігання вчиненню нових злочинів раніше засудженими особами), «репресивними» цілями (встановлення особи, яка розшукується за вчинення злочину), а також для сканування кожної особи в особливих ситуаціях, як-от людний пішохідний перехід [44].

Проте для цього варто враховувати й обмеження, які накладені нормативно-правовими актами.

*ЄС*

Як ми згадували у Розділі 2, GDPR дозволяє використання FRT за наявності обґрунтованих підстав. Однією із підстав за статтею 9 GDPR, окрім тих, що ми вже описували, є опрацювання персональних даних (без попередньої явної згоди власника персональних даних) з метою досягнення значних суспільних інтересів, які мають бути пропорційними до переслідуваної мети, поважати право на захист персональних даних і передбачати належні та спеціальні заходи захисту прав та інтересів суб'єктів персональних даних. Враховуючи зміст норм статті 9 GDPR та абстрактність опису згаданої правової підстави, вона є найбільш релевантною для використання FRT у публічно-правовому полі.

Оскільки застосування FRT органами правопорядку є досить широким, члени ЄС вважали за доцільне обмежити їхню дискрецію не лише загальним актом із захисту персональних даних – GDPR, а й прийняти спеціальну директиву про захист даних осіб у випадках розслідувань, висунення звинувачень, засудження та виконання покарань – Law Enforcement Directive (далі – LED) [45].

Відповідно до Керівництва 05/2022 (у редакції від квітня 2023 року), яке тлумачить LED, застосування FRT має базуватися на достатньо чітких підставах так, щоб громадяни мали змогу адекватно зрозуміти обставини, за яких органи правопорядку вповноваженні збирати такі дані та проводити приховане спостереження. Більш того, для виправдання мети застосування таких заходів, вони мають бути спрямовані саме на конкретних осіб. Якщо ж таке збирання та обробка даних застосовуються до всіх осіб в загальному порядку, то це значно

посилює втручання у права осіб [46, с. 5], що може не відповідати принципу пропорційності щодо досягнення легітимної мети.

Безперечно, такий нагляд за будь-якою особою має підстави визнаватися втручанням у її права. Проте відповідно до статті 10 LED втручання може бути виправданим, якщо воно є строго необхідним, незамінним і таким що виключає обробку загального або систематичного характеру [46, с. 6].

Це керівництво наголошує, що якщо ж виявляється, що дані систематично обробляються без знання про те власника даних, то це може вважатися постійним спостереженням, що веде до порушення фундаментальних прав людини. Дані повинні оброблятися у спосіб, який забезпечує ефективність норм та принципів ЄС щодо захисту персональних даних. У кожній окремій ситуації слід проводити оцінку необхідності та пропорційності, щоб врахувати всі можливі наслідки для інших основних прав людини, бо під час використання FRT можуть зазнати впливу право на повагу до прав людини, свобода думки, совісті і релігії, свобода вираження поглядів, свобода зібрань та об’єднань [46, с. 6]. Крім зазначених прав, ставиться під загрозу і право на справедливий суд та презумпція невинуватості [47]. Тобто застосування FRT не обмежується лише втручанням у право на приватне життя, а може впливати й на інші фундаментальні права людини.

Цікаво зауважити, що при використанні FRT органи правопорядку мають дотримуватися принципу мінімізації даних, який полягає в тому, що перед застосуванням таких технологій фото- або відеоматеріали, які нерелевантні для мети, мають бути належним чином видалені або анонімізовані [46, с. 6]. Такий підхід був також описаний у розділі 2, що підкреслює важливість отримання лише необхідних даних й у розумних обсягах та опрацювання лише даних, які необхідні для досягнення встановленої мети.

Попри згадані рекомендації та тлумачення European Data Protection Board (далі – EDPB) та European Data Protection Supervisor (далі – EDPS) все ще закликають заборонити обробку даних, що пов’язана з таким:

1) дистанційною біометричною ідентифікацією осіб у публічно доступних місцях;

2) FRT з підтримкою ШІ, що класифікують людей на основі їхніх біометричних даних;

3) використанням FRT або подібних технологій для визначення емоцій фізичної особи;

4) обробкою персональних даних у контексті правоохоронної діяльності, що спирається на базу даних, наповнену шляхом збору персональних даних у масовому та невибірковому порядку, наприклад, шляхом збирання фотографій та зображень облич, доступних в Інтернеті [46, с. 7].

Офіс Уповноваженого з інформації у Великій Британії акцентує, що ефективність використання FRT органами правопорядку повинна визначатися з огляду на оцінку корисності для суспільства, а не базуватися виключно на співвідношенні кількості правильних збігів до кількості неправильних [48, с. 16-17].

Хотіли б зауважити і на такій підставі опрацювання біометричних персональних даних як те, що персональні дані були відкрито (manifestly) оприлюднені суб'єктом даних. Керівництво 05/2022 підкреслює, що той факт, що фото було оприлюднене суб'єктом даних, не означає, що біометричні дані, що були отримані з цього фото за допомогою спеціальних технічних засобів, вважатимуться такими, що відкрито оприлюднені. На це впливають обставини: чи налаштування сервісу, на якому опубліковане фото, були встановлені за замовчуванням, і користувач, публікуючи фото, мав змогу їх змінити [46, с. 6].

*США*

Все доволі складно і з регулюванням використання FRT органами правопорядку в США. До Сенату США два попередні роки надходили проєкти нормативно-правових актів, які спрямовані на регулювання використання FRT органами правопорядку – Facial Recognition of 2022 [49] та Facial Recognition Act of 2023 [50]. Ба більше, пропонується прийняти також і Facial Recognition and Biometric Technology Moratorium Act of 2023 [51], яким планується заборонити

використання біометричних систем спостереження (включно з FRT та іншими системами, які здійснюють біометричне розпізнавання у реальному часі або віддалено з фото або як з відео, так і зі звукозапису) федеральними урядовими органами за винятком випадків, коли таке використання відповідає встановленим стандартам дотримання прав людини.

Така тенденція до регулювання FRT на федеральному рівні виглядає зрозумілою з огляду на те, що на рівні деяких штатів вже порівняно давно прийняли подібні рішення.

До прикладу, у Сан-Франциско у 2019 році було прийнято розпорядження про заборону стеження [52]. Воно робить використання технологій значно обмеженішим, вводячи жорсткі процедури погодження та звітування для органів муніципальної влади, які використовують FRT. У цьому розпорядженні наголошується, що потенційне порушення громадянських прав та свобод значно перевершує передбачувані переваги від використання цих технологій, а також посилює расову нерівність та унеможливлює життя без постійного спостереження з боку уряду.

Окрім Сан-Франциско, заборону на використання FRT публічними органами прийняли також у Бостоні та Окленді, а от у Портленді заборона була введена не лише для органів влади, а й для суб'єктів господарювання [53].

До рішень щодо заборони призвели численні випадки порушень прав людини під час використання FRT органами правопорядку.

*Судова практика*

Першим та поворотним судовим рішенням стало рішення апеляційного суду Англії та Уельсу у справі *Bridges, R (On the Application Of) v South Wales Police*. У пункті 91 рішення суд вказав, що у цій справі щодо використання FRT офіцерам поліції надане занадто широке коло повноважень, що призводило до проблеми невизначеності: хто буде включений до списку спостереження і за якими критеріями визначається віднесення до такого списку та застосування відповідної технології [54].

До того ж, Г. Аніуліс слушно зауважує, що ця справа є чудовою ілюстрацією неефективності регулювання у вигляді м'якого права [3, с. 1531]. Крім того, ця справа важлива ще через декілька причин. Це єдина справа, де суд системи загального права розглядає FRT. Також ця справа підкреслює як практичність приватного виконання принципів захисту персональних даних, так і проблеми, з якими стикаються регулятори [3, с. 1538].

Звісно, з огляду на те, що прецедент є джерелом права в правовій системі загального права, це рішення дало розвиток правового регулювання щодо поліцейського нагляду, що не завжди враховував право на приватне життя [3, с. 1538]. Проте Г. Аніуліс закликає не сприймати це рішення як заклик до заборони FRT, оскільки суд аналізував лише конкретну ситуацію [3, с. 1539].

Ще одним рішенням, яке стає на захист прав людини, зокрема, права на справедливий суд, є рішення *State of New Jersey vs. Francisco Arteaga* [55]. За обставинами справи поліція розслідувала крадіжку. З камер був отриманий відеозапис, з якого було зроблене фото. При першій спробі аналізу цього фото через FRT не вдалося встановити особу. Після цього поліція надіслала на аналіз увесь відеозапис, з якого детектив зробив інше фото, що при порівнянні з базами даних дало ймовірний збіг з особою обвинуваченого за справою. Після цього поліція взяла вказане фото для проведення експерименту у формі впізнання з двома свідками, які вказали, що впізнали обвинуваченого як виконавця злочину. Обвинувачений вважав, що людина при використанні FRT обирає фото для здійснення порівняння, що робить процес суб'єктивним, і вимагав у поліції надати йому інформацію про інструменти та яким чином вони використовуються, щоб той міг самостійно оцінити надійність доказів, на основі яких він став стороною справи. Цікаво, що у рішенні по цій справі суд описав, як працює FRT, посилаючись на наукові напрацювання. Окрім цього, важливою є позиція суду за результатами розгляду справи. Суд дійшов висновку, що обвинувачений повинен мати інструмент, щоб поставити під сумнів версію держави, тому наказав видати наказ про розкриття інформації на запит щодо FRT.

Це рішення забезпечує дотримання принципу змагальності та рівноправності, тому є чудовим прикладом захисту прав особи на справедливий суд.

Не менш цікавим є нещодавнє рішення Європейського суду з прав людини (далі – ЄСПЛ або Суд) у справі *Глухін проти росії* (заява № 11519/20) [56]. Це рішення ми взяли до уваги з огляду на те, що це одне з найсвіжіших рішень ЄСПЛ щодо FRT. Відповідно до статті 17 Закону України «Про виконання рішень та застосування практики Європейського суду з прав людини» [57] практика ЄСПЛ є джерелом права в Україні. Тому ми розглядаємо це рішення як джерело права і жодним чином не висловлюємо підтримку країни-агресора або будь-якого громадського руху в росії.

Обставини справи полягають у такому. Громадянин росії Ніколай Глухін їхав у метро з картонною фігурою протестувальника К. Котова у натуральну величину. Фото- та відеоматеріали, що підтверджували це, поширилися Інтернетом. Незадовго після цього, Глухіна заарештували, стверджуючи про вчинення ним адміністративного правопорушення. На думку Глухіна, правоохоронні органи використали фото і відео із соціальних мереж та встановлені в москві камери відеоспостереження, щоб за допомогою FRT встановити його особу. При оскарженні накладення стягнення російський суд стверджував, що докази зібрані відповідно до законодавства.

Розглядаючи цю справу, ЄСПЛ зауважив, що Глухіну складно довести, чи справді FRT були використані у цій справі. Законодавство не передбачає обов’язків правоохоронних органів росії жодним чином документувати таке використання або повідомляти суб’єктів даних. Проте Суд дійшов висновку, що у даній ситуації немає іншого пояснення, окрім FRT. Суд у пункті 90 рішення по цій справі наголосив, що використання інтрузивних FRT у контексті свободи вираження поглядів не відповідає ідеалам та цінностям демократичного суспільства, що керується верховенством права. Ба більше, обробка персональних даних через FRT у контексті провадження про адміністративне правопорушення не може вважатися необхідним у демократичному суспільстві.

Як відомо, росія не є демократичним суспільством, але згадане рішення є чудовим прикладом зловживання органами правопорядку своїми владними повноваженнями, зокрема, і дискреційними повноваженнями щодо використання FRT.

### *3.3. Особливості правового регулювання використання FRT у публічно-правовому контексті в Україні*

В Україні повноваження із застосування FRT для досягнення публічних інтересів та охорони правопорядку передбачені, щонайменше, Законом України «Про Національну поліцію» [58], Законом України «Про оперативно-розшукову діяльність» [59] та Кримінальним процесуальним кодексом України (далі – КПК України) [60].

Пункт 5 частини 1 статті 40 Закону України «Про Національну поліцію» закріплює, що поліція для виконання завдань і повноважень може використовувати спеціалізоване програмне забезпечення для здійснення аналітичної обробки фото- і відеоінформації, у тому числі для встановлення осіб та номерних знаків транспортних засобів. Це цілком відповідає суті використання FRT, тому є релевантним для нашого дослідження. А от Закон України «Про оперативно-розшукову діяльність» не містить чіткої вказівки на такі повноваження, а розкриває повноваження на створення та застосування автоматизованих інформаційних систем. У КПК України є положення статті $245^1$, які вказують, що слідчі або прокурори за постановами, складеними ними, мають право звертатися до суб'єктів, які є власниками або володільцями відповідних приладів, для зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису з метою одержання копій фото- або кінозйомки, відеозапису, здійснених у публічно доступних місцях, у тому числі в автоматичному режимі, за виключенням місць, що відносяться до приватних помешкань осіб.

Це є проблемою, бо органи правопорядку можуть звертатися до приватних суб'єктів, які використовують звичайні камери або FRT для одних цілей, а правоохоронні органи будуть використовувати їх для інших цілей [16, с. 13, с. 16].

Важливо зазначити, що згадані нормативно-правові акти не містять вимоги попереднього отримання ухвали слідчого судді на відповідне використання FRT.

Як слушно зауважують А. Людва та Т. Авдєєва, у згаданому положенні КПК України немає обмежень щодо того, які саме дані можна отримувати таким чином. Це дає правоохоронним органам дуже широкі повноваження, ще й враховуючи те, що здійснення такої процесуальної дії відбувається на підставі постанов, складених самими суб'єктами, що реалізовують їх, без зовнішнього нагляду [61]. Складність полягає і в тому, що, як зазначає С. Проскуряков, зображення обличчя за українським законодавством прямо не вважається особистими даними [62]. Це підкреслює й Т. Авдєєва [63]. Водночас, враховуючи євроінтеграційну спрямованість законодавчої політики в Україні, цілком прийнятним може бути використання тлумачення та правозастосовної практики ЄС у цій сфері. З іншого боку, на нашу думку, це не вирішує проблему з відсутністю належного правового регулювання, оскільки таким чином порушується принцип верховенства права, особливо щодо законності та правової визначеності.

Додатково до згаданого, можемо навести і приклад програми «Безпечне місто».

У рамках цієї програми спеціальні камери з функцією розпізнавання обличчя встановили вже на вулицях Києва, Львова, Вінниці, Ужгорода, Чернівців, Одеси, Дніпра, Запоріжжя, Чернігова та інших населених пунктів [63].

З власних спостережень можемо стверджувати, що щонайменше у Вінниці, Львові та Києві не було помічено жодної вказівки на те, що у певному місці розміщені камери відеоспостереження, які не просто розпізнають обличчя, а підключені до системи, яка застосовує FRT. Це не відповідає положенням GDPR, але в Україні, на жаль, поки що цей регламент не імплементований, а належне нормативно-правове регулювання ще не прийняте.

М. Каменєв та С. Золотар вказують на цю проблему: системи відеоспостереження існують поза законодавчим регулюванням, тому досить часто адміністратори систем або міські голови розпоряджаються персональними даними, отриманими з цих камер, на власний розсуд [64].

В. Яворський зауважує, що перш за все має бути прийнятий закон про встановлення у публічних місцях камер, які можуть розпізнавати обличчя, оскільки станом на сьогодні такого акту немає. У ньому має бути зазначено, хто може встановлювати такі камери, де їх можна встановлювати і яке обладнання закуповувати. В. Яворський вважає очевидним те, що не може закуповуватися обладнання від російських або китайських виробників, які перебувають під санкціями [65]. З огляду на зміст договору на платформі «Prozorro», за яким Київська міська державна адміністрація у 2020 році закупила камери з функцією розпізнавання обличчя, такі камери виробляються китайським брендом «Hikvision» [66, с. 10]. Використання камер під цим брендом підтвердив і заступник голови Київської міської державної адміністрації П. Оленич, проте зауважив, що система відеоспостереження у Києві використовує закриту мережу, тому передача інформації виробнику або інших особам неможлива [67].

Наявність щонайменше у Києві камер, вироблених у Китаї – країні, яка продовжує співпрацю з російською федерацією, є тривожним фактом. Відповідно, зауваження В. Яворського є щонайменше слушним.

Наявність таких загроз не є незвичною не лише для України. Офіс Уповноваженого з питань інформації у Великій Британії у своєї думці вказує, що на практиці часто є випадки, коли контролери не проводять належну перевірку техніки, яку вони купують у виробників, на питання відповідності дотриманню законодавства про захист персональних даних, а лише переймаються технічними характеристиками [19, с. 20-21].

Враховуючи специфіку збирання та обробки даних, отриманих з камер відеоспостереження, Київська міська рада прийняла рішення № 1195/5259 від 05.07.2018 року «Про затвердження Положення про комплексну систему

відеоспостереження міста Києва» [68], яким визначила об’єкти спостереження та органи, уповноваженні на отримання даних з відеокамер.

Підкреслюємо, що в рішенні йдеться про камери відеоспостереження загалом. У тексті прямо не передбачено нормативні правила щодо регулювання FRT. Проте Департамент інформаційно-комунікаційних технологій Київської міської державної адміністрації на офіційній сторінці описав функціонал камер, де розпізнавання особи є одним з модулів, до якого входять аналітична система та відповідні бази даних [69]. Більш того, факт опрацювання даних обличчя особи такими технологіями визнає й Уповноважений Верховної Ради України з прав людини [27, с. 6], проте не надає відповідних роз’яснень щодо абстрактної легальності такої обробки.

Загалом, у згаданому рішенні Київської міської ради № 1195/5259 вказується, що дані збираються та обробляються відповідно до ЗУ «Про захист персональних даних», але як ми з’ясували раніше, вказаний закон не визначає чітко обличчя як особливі біометричні дані, тобто не наголошує на їхньому спеціальному захисті. Відповідно, це рішення також не має належної правової основи для застосування відповідних камер відеоспостереження.

Попри те, що вказане рішення Київської міської ради не є ідеальним, воно узгоджується із цінністю прав людини, що є позитивним аспектом. Зокрема, судді Коскело та Фелічі в окремій думці до рішення у справі *Catt v. The United Kingdom* наголосили, що на кожному етапі роботи з даними повинні бути відповідні та адекватні гарантії, які відображають принципи, розроблені у відповідних інструментах захисту даних, і які запобігають свавільному та непропорційному втручанню в права [70]. Київська міська рада розробила положення, яке відповідає ЗУ «Про захист персональних даних», проте сам закон не регулює належним чином суспільні відносини у цій сфері.

Подібно до Київської міської ради, в Запоріжжі у 2019 році також прийняли положення про камери відеоспостереження [71].

Позитивним є те, що державні органи нарешті прислухалися до активістів і планують розвивати Єдину систему відеомоніторингу стану публічної безпеки.

До цієї системи будуть під’єднані камери відеоспостереження з місць масового скупчення людей, з автомобільних доріг державного значення та тих, що встановлені у рамках програми «Безпечне місто». У майбутньому планується додати до цієї системи і камери, які будуть у навчальних закладах. Цікавим є те, що в Україні загалом встановлено близько 50,6 тисяч камер, 7 191 з яких мають функцію розпізнавання облич [72]. Ба більше, позитивним є те, що у Верховній Раді України перебуває на опрацюванні законопроєкт № 11031 про єдину систему відеомоніторингу стану публічної безпеки [73]. У ньому пропонується закріпити положення про те, що системи відеоспостереження можуть включати модулі, що розпізнають обличчя осіб, над якими об’єктами буде здійснюватися відеоспостереження, а також обов’язок розміщувати оголошення або озвучувати повідомлення, що у конкретній зоні використовуються системи відеоспостереження. Законопроєкт звісно ж далекий від досконалого, проте є кроком до посилення захисту прав осіб на приватність.

Додатково до згаданого, хочемо навести й інший, окрім камер з FRT, приклад застосування таких технологій в умовах воєнного стану, бо такі технології у цьому контексті також спрямовані на охорону та забезпечення публічних інтересів.

У березні 2022 року Reuters повідомили, що Міністерство оборони України почало використовувати додаток «Clearview AI», який дає змогу розпізнавати обличчя осіб. Вказується, що невідомо, з якою конкретною метою його мають використовувати, проте сам розробник додатка вказував, що в їхній базі даних наявні безліч фото з російських соціальних мереж, як-от «Вконтакте», що даватиме змогу розпізнавати осіб-противників, допомагати в об’єднані біженців або ж ідентифікувати мертву особу швидше, ніж за відбитком пальця [74].

Зауважимо на проблематиці згаданого. База даних додатку «Clearview AI» поповнюється шляхом отримання публічно розміщених в Інтернеті фото, що порушує права осіб на приватність. У Великій Британії та Австралії вважають таку практику нелегальною [74]. Це є порушенням з огляду на відсутність згоди власників фото на використання їхніх зображень у таких цілях.

Станом на зараз, як нам відомо, офіційні органи держав світу ще не прийняли рішення щодо свого схвалення або обурення використанням «Clearview AI» в Україні, проте багато дослідників у сфері захисту персональних даних висловили своє занепокоєння щодо такого використання.

Система розпізнавання обличчя за своїм функціоналом є нескладною, тому може використовуватися непрофесіоналами, на відміну від розпізнавання за відбитками пальців або зубів [75, с. 2]. Більш того, FRT іноді недостатньо точна, тому є побоювання, що в Україні існує ризик хибного розпізнавання особи, що в умовах війни може мати неприпустимі наслідки [76].

Однією з небагатьох авторитетних позицій, яка має значну вагу, є твердження міжнародної організації Privacy International. Вони наголошують, що потенційні наслідки використання FRT у контексті війни можуть бути занадто жахливими, щоб їх прийнятно було б толерувати. Організація стверджує, що навіть найретельніші гарантії, які спільнота може встановити в часи миру та стабільності, зникають під час беззаконня і непередбачуваності війни. Саме тому Privacy International закликала керівництво компанії з розробки додатка «Clearview AI» відкликати надання такої технології в користування українським військовим [77].

Крім того, вагомою є й позиція Європейського парламенту. В одному з рішень він розкрив свої занепокоєння щодо використання органами правопорядку приватних баз, які містять матеріали для FRT, згадуючи у цьому контексті, зокрема, «Clearview AI». Європейський парламент наголошує, що більш ніж 3 мільярди фото були протиправно зібрані із соціальних мереж та інших Інтернет джерел, тому закликає органи правопорядку розкрити інформацію, чи ті користуються «Clearview AI» або аналогічними сервісами [78].

У межах справи *ACLU v. Clearview AI* було укладено угоду про врегулювання спору між Американським союзом захисту громадянських прав і «Clearview AI», за результатами якої було прийнято наказ суду. Положення цього наказу заборонили «Clearview AI» надавати безкоштовно або продавати доступ до своєї бази даних будь-якому приватному суб’єкту по всій країні загалом та на

п’ять років – будь-якому суб’єкту зі штату Іллінойс, включно з органами штату та місцевою поліцією [79].

Тож, можемо простежити, що хоч міжнародна спільнота не схвалювала використання цього додатка у мирний час, проте й за таких безпрецедентних обставин, як війна, залишається на такій позиції. Як стверджували низка дослідників та журналістів, його використання органами правопорядку було виправданим лише в досить обмежених випадках, коли були встановлені відповідні запобіжники, а на війні, де обставини є непередбачуваними, є підстави вважати, що це створює загрозу демократичним засадам.

Існує думка, що якщо вступ України до ЄС відбудеться дуже швидко, то використання «Clearview AI» у військових та потенційно цивільних цілях в Україні може стати тривожним прецедентом для країн ЄС [80].

Також для поглиблення нашого аналізу, ми дослідили наявну в Україні судову практику щодо використання FRT, щоб зрозуміти, по-перше, масштаб використання на практиці, а не покладатися на інформацію зі ЗМІ, а по-друге, спробувати виявити, чи судді власною правотворчістю уточнили згадані норми для балансування дискреційних повноважень.

Детальніше з переліком проаналізованих судових рішень та цитат можна ознайомитися у додатку до нашої роботи.

З проаналізованого ми можемо зробити висновок, що станом на зараз відсутня практика українських судів, які б розширено тлумачили Закон України «Про захист персональних даних», КПК України або інші акти, прийняті в Україні, у контексті FRT. Проте попри абстрактне і недостатнє правове регулювання використання FRT в Україні, ці технології знаходять своє застосування при виконанні правоохоронними органами своїх повноважень. Це зайвий раз підкреслює необхідність розробки належних нормативно-правових актів.

### *3.4. Використання штучного інтелекту в FRT для забезпечення публічних інтересів*

Додатково до згаданого, Європейський парламент має ще низку занепокоєнь щодо використання FRT у зв'язку з тим, що ці технології побудовані на базі ШІ. Європейський парламент у своєму рішенні від 6 жовтня 2021 року висловив свої побоювання щодо ризиків використання ШІ, зокрема, і в контексті застосування FRT органами правопорядку, а також рекомендації до дії. Серед іншого, у пункті 27 цього рішення Європейський парламент закликає ввести мораторіум на використання FRT органами правопорядку для цілей ідентифікації осіб, за винятком використання суто для ідентифікації жертв злочинів, до того часу, доки технічні стандарти таких технологій не стануть такими, які цілком відповідають фундаментальним правам людини. Водночас, отримані результати повинні бути неупереджені та недискримінаційні, а правове регулювання - закріплювати жорсткі заходи обмеження проти зловживань та суворий демократичний контроль і нагляд [78].

Враховуючи зазначені занепокоєння, а також розширення кола ризиків та неоднозначності щодо випадків застосування FRT, члени ЄС зараз працюють над нормативно-правовим актом, який би набагато краще врегулював питання використання цих технологій так, щоб мінімізувати порушення прав індивідів. Цим актом є AI Act, який зараз, як ми згадували, перебуває на стадії проєкту. Звертаємо увагу, що це саме регламент, а не директива. Норми регламенту мають пряму дію, а за директивою державам надаються дискреційні повноваження щодо шляхів імплементації відповідних положень.

Проте і цей акт не позбавлений недоліків. EDPB та EDPS у своїй окремій думці щодо проєкту цього акту критикують статтю щодо визначеного переліку випадків легального застосування технологій. На думку EDPB та EDPS, навіть встановлені в AI Act обмеження не є достатніми. Все одно кількість підозрюваних або злочинців буде достатньо високою, щоб цілком виправдовувати на цій підставі безперервне використання FRT [81, с. 11]. Саме тому EDPB та EDPS

рекомендують цілком заборонити використання FRT для автоматизованого розпізнавання у загальнодоступних місцях у будь-якому контексті [81, с. 11-12].

Такі побоювання є цілком зрозумілими. Особливо враховуючи практику використання ШІ у FRT для правоохоронних цілей, зокрема, і згаданий застосунок «Clearview AI», використання якого викликало багато занепокоєнь у регуляторів по всьому світу.

Попри згадані недоліки використання ШІ в FRT, є й протилежна думка. Т. Портер та Н. Фінк вважають, що повна заборона FRT піде на користь лише злочинцям. Вони стверджують, що заборона цих технологій – це легкий крок, але безвідповідальний. Усі засоби спостереження певною мірою порушують права людини. Нормотворці ЄС можуть та повинні забезпечити баланс між захистом приватності та захистом людей. Більш того, автори наголошують, що занепокоєння щодо упередженості, дискримінативності та неефективності FRT давно втратили свою актуальність. Такі твердження були правильні на ранніх етапах розвитку FRT. Наразі показники ілюструють порівняно кращі результати [82].

Існують і думки, що AI Act не буде відповідати GDPR. Проте Дослідницька служба Європейського парламенту у своєму звіті розкриває думку, що дуже ймовірно, що GDPR буде тлумачитися таким чином, щоб задовольнити як права суб’єктів даних, так і забезпечення корисного застосування ШІ [83, с. 76]. Дослідники погоджуються, що GDPR є дещо нечітким та невизначеним. Проте вони наголошують, що ефективне застосування норм AI Act значною мірою буде залежати, яким чином будуть надані відповідні рекомендації по GDPR [83, с. 77-78].

Не менш важливо зауважити, що ШІ може використовуватися для публічних інтересів, але FRT буде застосовуватися не щодо потенційних правопорушників, а щодо представників органів правопорядку.. Яскравим прикладом цього є розробка та використання FRT правозахисником та протестувальником з Портленду для виявлення та притягнення до

відповідальності поліцейських, які можуть зловживати власними повноваженнями [84].

*  *  *

Отже, під час дослідження правового регулювання FRT щодо використання цих технологій у публічно-правовому аспекті ми дійшли висновку, що попри його більшу зарегульованість порівняно з приватно-правовим контекстом, наявне регулювання є недостатнім та малоефективним, а часто навіть таким, що призводить до порушення прав людини.

Основною проблематикою публічного аспекту використання FRT є дуже високий шанс, що органи правопорядку через прагнення ефективніше виконувати свої обов'язки або спростити власну роботу будуть залучатися допомогою FRT із перевищенням власних дискреційних повноважень, що у багатьох випадках призводить до порушення низки прав людини. Здебільшого, таке трапляється через намагання забезпечити публічний інтерес за рахунок втручання у приватне життя осіб або у посягання на їхню свободу вираження поглядів або свободу зібрань. Таке втручання часто є непропорційним і може вести за собою порушення й інших прав осіб.

Через це низка регуляторів, дослідників та громадських активістів занепокоєнні використанням FRT органами правопорядку та закликали заборонити це. Проте існують і контрпозиції, які стверджують, що заборонивши використання FRT для більш ефективних охорони та забезпечення публічного правопорядку, спільнота уникне складної та контроверсійної теми, але тим самим зробить краще лише злочинцям.

Дійсно, описане у цьому розділі є доволі дискусійним питанням і, на нашу думку, буде залишатися таким ще довгий час. Особливо, якщо враховувати стрімкий розвиток ШІ та плани щодо прийняття спеціального нормативного регулювання щодо нього у доволі близькому майбутньому.

Загалом, ми схильні вважати, що ідеальне нормативно-правове регулювання для використання FRT у публічній сфері майже неможливо розробити. Такий позитивістський підхід, як правило, не охоплює всіх можливих випадків, а недостатня зарегульованість реалізації повноважень органів, які мають права використовувати FRT, призводитиме до перевищення ними своїх повноважень. Відповідно, доречними є низка роз'яснень, керівництв та досліджень, які тлумачать акти, зокрема, GDPR та LED, і надають роз'яснення, як правоохоронним органам доцільніше реалізовувати свої повноваження і що враховувати, щоб їхня поведінка забезпечувала дотримання прав людини, але водночас допомагала оберігати публічний порядок, тобто була збалансованою.

# ВИСНОВКИ

У межах цього дослідження, на наш погляд, нам вдалося виконати завдання, поставленні перед проведенням цього дослідження. Нижче описуємо висновки, до яких ми дійшли, виконавши кожне із завдань.

*Завдання 1*

FRT базуються на використанні комп'ютерних алгоритмів та ШІ. Процес функціонування таких технологій може бути спрямований на досягнення різних цілей, проте узагальнено поділяється на декілька етапів:

1) збір даних, які використовуються для тренування системи, з різноманітних джерел, якими можуть бути як соціальні мережі, так і внутрішні бази даних певних підприємств, органів правопорядку тощо;

2) тренування алгоритму за допомогою технології машинного навчання для забезпечення ефективності FRT, під час якого алгоритм аналізує різні параметри, як-от відстань між очима, ніздрями, вухами, площу лоба тощо;

3) після такого тренування відбувається тестування алгоритму та його доопрацювання;

4) остаточним етапом є впровадження розробленої технології для використання у реальних умовах.

*Завдання 2*

Галузями, сфера регулювання яких поширюється на FRT, є щонайменше захист персональних даних, цивільне право, адміністративне право та кримінально-процесуальне право. Ця знахідка дала змогу нам більш ефективно дослідити застосування FRT.

*Завдання 3*

При використанні FRT у приватно-правовому аспекті основним є дотримання прав людини, зокрема, права на приватне життя, норми щодо захисту якого віднайшли свій розвиток у законодавстві про персональні дані. Тому при використанні FRT приватними суб'єктами слід забезпечити відповідність такої поведінки закріпленим нормам про захист персональних даних та нормам про

використання ШІ, які будуть прийняті найближчим часом, бо зараз перебувають у розробці. Водночас, поряд з правом на приватне життя є й свобода ведення підприємницької діяльності. На осіб, що застосовують FRT при веденні підприємницької діяльності, покладено більше обов'язків щодо дотримання відповідного законодавства, ніж на їхніх споживачів чи клієнтів. На противагу, суб'єкти господарювання володіють свободою ведення підприємницької діяльності та свободою договору, що не зобов'язує їх використовувати FRT. Такі суб'єкти на власний розсуд та з усвідомленням зобов'язань та загроз ведуть ризикову господарську діяльність, спрямовану на одержання прибутку.

*Завдання 4*

Щодо публічно-правового аспекту, у багатьох країнах світу закріплено норми щодо використання FRT органами правопорядку, оскільки застосування технологій цими суб'єктами часто порушує принцип обмеження дискреційних повноважень та найбільше загрожує дотриманню прав людини. Попри нормативне закріплення регуляторних положень, практика їх застосування не завжди є ефективною. У зв'язку з тим, що закріплені норми є дещо абстрактними та відкритими до тлумачення, при безпосередньому використанні FRT для забезпечення публічних інтересів на практиці виникає багато запитань. Тому багато науково-дослідних та консультативних органів розробили власні рекомендації щодо того, як слід тлумачити законодавство щодо застосування органами правопорядку FRT. Попри це, у суспільстві все одно залишаються занепокоєння щодо таких технологій, тому уряди деяких країн, а у деяких випадках і муніципальна влада адміністративно-територіальних одиниць, приходять до рішення заборонити використання FRT. Такі занепокоєння зрозумілі, особливо враховуючи практику судів, які неодноразово доходили до рішення, що органи правопорядку порушують права осіб при використанні FRT. Деякі дослідники вважають підходи щодо заборони FRT дещо радикальними та непропорційними. Особливо враховуючи, що наразі розробляється перший нормативно-правовий акт про регулювання ШІ, прийняття якого може сприяти більш розумному, пропорційному та ефективному регулюванню FRT.

*Завдання 5*

Ми з упевненістю можемо стверджувати, що наявне наразі правове регулювання FRT у приватно-правовій та публічно-правовій сфері не є достатнім. Такий наш висновок ґрунтувався на дослідженому законодавстві ЄС, США та України.

Законодавство ЄС найбільш розроблене та системне з нам відомих. Проте навіть такий обсяг правових норм не забезпечує належного регулювання FRT ні у приватно-правовому, ні у публічно-правовому аспекті.

У США дещо інша специфіка правового регулювання через федеративний устрій цієї країни. На рівні федерації ще не прийнято ані положень, які б регулювали FRT, ані системного акту про захист персональних даних. Хоч деякі штати на своєму рівні розробили та прийняли відповідні акти, це не забезпечує достатнього захисту прав людини.

Законодавство України майже не містить норм, які належним чином регулювали використання FRT як приватними, так і публічними суб'єктами, включно з органами правопорядку. Можна було б стверджувати, що за відсутності належного нормативно-правового регулювання можна керуватися загальними принципами права, проте досліджена нами практика українських судів показала, що наразі такий підхід не віднайшов свого застосування серед суддів.

З проаналізованого ми вбачаємо перспективним розвиток законодавства щодо застосування FRT, оскільки по-перше, ці технології надають низку можливостей, якими було б нерозумно нехтувати, по-друге, їхнє застосування викликає багато дискусій та побоювань у суспільства вже багато років, а по-третє, FRT функціонує за допомогою ШІ, зацікавленість навколо якого зросла останнім часом. З огляду на це, ми припускаємо, що найближчим часом не лише у ЄС, а й в інших країнах, включно з Україною, будуть розроблені та прийняті акти про регулювання ШІ, що впливатимуть на застосування FRT всіма суб'єктами. Проте ми думаємо, що воно є лише частиною необхідного регулювання, тому слід буде доопрацювати норми про захист персональних даних та застосування таких

технологій публічними органами. В Україні це питання є маловрегульованим, що хоч не усуває загроз порушення прав людини, але надає перспективи та простір для розробки правового регулювання, яке буде більш ефективним, ніж в ЄС та США.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

*У магістерській роботі:*

1. Almeida D., Shmarko K., Lomas E. The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. AI and Ethics. Volume 2. 2022. URL: https://link.springer.com/article/10.1007/s43681-021-00077-w (дата звернення: 25.01.2024).

2. Madiega T., Mildebrath H. Regulating facial recognition in the EU. European Parliamentary Research Service. 2021. 38 p. URL: https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf (дата звернення: 26.01.2024).

3. Aniulis H. Facial Recognition Technology, Privacy and Administrative Law. UNSW Law Journal. Volume 45(4). 2022. P. 1513-1555. URL: https://www.unswlawjournal.unsw.edu.au/wp-content/uploads/2022/12/Issue-454-07-Aniulis.pdf (дата звернення: 25.01.2024).

4. Machine Learning. IBM Cloud Education. 2020. URL: https://www.ibm.com/cloud/learn/machine-learning (дата звернення: 26.01.2024).

5. Lewis J., Crumpler W. How Does Facial Recognition Work? Center for Strategic & International Studies. 2021. URL: https://www.csis.org/analysis/how-does-facial-recognition-work (дата звернення: 26.01.2024).

6. Matyunina J. The Ultimate Guide to Face Recognition. Codetiburon. 2020. URL: https://codetiburon.com/ultimate-guide-to-face-recognition/ (дата звернення: 26.01.2024).

7. Kortli Y., Jridi M., Al Falou A., Atri M. Face Recognition Systems: A Survey. Sensors (Basel). 2020. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7013584/ (дата звернення: 06.05.2024).

8. Ahmed Z. Can facial recognition technology detect you with a mask?. Gulf Business. 2022. URL: https://gulfbusiness.com/can-facial-recognition-technology-detect-you-with-a-mask/ (дата звернення: 28.04.2024).

9. Buckley B., Hunter M. Say cheese! Privacy and facial recognition. Computer Law & Security Review. Volume 27, Issue 6. 2011. P. 637-640.

10. Law Enforcement Facial Recognition Use Case Catalog. IJIS Institute and International Association of Chiefs of Police (IACP). 2019. 21 p. URL: https://www.theiacp.org/sites/default/files/2019-10/IJIS_IACP%20WP_LEITTF_Facial%20Recognition%20UseCasesRpt_20190322.pdf (дата звернення: 26.01.2024).

11. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. Дата оновлення: 27.10.2022 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 26.01.2024).

12. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата звернення: 26.01.2024).

13. California Consumer Privacy Act of 2018. Amended by initiative Proposition 24 dated 3 November 2020. URL: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5# (дата звернення: 26.01.2024).

14. Ustaran E. European Dara Protection Law and Practice. Second Edition. The International Association of Privacy Professionals. 2019. 477 p.

15. 14 Intriguing New And Potential Uses For Facial Recognition Technology. 2023. Forbes. URL: https://www.forbes.com/sites/forbestechcouncil/2023/08/18/14-intriguing-new-and-potential-uses-for-facial-recognition-technology/?sh=1892d0ef2666 (дата звернення: 31.01.2024).

16. 4 The Impact of FRT Deployment on Human Rights. Facing the Risk: Part 2: Mapping the Human Rights Risks in the Deployment of Facial Recognition

Technology. 2021. P. 10-25. URL: https://www.jstor.org/stable/resrep33749.7 (дата звернення: 31.01.2024).

17. Забули картку та телефон? Не проблема. Приватбанк. URL: https://privatbank.ua/facepay24 (дата звернення: 06.02.2024).

18. Як отримати Дія.Підпис? URL: https://paperless.diia.gov.ua/instruction/yak-otrimati-diyapidpis (дата звернення: 06.02.2024).

19. Information Commissioner's Opinion: The use of live facial recognition technology in public places. Information Commissioner's Office. 2021. 67 p. URL: https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf (дата звернення: 06.02.2024).

20. Li S., Sarno D. Advertisers start using facial recognition to tailor pitches. Los Angeles Times. 2011. URL: https://www.latimes.com/business/la-xpm-2011-aug-21-la-fi-facial-recognition-20110821-story.html (дата звернення: 06.02.2024).

21. Конвенція про захист прав людини та основоположних свобод. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 06.02.2024).

22. Загальна декларація прав людини. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text (дата звернення: 05.05.2024).

23. Borrell J. Let's make 2023 a year of turning the tide on human rights. The European External Action Service. 2023. URL: https://www.eeas.europa.eu/eeas/let%E2%80%99s-make-2023-year-turning-tide-human-rights_en (дата звернення: 06.02.2024).

24. CPRA vs. GDPR – The notable similarities and differences. Securiti. URL: https://securiti.ai/cpra-vs-gdpr/ (дата звернення: 06.02.2024).

25. Rippy S. Virginia passes the Consumer Data Protection Act. IAPP. 2021. URL: https://iapp.org/news/a/virginia-passes-the-consumer-data-protection-act/ (дата звернення: 06.02.2024).

26. Biometric Information Privacy Act. 740 ILCS 14/. URL: https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57 (дата звернення: 06.02.2024).

27. Камери відеоспостереження: що варто знати кожному, щоб захистити свою приватність: роз'яснення Уповноваженого Верховної Ради України з прав людини. Київ. 2022. 28 с. URL: https://ombudsman.gov.ua/storage/app/media/%D0%97%D0%9F%D0%94/rozyasnennya.pdf (дата звернення: 05.05.2024).

28. Julin S. 3 Key Considerations for GDPR Compliance with Facial Recognition Technology. Lexology. 2020. URL: https://www.lexology.com/library/detail.aspx?g=bf9441e4-d70c-4a1a-ab15-726b2b281345 (дата звернення: 06.02.2024).

29. Guidelines 3/2019 on processing of personal data through video devices. The European Data Protection Board. 2020. 33 p. URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf (дата звернення: 06.02.2024).

30. Coseraru R. Facial Recognition Systems and Their Data Protection Risks under the GDPR: Master Thesis. Tilburg University. 2017. 91 p. URL: https://arno.uvt.nl/show.cgi?fid=143731 (дата звернення: 06.02.2024).

31. Commercial Facial Recognition Privacy Act of 2019. S.847. 2019. URL: https://www.congress.gov/bill/116th-congress/senate-bill/847/text (дата звернення: 06.02.2024).

32. Rowe E. Regulating Facial Recognition Technology in the Private Sector. Stanford Technology Law Review. Vol. 24:1. 2020. 54 p. URL: https://web.archive.org/web/20220701031613/https:/www-cdn.law.stanford.edu/wp-content/uploads/2020/12/Rowe-FINAL-Facial-Recognition.pdf (дата звернення: 06.02.2024).

33. Slate et al. v. TikTok, Inc. et al. Case Number 3:2020cv02992. U.S. District Court for the Northern District of California. 2020. 19 p. URL:

https://www.classaction.org/media/slate-et-al-v-tiktok-inc-et-al.pdf (дата звернення: 17.02.2024).

34. Fambrough v. Uber Technologies Inc. The United States District Court for the Western District of Missouri. No. 4:19-cv-0398-DGK. 2019. 4 p. URL: https://www.govinfo.gov/content/pkg/USCOURTS-mowd-4_19-cv-00398/pdf/USCOURTS-mowd-4_19-cv-00398-0.pdf (дата звернення: 17.02.2024).

35. Corrigendum to the position of the European Parliament adopted at first reading on 13 March 2024 with a view to the adoption of Regulation (EU) 2024/ ..... of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). P9_TA(2024)0138. European Parliament. 2024. 458 p. URL: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf (дата звернення: 05.05.2024).

36. Rozen C., Deutsch J. Regulate AI? How US, EU and China Are Going About It. Bloomberg. 2024. URL: https://www.bloomberg.com/news/articles/2024-03-13/regulate-ai-how-us-eu-and-china-are-going-about-it (дата звернення: 01.05.2024).

37. Про схвалення Концепції розвитку штучного інтелекту в Україні: розпорядження Кабінету Міністрів України від 02.12.2020 р. № 1556-р. Дата оновлення: 29.12.2021 р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 11.02.2024).

38. Sioli L. A European Strategy for Artificial Intelligence. CEPS webinar – European approach to the regulation of artificial intelligence. 2021. 21 p. URL: https://www.ceps.eu/wp-content/uploads/2021/04/AI-Presentation-CEPS-Webinar-L.-Sioli-23.4.21.pdf (дата звернення: 11.02.2024).

39. EU AI Act: first regulation on artificial intelligence. European Parliament. 2023. URL: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence (дата звернення: 11.02.2024).

40. EthanBradberry098. Bing’s AI image input blurs any faces including anime characters. Reddit. 2023. URL: https://www.reddit.com/r/bing/comments/14ojj5o/bings_ai_image_input_blurs_any_faces_including/?rdt=41016 (дата звернення: 11.02.2024).

41. Advances in Facial Recognition Technology Have Outpaced Laws, Regulations; New Report Recommends Federal Government Take Action on Privacy, Equity, and Civil Liberties Concerns. The National Academies of Sciences, Engineering, and Medicine. 2024. URL: https://www.nationalacademies.org/news/2024/01/advances-in-facial-recognition-technology-have-outpaced-laws-regulations-new-report-recommends-federal-government-take-action-on-privacy-equity-and-civil-liberties-concerns (дата звернення: 11.02.2024).

42. Doffman Z. New York School District First In U.S. To Adopt Controversial Facial Recognition. Forbes. 2019. URL: https://www.forbes.com/sites/zakdoffman/2019/05/30/foolish-facial-recognition-about-to-hit-u-s-public-schools-for-the-first-time/?sh=2ac31d2646a0 (дата звернення: 11.02.2024).

43. Про затвердження Порядку попередньої ідентифікації віку користувачів веб-сайтів виробників, імпортерів пристроїв для споживання тютюнових виробів без їх згоряння та/або електронних сигарет: постанова Кабінету Міністрів України від 11.08.2023 р. № 839. URL: https://zakon.rada.gov.ua/laws/show/839-2023-%D0%BF#Text (дата звернення: 11.02.2024).

44. Raposo V. The Use of Facial Recognition Technology by Law Enforcement in Europe: a Non-Orwellian Draft Proposal. European Journal on Criminal Policy and Research. 2022. URL: https://link.springer.com/article/10.1007/s10610-022-09512-y#auth-Vera_L_cia-Raposo (дата звернення: 11.02.2024).

45. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation,

detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680 (дата звернення: 11.02.2024).

46. Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Version 2. 2023. 52 p. URL: https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf (дата звернення: 11.02.2024).

47. Report on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters. (2020/2016(INI)). The European Parliament. 2021. URL: https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.html (дата звернення: 12.02.2024).

48. Information Commissioner's Opinion: The use of live facial recognition technology by law enforcement in public places. Information Commissioner's Office. 2019. 24 p. URL: https://jerseyoic.org/media/moqjayy1/live-frt-law-enforcement-opinion-20191031.pdf (дата звернення: 12.02.2024).

49. Facial Recognition Act of 2022. H.R.9061. 2022. URL: https://www.congress.gov/bill/117th-congress/house-bill/9061/text?s=1&r=7 (дата звернення: 12.02.2024).

50. Facial Recognition Act of 2023. H.R.6092. 2023. URL: https://www.congress.gov/bill/118th-congress/house-bill/6092/text?s=1&r=1&q=%7B (дата звернення: 12.02.2024).

51. Facial Recognition and Biometric Technology Moratorium Act of 2023. H.R.1404. 2023. URL: https://www.congress.gov/bill/118th-congress/house-bill/1404/text (дата звернення: 13.02.2024).

52. Amended in Committee 5/6/19. File No. 190110. Ordinance. 2019. 21 p. URL: https://sfgov.legistar.com/View.ashx?M=F&ID=7206781&GUID=38D37061-4D87-4A94-9AB3-CB113656159A (дата звернення: 13.02.2024).

53. Ng A. Portland, Oregon, passes toughest ban on facial recognition in US. CNET. 2020. URL: https://www.cnet.com/news/politics/portland-passes-the-toughest-ban-on-facial-recognition-in-the-us/ (дата звернення: 13.02.2024).

54. Bridges, R (On the Application Of) v South Wales Police [2020] EWCA Civ 1058. 2020. URL: https://www.bailii.org/ew/cases/EWCA/Civ/2020/1058.html (дата звернення: 13.02.2024).

55. State of New Jersey vs. Francisco Arteaga. Superior Court of New Jersey. Docket No. A-3078-21. 2023. URL: https://law.justia.com/cases/new-jersey/appellate-division-published/2023/a-3078-21.html (дата звернення: 13.02.2024).

56. Glukhin v. Russia. 11519/20. 2023. URL: https://hudoc.echr.coe.int/eng?i=001-225655 (дата звернення: 05.05.2024).

57. Про виконання рішень та застосування практики Європейського суду з прав людини: Закон України від 23.02.2006 р. № 3477-IV. Дата оновлення: 02.12.2012 р. URL: https://zakon.rada.gov.ua/laws/show/3477-15#Text (дата звернення: 13.02.2024).

58. Про Національну поліцію: Закон України від 02.07.2015 р. № 580-VIII. Дата оновлення: 04.05.2024 р. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 05.05.2024).

59. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 р. № 2135-XII. Дата оновлення: 31.03.2023 р. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text (дата звернення: 13.02.2024).

60. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 р. № 4651-VI. Дата оновлення: 19.04.2024 р. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 05.05.2024).

61. Авдєєва Т., Людва А. Наскільки “прозора” законність діяльності Clearview AI в Україні? Лабораторія цифрової безпеки. 2023. URL: https://dslua.org/publications/clearview-ai-v-ukraini/ (дата звернення: 13.02.2024).

62. Проскуряков С. Камери спостереження використовують у боротьбі з коронавірусом. Ми вивчили, як ця система працює в Києві й чому це небезпечно.

Заборона. 2020. URL: https://zaborona.com/kamery-sposterezhennya-vykorystovuyut/ (дата звернення: 13.02.2024).

63. Авдєєва Т. Чи легально встановлювати на міських вулицях камери із системою розпізнавання облич? Центр демократії та верховенства права. 2021. URL: https://cedem.org.ua/analytics/kamery-rozpiznavannya-oblych/ (дата звернення: 13.02.2024).

64. Каменєв М., Золотар С. Гостре око Старшого Брата. Реанімаційний Пакет Реформ. 2019. URL: https://rpr.org.ua/news/hostre-oko-starshoho-brata/ (дата звернення: 13.02.2024).

65. Курманова Т., Яворський В. Систему розпізнавання обличчя встановлюють без жодного профільного закону – Яворський. Громадське Радіо. 2023. URL: https://hromadske.radio/podcasts/my-ie-buly-y-budem-informatsiynyy-maraton/systemu-rozpiznavannia-oblychchia-vstanovliuiut-bez-zhodnoho-profilnoho-zakonu-yavorskyy (дата звернення: 13.02.2024).

66. Договір № 10/20-04 від 02.04.2020 р. Prozorro. 2020. 15 с. URL: https://public.docs.openprocurement.org/get/3177061844e541b490ee1b8188140464?KeyID=52462340&Signature=%252BxSVcX26YLu%252Be4Z1oGkwcYWiCRI3G2kV9BtprctzNroU5L0n0KNS7cQibRMebPkaU7hZfxJD7rlk7CFPvW%2FGAg%253D%253D (дата звернення: 13.02.2024).

67. Ільченко Л. У КМДА відреагували на розслідування щодо камер спостереження Hikvision. Економічна правда. 2024. URL: https://www.epravda.com.ua/news/2024/01/26/709216/ (дата звернення: 13.02.2024).

68. Про затвердження Положення про комплексну систему відеоспостереження міста Києва: рішення Київської міської ради від 05.07.2018 р. № 1195/5259. URL: https://kyivcity.gov.ua/npa/pro_zatverdzhennya_polozhennya_pro_kompleksnu_sistemu_videosposterezhennya_mkiyeva/File_2sfxfncsme_1195-5259/ (дата звернення: 13.02.2024).

69. У рамках проекту «Безпечне місто» запущено новий аналітичний модуль відеоспостереження, що прискорить пошук правопорушників. Офіційний

портал Києва. 2019. URL: https://kyivcity.gov.ua/news/u_ramkakh_proektu_bezpechne_misto_zapuscheno_noviy_analitichniy_modul_videosposterezhennya_scho_priskorit_poshuk_pravoporushnikiv/ (дата звернення: 13.02.2024).

70. Case of Catt v. The United Kingdom. Application no. 43514/15. 2019. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-189424%22]} (дата звернення: 13.02.2024).

71. Положення про систему відеоспостереження міста Запоріжжя, затверджене рішенням міської ради 27.03.2019 р. № 23. 14 с. URL: https://zp.gov.ua/upload/content/o_1d7uhc8rt1dmvdtc13li1l2e1oes2n.pdf (дата звернення: 13.02.2024).

72. Мамченко Н. В Україні запускають Єдину системи відеомоніторингу стану публічної безпеки, у тому числі – розпізнавання обличчя. Судово-юридична газета. 2024. URL: https://sud.ua/uk/news/publication/290740-v-ukraine-zapuskayut-edinuyu-sistemu-videomonitoringa-sostoyaniya-publichnoy-bezopasnosti-v-tom-chisle-raspoznavanie-litsa (дата звернення: 13.02.2024).

73. Про єдину систему відеомоніторингу стану публічної безпеки: Проєкт Закону від 20.02.2024 р. № 11031. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/43733 (дата звернення: 05.05.2024).

74. Dave P., Dastin J. Exclusive: Ukraine has started using Clearview AI's facial recognition during war. Reuters. 2022. URL: https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/ (дата звернення: 13.02.2024).

75. Cornett III D., Bolme D., Steadman D., Sauerwein K., and Saul T. Effects of Postmortem Decomposition on Face Recognition. Conference: IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS 2019) – Tampa, Florida, United States of America. 2019. 8 p. URL: https://www.osti.gov/servlets/purl/1559672 (дата звернення: 13.02.2024).

76. Moreno F. Facial recognition technology: how it's being used in Ukraine and why it's still so controversial. The Conversation. 2022. URL:

https://theconversation.com/facial-recognition-technology-how-its-being-used-in-ukraine-and-why-its-still-so-controversial-183171 (дата звернення: 13.02.2024).

77. The Clearview/Ukraine partnership – How surveillance companies exploit war. Privacy International. 2022. URL: https://privacyinternational.org/news-analysis/4806/clearviewukraine-partnership-how-surveillance-companies-exploit-war (дата звернення: 13.02.2024).

78. 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)). European Parliament. 2021. URL: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html (дата звернення: 13.02.2024).

79. Consent Order of Permanent and Time-Limited Injunctions Against Defendant Clearview AI, Inc. 2022. URL: https://www.aclu.org/cases/aclu-v-clearview-ai?document=aclu-v-clearview-ai-order-denying-motion-dismiss (дата звернення: 13.02.2024).

80. Meacham D., Gak M. Does facial recognition tech in Ukraine's war bring killer robots nearer? OpenDemocracy. 2022. URL: https://www.opendemocracy.net/en/technology-and-democracy/facial-recognition-ukraine-clearview-military-ai/ (дата звернення: 13.02.2024).

81. EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). 2021. 22 p. URL: https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf (дата звернення: 13.02.2024).

82. Porter T., Fink N. Euroviews. Facial recognition technology should be regulated, but not banned. Euronews. 2023. URL: https://www.euronews.com/2023/08/07/facial-recognition-technology-should-be-regulated-but-not-banned (дата звернення: 13.02.2024).

83. The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. European Parliamentary Research Service. 2020. 84 p. URL:

https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf (дата звернення: 13.02.2024).

84. Hill K. Activists Turn Facial Recognition Tools Against the Police. The New York Times. 2020. URL: https://www.nytimes.com/2020/10/21/technology/facial-recognition-police.html (дата звернення: 13.02.2024).

*У додатку до магістерської роботи:*

85. Ухвала Шаргородського районного суду Вінницької області від 24.07.2023 р. у справі № 152/871/23. URL: https://reyestr.court.gov.ua/Review/112355225 (дата звернення: 16.02.2024).

86. Ухвала Білоцерківського міськрайонного суду Київської області від 09.09.2022 р. у справі № 357/4979/22. URL: https://reyestr.court.gov.ua/Review/106154081 (дата звернення: 16.02.2024).

87. Рішення Дружківського міського суду Донецької області від 04.03.2024 р. у справі № 229/7853/23. URL: https://reyestr.court.gov.ua/Review/117616021 (дата звернення: 02.04.2024).

88. Вирок Київського районного суду м. Харкова від 30.05.2023 р. у справі № 953/1712/23. URL: https://reyestr.court.gov.ua/Review/111213116 (дата звернення: 16.02.2024).

89. Вирок Обухівського районного суду Київської області від 06.12.2022 р. у справі № 761/31532/21. URL: https://reyestr.court.gov.ua/Review/107735753 (дата звернення: 16.02.2024).

90. Вирок Деснянського районного суду м. Києва від 23.12.2021 р. у справі № 754/4733/21. URL: https://reyestr.court.gov.ua/Review/102187979 (дата звернення: 16.02.2024).

91. Вирок Кузнецовського районного суду Рівненської області від 09.02.2021 р. у справі № 565/1354/19. URL: https://reyestr.court.gov.ua/Review/94809162 (дата звернення: 16.02.2024).

92. Ухвала Івано-Франківського міського суду Івано-Франківської області від 18.12.2023 р. у справі № 344/22934/23. URL: https://reyestr.court.gov.ua/Review/115701140 (дата звернення: 16.02.2024).

93. Ухвала Оболонського районного суду м. Києва від 10.11.2023 р. у справі № 756/14096/18. URL: https://reyestr.court.gov.ua/Review/114871905 (дата звернення: 16.02.2024).

94. Ухвала Подільського районного суду м. Києва від 14.03.2023 р. у справі № 758/2767/23. URL: https://reyestr.court.gov.ua/Review/110067415 (дата звернення: 16.02.2024).

95. Ухвала Голосіївського районного суду м. Києва від 19.09.2022 р. у справі № 752/8627/21. URL: https://reyestr.court.gov.ua/Review/106360351 (дата звернення: 16.02.2024).

96. Ухвала Подільського районного суду м. Києва від 15.09.2022 р. у справі № 758/8070/22. URL: https://reyestr.court.gov.ua/Review/110647672 (дата звернення: 16.02.2024).

97. Ухвала Дніпровського районного суду м. Києва від 31.08.2022 р. у справі № 755/4620/21. URL: https://reyestr.court.gov.ua/Review/106134218 (дата звернення: 16.02.2024).

98. Ухвала Личаківського районного суду м. Львова від 11.08.2022 р. у справі № 463/4922/22. URL: https://reyestr.court.gov.ua/Review/105704391 (дата звернення: 16.02.2024).

99. Ухвала Дубенського міськрайонного суду Рівненської області від у 26.11.2021 р. справі № 559/2971/21. URL: https://reyestr.court.gov.ua/Review/101411386 (дата звернення: 16.02.2024).

100. Ухвала Київського апеляційного суду від 29.06.2021 р. у справі № 757/3027/21-к. URL: https://reyestr.court.gov.ua/Review/98127232 (дата звернення: 16.02.2024).

101. Ухвала Шевченківського районного суду м. Києва від 11.07.2020 р. у справі № 761/20554/20. URL: https://reyestr.court.gov.ua/Review/90333610 (дата звернення: 16.02.2024).

102. Постанова Шостого апеляційного адміністративного суду від 28.02.2023 р. № 358/857/22. URL: https://reyestr.court.gov.ua/Review/109255753 (дата звернення: 16.02.2024).

103. Постанова Третього апеляційного адміністративного суду від 12.01.2021 р. у справі № 280/4979/20. URL: https://reyestr.court.gov.ua/Review/94263010 (дата звернення: 16.02.2024).

## ДОДАТОК

**Таблиця з описом дослідженої судової практики українських судів, де згадується застосування FRT**

| ***Судове рішення*** | ***Згадка про використання технології*** |
|---|---|
| **Приватно-правова сфера** | |
| Ухвала Шаргородського районного суду Вінницької області від 24.07.2023 р. у справі № 152/871/23 | *«Підписавши 12.11.2020 року Анкету-заяву цифровим власноручним підписом на екрані власно смартфону у мобільному додатку «monobank», відповідач підтвердив, що отримав примірник Договору в мобільному додатку «monobank», ознайомився та погодився з умовами Договору, уклав Договір та зобов`язався виконувати його умови.»* [85]<br><br>*«Пунктом 4.3 Розділу 1 Умов визначено, що згоду клієнта зі змінами, доповненнями Умов і правил, може бути підтверджено, зокрема та не виключно: проведенням клієнтом банківських операцій, отриманням банківських послуг, яке супроводжується оформленням касових документів; документом на паперовому носії з* |

| *Судове рішення* | *Згадка про використання технології* |
|---|---|
| | *реквізитами, що дозволяють ідентифікувати цей документ; документом в електронному вигляді із застосуванням електронного/електронного цифрового підпису; введенням пін-коду, паролів доступу до додатку, використанням біометричних даних клієнта (відбитки пальців, в тому числі за допомогою технології TouchID, або розпізнавання обличчя, в тому числі за допомогою технології FaceID).»* [85] |
| Ухвала Білоцерківського міськрайонного суду Київської області від 09.09.2022 р. у справі № 357/4979/22 | *«Разом з цим, під час досудового розслідування отримано інформацію про те, що « ІНФОРМАЦІЯ_1 » є системою, призначеною для дистанційного керування банківськими рахунками АТ КБ « ІНФОРМАЦІЯ_2 » й інших українських банків у режимі реального часу. Доступ до системи може бути здійснений як через веб-версію, так і через мобільні додатки на операційних системах «Android» та «IOS». Доступ до автоматизованої інформаційної системи «ІНФОРМАЦІЯ_4» у мобільній версії доступний як по введенню звичайного пароля, такі з допомогою технологій* |

| *Судове рішення* | *Згадка про використання технології* |
|---|---|
| | *біометричної автентифікації по відбитку пальця або через розпізнавання обличчя.»* [86] |
| Рішення Дружківського міського суду Донецької області від 04.03.2024 р. у справі № 229/7853/23 | *«Для наступних входів в Систему Клієнту необхідно: ввести Логін для входу; ввести Пароль для входу. На Мобільних пристроях, які підтримують технології біометрії, Клієнту може бути надана можливість виконати вхід в Мобільний додаток «Райффайзен Онлайн» з використанням власних біометричних даних, а саме за відбитком пальця або технологією розпізнавання обличчя.»* [87] |
| **Публічно-правова сфера** | |
| Вирок Київського районного суду м. Харкова від 30.05.2023 р. у справі № 953/1712/23 | *«Увечері 08 березня 2022 року, більш точний час не встановлений, ОСОБА_7 , діючи умисно на шкоду суверенітетові, територіальній цілісності та недоторканності, обороноздатності, державній безпеці України […] прибув та незаконно проник разом з невстановленими представниками військових формувань* |

| ***Судове рішення*** | ***Згадка про використання технології*** |
|---|---|
| | *держави-агресора на територію приватного домоволодіння депутата Вовчанської міської ради Харківської області ОСОБА_23 […] ОСОБА_7 з метою належного виконання представниками військових формувань держави-агресора поставленого завдання здійснив ідентифікацію особи ОСОБА_23 шляхом розпізнавання його обличчя та підтвердження особи.»* [88] |
| Вирок Обухівського районного суду Київської області від 06.12.2022 р. у справі № 761/31532/21 | *«Хлопець в білому повідомив, що вб`є його, якщо потерпілий не віддасть всі цінні речі та кошти. Потерпілий віддав їх свій годинник «Ролекс», браслет та банківські картки. Потім, вони забрали його телефон, виявили на ньому крипто гаманець та намагались отримати до нього доступ. Для цього вони у функції розпізнавання обличчя змінили обличчя потерпілого на хлопця в білому, проте все рівно не могли отримати доступ. Протягом всього часу йому надягали на голову балаклаву і він не міг бачити, декілька разів її знімали.* |

| ***Судове рішення*** | ***Згадка про використання технології*** |
|---|---|
| | *Щоб примусити його дати доступ до всіх програм на телефону де були фінансові рахунки, хлопець в чорному дістав ніж та поранив його в ліву ногу та продовжували йому погрожувати та били кулаками в груди.»* [89] |
| Вирок Деснянського районного суду м. Києва від 23.12.2021 р. у справі № 754/4733/21 | *«Так, представник потерпілого ОСОБА_6 показав, що 5.03.2021 р. приблизно о 18 год. по радіостанції йому повідомила охорона про затримання жінки, яка намагалась винести з торгового залу магазину неоплачений товар. На його пропозицію цю жінку, якою виявилася обвинувачена ОСОБА_3 , завели до кімнати охорони, де вона називалася різними прізвищами. Він запропонував обвинуваченій розрахуватися за товар, який вона намагалася викрасти, але вона повідомила, що у неї немає грошей. Він викликав поліцію і вже в присутності працівників поліції ОСОБА_3 витягла зі свого рюкзаку товар, що намагалася викрасти, дві упаковки по 210 г дитячої каші, індюшине філе вагою 3212 г, свиний биток вагою 1686 г, свиний кострець вагою 2,420 г. На його* |

| *Судове рішення* | *Згадка про використання технології* |
|---|---|
| | *запитання обвинувачена повідомила, що раніше не затримувалась, але в базі ТОВ "Сільпо-Фуд" встановлена програма розпізнавання облич, завдяки якій було встановлено, що ОСОБА_3 раніше вчинила крадіжку в магазині "Сільпо" на Харківському шосе в м. Києві.»* [90] |
| Вирок Кузнецовського районного суду Рівненської області від 09.02.2021 р. у справі № 565/1354/19 | *«Лист заступника начальника УКР ГУНП в Рівненській області ОСОБА_332 №255/14/02-2019 від 14 лютого 2019 року, /том 1 а.п.274/ свідчить про направлення слідчому СУ ГУНП в Рівненській області ОСОБА_45 матеріалів та відеозаписів з наступних камер відео спостереження «Безпечне місто» в м.Рівне за 06 лютого 2019 року, розташованих на привокзальній площі залізничного вокзалу м.Рівне: КО 13.1 (перехрестя вул.Ніла Хасевича - привокзальний майдан); КО 13.3 (привокзальний майдан); КО 13.4 (привокзальний майдан); КО 13.5 (привокзальний майдан); камери 46 (розпізнавання облич); камери 45 (розпізнавання обличь).»* [91] |
| Ухвала Івано-Франківського міського суду Івано- | *«Впродовж 2023 року дізнавачем неодноразово* |

| ***Судове рішення*** | ***Згадка про використання технології*** |
|---|---|
| Франківської області від 18.12.2023 р. у справі № 344/22934/23 | *надавались доручення оперативному підрозділу на проведення слідчих (розшукових) дій у кримінальному провадженні щодо встановлення особи, якій видано паспорт громадянина України для виїзду за кордон серії НОМЕР_3 . У ході виконання вказаних доручень зображення особи, якій видано паспорт громадянина України для виїзду за кордон серії НОМЕР_3 перевірялось по базах НПУ та по наявних он-лайн програмах розпізнавання обличчя, однак встановити особу, яка зображена на фото, не представилось можливим.»* [92] |
| Ухвала Оболонського районного суду м. Києва від 10.11.2023 р. у справі № 756/14096/18 | *«На вирішення експертів поставити наступні запитання:[…]»* [93]<br>*«[…]3.Чи проводилася станом на січень 2014 року ідентифікація облікового запису користувача до конкретної фізичної особи під час здійснення входу та упродовж активної сесії АСДС (КП "Д-3") Обухівського районного суду Київської області за допомогою* |

| ***Судове рішення*** | ***Згадка про використання технології*** |
|---|---|
| | *використання КЕП/ЕЦП та/або біометричних параметрів (відбитки пальців, розпізнавання сітківки ока або обличчя тощо) та/або вбудованої або зовнішньої периферійної відеокамери? […]»* [93] |
| Ухвала Подільського районного суду м. Києва від 14.03.2023 р. у справі № 758/2767/23 | *«Проведено моніторинг ОСОБА_5 , ІНФОРМАЦІЯ_1 , по базі відео спостереження «Безпечне місце», а саме системи розпізнавання обличчя з метою встановлення маршруту пересування останнього по місту Києву, під час моніторингу за період з 07.03.2023 по 13.03.2023 фактів пересування не виявлено.»* [94] |
| Ухвала Голосіївського районного суду м. Києва від 19.09.2022 р. у справі № 752/8627/21 | *«Ухвалою Голосіївського районного суду м. Києва від 16.08.2022 явка ОСОБА_1 була забезпечена шляхом приводу через органи внутрішніх справ. Згідно даних рапорту ст.оперуповноваженого ВКП УП в метрополітені ГУНП у м. Києві капітана поліції Сухарєва О., в ході виконання приводу ним було встановлено, що за останнім відомим місце проживання у землянці, що* |

| ***Судове рішення*** | ***Згадка про використання технології*** |
|---|---|
| | *розташована у Голосіївському парку, ОСОБА_1 відсутній. Перевірка через комплексну систему відеоспостереження та розпізнавання облич м. Києва «Безпечне місто» та базу даних системи «Аркан» виявилася безрезультатною. Місце знаходження обвинуваченого ОСОБА_1 не встановлено.»* [95] |
| Ухвала Подільського районного суду м. Києва від 15.09.2022 р. у справі № 758/8070/22 | *«Також проведено моніторинг ОСОБА_5 по базі відео спостереження «Безпечне місце», а саме системи розпізнавання обличчя з метою встановлення маршруту пересування останнього по місту Києву, під час моніторингу за період з 01.01.2020 по 07.09.2022 фактів пересування не виявлено.»* [96] |
| Ухвала Дніпровського районного суду м. Києва від 31.08.2022 р. у справі № 755/4620/21 | *«Для вчинення злочинів, учасниками злочинної організації заздалегідь було розроблено план з розподілом функцій, згідно з яким необхідно було: підшукати та отримати в оренду нежитлові приміщення, розташовані на території міста Києва, які були б придатні для відкриття закладів,* |

| *Судове рішення* | *Згадка про використання технології* |
|---|---|
| | *пов`язаних з наданням доступу населенню до азартних ігор; підшукати сервер, розташований у недоступному місці для правоохоронних органів, з метою проведення азартних ігор в електронному (віртуальному) казино; придбати та встановити у гральних закладах комп`ютерну техніку, а також встановити програмне забезпечення для проведення азартних ігор; обладнати нежитлові приміщення місцями для проведення азартних ігор, що будуть складатись з комп`ютерної техніки (системних блоків, моніторів, комп`ютерних мишок, мережевого обладнання столів та стільців), робочих місць касирів (адміністраторів) гральних закладів, місцями для відпочинку гравців з метою надання доступу населенню до азартних ігор та відео спостереженням з метою контролю персоналу; організувати конспірацію закладів з надання доступу до азартних ігор, зокрема встановивши камери відео спостереження і розробивши схему входу до закладу, за системою розпізнавання в* |

| ***Судове рішення*** | ***Згадка про використання технології*** |
|---|---|
| | *обличчя постійних відвідувачів, забезпечити гральні заклади засобами мобільного зв`язку робочими телефонами для здійснення комунікації з організаторами; організувати та здійснювати забезпечення технічного обслуговування комп`ютерної техніки, доставки і переміщення ігрового обладнання; підшукати та прийняти на роботу без документального оформлення операторів-касирів гральних закладів, координувати та контролювати їх роботу по наданню гравцям послуг з проведення і надання доступу до азартних ігор; організувати та виконати інші заходи з метою забезпечення діяльності закладів, пов`язаних з наданням доступу населенню до азартних ігор.»* [97] |
| Ухвала Личаківського районного суду м. Львова від 11.08.2022 р. у справі № 463/4922/22 | *«Надати дозвіл слідчим слідчої групи […]»* [98] *«[…] на тимчасовий доступ до документів та відомостей, що знаходяться у володінні компанії « ІНФОРМАЦІЯ_1 », розташованої за адресою: АДРЕСА_1 ) з можливістю* |

| *Судове рішення* | *Згадка про використання технології* |
|---|---|
| | *ознайомитися з ними, зробити їх копії та вилучити, а саме до аккаунтів за посиланнями ІНФОРМАЦІЯ_10 та ІНФОРМАЦІЯ_3 з отриманням відомостей про: […]» «[…] пристрої, які використовуються, та інформацію про них, їх тип, операційну систему, веб-браузер, версії апаратного і програмного забезпечення; дії на пристрої; назви мобільного оператора або провайдера, а також про базові станції GSM (CDMA); контакти з адресної книги, журналу викликів або SMS; мови, часового поясу, абонентського номеру мобільного зв`язку, IP-адреси; дані про місцезнаходження (GPS), а саме: поточне місцезнаходження, місце проживання; спосіб використання камери, дату, час і місце, де був зроблений знімок; дані, отримані в результаті технології розпізнавання обличь, обліку підключень пристрою та інформації про найближчі точки доступу Wi-Fi; […]»* [98] |

| ***Судове рішення*** | ***Згадка про використання технології*** |
|---|---|
| Ухвала Дубенського міськрайонного суду Рівненської області від у 26.11.2021 р. справі № 559/2971/21 | *«Під час досудового розслідування, відповідно до «Домовленості між МВС Грузії та МВС України про співробітництво в сфері боротьби з злочинністю», аташе МВС Грузії в Україні проінформувало, що інформація відносно громадян ОСОБА_5 ( ОСОБА_6 ), ОСОБА_7 , ОСОБА_8 ( ОСОБА_9 ) у базі МВС Грузії відсутня. Відповідно до «системи розпізнавання обличчя особи» встановлено, що на представленій СВ Дубенського ВП ГУ НП в Рівненській області фотографії є громадяни Грузії:»* [99] |
| Ухвала Київського апеляційного суду від 29.06.2021 р. у справі № 757/3027/21-к | *«Твердження адвоката про те, що особа на відео це не ОСОБА_7 , те, що підозрювана у період з липня по листопад 2014 року перебувала на території Російської Федерації, те, що відносно ОСОБА_7 Службою безпеки України в 2015, 2016 роках здійснювалися оперативно-розшукові заходи з метою перевірки участі у діяльності у незаконних збройних формувань, колегія суддів визнає* |

| ***Судове рішення*** | ***Згадка про використання технології*** |
|---|---|
| | *передчасними, оскільки вони стосуються доведеності вини особи, що не є предметом розгляду на даному етапі провадження, як і доводи апеляційної скарги з приводу того, що ресурсом « ІНФОРМАЦІЯ_3 » встановлено, що особа зафіксована на відео (жінка з білим волоссям та багнетом в руках) це ОСОБА_10 , а за допомогою програм порівняння/розпізнавання облич, що використовують штучні нейронні мережі, встановлено відсутність схожості між зображеннями жінки на відео та ОСОБА_7 , проте підлягають перевірці на досудовому розслідуванні.»* [100] |
| Ухвала Шевченківського районного суду м. Києва від 11.07.2020 р. у справі № 761/20554/20 | *«У ході відпрацювання прилеглої території працівниками Департаменту карного розшуку було виявлено та опрацьовано зовнішні камери відеоспостереження на яких фіксується особа, яка може бути причетна до скоєння даного злочину. В подальшому відпрацьовано можливий маршрут руху злочинця після вчинення злочину.* |

| ***Судове рішення*** | ***Згадка про використання технології*** |
|---|---|
| | *За допомогою Єдиного державного демографічного реєстру, а саме розпізнавання обличчя «Face-id», встановлено особу та її повні анкетні дані, а саме: ОСОБА_7 , ІНФОРМАЦІЯ_1 , зареєстрований за адресою: АДРЕСА_2 , проживає за адресою: АДРЕСА_3 , користується мобільним телефоном НОМЕР_2 , у власному користуванні має автомобіль «SUBARU FORESTER» сірого кольору, д.н.з. НОМЕР_3 . Одружений з громадянкою ОСОБА_8 , ІНФОРМАЦІЯ_2 , проживає за адресою: АДРЕСА_3 , а також періодично мешкає за адресою: АДРЕСА_4 , користується мобільним телефоном НОМЕР_4.*<br><br>*Під час вивчення сторінок соціальних мереж ОСОБА_7 , а також його побутового життя, встановлено тісний зв`язок з потерпілим ОСОБА_6 .»* [101] |
| Постанова Шостого апеляційного адміністративного суду від 28.02.2023 р. № 358/857/22 | *«Щодо надання до суду доказу, а саме відео з камер відеоспостереження Безпечне місто, на який посилається* |

| *Судове рішення* | *Згадка про використання технології* |
|---|---|
| | *скаржник, то даний доказ не міг бути зазначений відповідачем у постанові, оскільки створений такий відеозапис не ним, а іншим органом.*<br><br>*Так, у м. Києві в рамках «Безпечне місто» запущено новий аналітичний модуль відеоспостереження, що прискорить пошук правопорушників.*<br><br>*Унікальний модуль дозволяє шукати правопорушників не лише завдяки спеціалізованим камерам розпізнавання обличчя. Модуль фіксує зображення з будь-якої камери, що встановлена в рамках мережі та порівнює їх із базою правопорушників, що була створена правоохоронними органами. Якщо система виявляє подібність, оператор одразу отримує тривожний сигнал. Таким чином, система прискорює розшук злочинців та правопорушників.*<br><br>*У м. Києві камери розташовані у місцях великого скупчення людей: у дошкільних навчальних закладах,* |

| *Судове рішення* | *Згадка про використання технології* |
|---|---|
| | *школах, метрополітені, вокзалах, лікарнях тощо*.<br><br>*Модуль розпізнавання - апаратно-програмний. Він є частиною інтегрованого комплексу, центра обробки даних (ЦОД), що знаходиться у Києві. Апаратна частина - розробка компанії Hikvision. Програмна частина - підрозділу компанії Hikvision. Розробники аналітичного модуля орієнтувались саме на інтелектуальну систему розпізнавання обличь «Sky Net».*<br><br>*КП «Інформатика» та Київська міська державна адміністрація не надають відеоматеріали, отримані з камер міської системи відеоспостереження. Відповідно до пункту 8.1 «Положення про комплексну систему відеоспостереження міста Києва», доступ до інформації у системі надано посадовим особам Міністерства внутрішніх справ України, центральному органу управління Національної поліції України, Головного управління Національної поліції в м. Києві та його* |

| ***Судове рішення*** | ***Згадка про використання технології*** |
|---|---|
| | *територіальними підрозділам. Таким чином, відео з місця події можна отримати тільки від вказаних структур, написавши запит до них.*<br><br>*Отже, відповідач має доступ до зазначеної системи і в рамках даної справи надав відео як доказ, який, на його думку, свідчить про порушення позивачем ПДР.»* [102] |
| Постанова Третього апеляційного адміністративного суду від 12.01.2021 р. у справі № 280/4979/20 | *«Відповідно до п.54 Порядку № 784 ідентифікація та верифікація іноземців та осіб без громадянства, затриманих за незаконне перебування або порушення правил перебування в Україні, які мають документи, що посвідчують особу, передбачає, зокрема, здійснення таких заходів: 1) проведення перевірки тотожності обличчя особи та фотокартки, що міститься в паспортному документі; 2) проведення перевірки інформації про особу засобами Реєстру; 3) проведення у разі відсутності інформації про особу в Реєстрі перевірки згідно з картотеками та базами даних розпорядника* |

| ***Судове рішення*** | ***Згадка про використання технології*** |
|---|---|
| | *Реєстру, його територіальних органів/територіальних підрозділів; 4) сканування паспортного документа; 5) фотографування особи; 6) отримання відцифрованих відбитків пальців рук особи.*<br><br>*З метою здійснення ідентифікації особи може використовуватися програмно-апаратний комплекс розпізнавання обличчя, який ідентифікує особу шляхом співставлення отриманого відцифрованого зображення особи з відцифрованим образом обличчя особи, що зберігається Реєстрі (п.56 Порядку № 784).»* [103] |