Міністерство освіти і науки України
Національний університет «Києво-Могилянська академія»
Факультет правничих наук
Кафедра загальнотеоретичного правознавства та публічного права

Магістерська робота

освітній ступінь – магістр

на тему: «ТЕХНОЛОГІЇ РОЗПІЗНАВАННЯ ОБЛИЧ І ПРАВО НА ПРИВАТНІСТЬ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ» / «FACE RECOGNITION TECHNOLOGIES AND THE RIGHT TO PRIVACY AND PROTECTION OF PERSONAL DATA»

Виконала: студентка 2 року навчання
Спеціальності 081 Право
Максимович Тетяна Миколаївна

Керівник Мелешевич А.А., професор, Ph.D.

Рецензент_____
(прізвище та ініціали)

Магістерська робота захищена
з оцінкою «_____»

Секретар ЕК_____
«___»_____2021 р.

Київ – 2021

Декларація

академічної доброчесності

студента/ студентки НаУКМА

Я Максимович Тетяна Миколаївна,
студент(ка) 2 року навчання факультету правничих наук,
спеціальність 081 Право,
адреса електронної пошти t.maksymovych@ukma.edu.ua

- підтверджую, що написана мною кваліфікаційна/магістерська робота на тему «Технології розпізнавання облич і право на приватність та захист персональних даних» відповідає вимогам академічної доброчесності та не містить порушень, передбачених пунктами 3.1.1-3.1.6 Положення про академічну доброчесність здобувачів НаУКМА від 07.03.2018 року, зі змістом якого ознайомлений/ ознайомлена;
- підтверджую, що надана мною електронна версія роботи є остаточною і готовою до перевірки;
- згоден/ згодна на перевірку моєї роботи на відповідність критеріям академічної доброчесності, у будь-який спосіб, у тому числі порівняння змісту роботи та формування звіту подібності за допомогою електронної системи Unicheck.
- даю згоду на архівування моєї роботи в репозитаріях та базах даних університету для порівняння цієї та майбутніх робіт.

12.05.2021	[signature]	Максимович Т.М.
Дата	*Підпис*	*Прізвище, ініціали*

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ……...4

ВСТУП……5

РОЗДІЛ 1. ТЕХНОЛОГІЇ РОЗПІЗНАВАННЯ ОБЛИЧ ЯК ІНСТРУМЕНТ ВСТАНОВЛЕННЯ БЕЗПЕКИ В СУСПІЛЬСТВІ……...8

1.1. Поняття технологій розпізнавання облич та мета їх застосування……8

1.2. Достатність, відповідність та доцільність як основні критерії застосування технологій розпізнавання облич……...13

1.3. Необхідні гарантії при застосуванні технологій розпізнавання облич…...18

РОЗДІЛ 2. ОБРОБКА ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ПРИ ВИКОРИСТАННІ ТЕХНОЛОГІЙ РОЗПІЗНАВАННЯ ОБЛИЧ……27

2.1. Загальні принципи обробки персональних даних……27

2.2. Українське законодавство у сфері захисту персональних даних……30

2.3. Європейське регулювання технологій розпізнавання облич та питань захисту персональних даних ……32

2.4. Досвід США в регулюванні технологій розпізнавання облич та питаннях захисту персональних даних……42

РОЗДІЛ 3. ОБСЯГ ПРАВА НА ПРИВАТНІСТЬ ТА СПІВВІДНОШЕННЯ ІЗ ПРАВОМ НА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ……47

3.1. Обсяг права на приватність……47

3.2. Зв’язок між правом на приватність та правом на захист персональних даних……..……49

3.3. Межі втручання держави у право на приватність……51

РОЗДІЛ 4. РОЛЬ ТЕХНОЛОГІЙ РОЗПІЗНАВАННЯ ОБЛИЧ В ПЕРІОД COVID-19……...59

4.1. Запровадження заходів відстеження та спостереження для виявлення та карантину осіб, заражених COVID-19……59

4.2. Особливості та тенденції регулювання технологій розпізнавання облич та інших технологій відстеження в окремих державах в період встановлення карантинних обмежень……..62
ВИСНОВКИ……...……...75
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ…….78

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ТРО	Технологія розпізнавання облич
ПД	Персональні дані
ЗРПЗД, Регламент	Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)
ЄСС	Європейський суд справедливості

ВСТУП

На сучасному етапі розвитку суспільства спостерігаються постійно зростаючі можливості технологій спостереження, одними із яких є технології розпізнавання облич (ТРО).

Актуальність теми даного дослідження полягає в тому, що системи розпізнавання обличь все частіше розглядаються органами влади як способи вирішення проблем злочинності та запобігання порушенням громадського порядку, а в період пандемії коронавірусу також і як інструмент уповільнення поширення вірусу. Безумовно, ТРО можуть сприяти встановленню безпеки та навіть, як спостерігаємо з останніх подій, забезпеченню прав громадян на охорону здоров'я. Та в той же час існує негативний ризик втручання у приватність кожної особи, як в романі Дж. Оруелла «1984», котрий і відіграв основну роль при виборі теми дослідження для кваліфікаційної роботи. Дж. Оруелл змальовує світ, у якому за громадянами повсюди слідкують телевізори. Хоча роман визначається як фантастична розповідь, світ описаний в ньому є дуже близьким до сучасних реалії. На сьогоднішній день практично кожен крок може відслідковуватись системами відеоспостереження. Тільки в Києві у 2019 році для прискорення розшуку злочинців та правопорушників було встановлено понад 200 оглядових камер із новим аналітичним модулем розпізнавання обличь [1]. Тому у зв'язку з безпрецедентною швидкістю розвитку технологій, існує побоювання створення суспільства тотального спостереження, як у романі Дж. Оруелла.

Вибір теми дослідження обумовлюється рядом невирішених питань, які постають у зв'язку із втручанням у право на приватність та право на захист ПД, в умовах впровадження та використання ТРО. Стрімкий розвиток ТРО як в світі, так і в Україні свідчить про гостру потребу встановлення правил застосування таких технологій та порядку використання результатів, отриманих завдяки їх функціонуванню.

Перегляд українського законодавства у сфері регулювання захисту ПД, новітніх технологій є необхідним кроком на даному етапі для того, щоб мінімізувати негативний вплив ТРО на права індивідів. Питання впровадження та застосування ТРО по різному вирішується в іноземних державах. Протягом кількох останніх років дискусія щодо цього питання є актуальною, адже з'являються нові виклики, які потребують перегляду прийнятих рішень щодо функціонування ТРО. Український законодавець досі не визначив, чи забороняти ТРО чи встановити правила їх застосування та поступово впроваджувати технологію.

Метою дослідження є визначення впливу ТРО на право на приватність та на право на захист ПД, здійснення аналізу підстав обмеження права на приватність та допустимих меж втручання у право на захист ПД у зв'язку із впровадженням ТРО з міркувань забезпечення безпеки громадськості.

Для досягнення вказаної мети в дослідженні поставлено такі *завдання*:

- визначити сутність ТРО та мету їх застосування;
- встановити роль ТРО для забезпечення права на безпеку та інших суспільних благ;
- проаналізувати акти, які регулюють ТРО;
- визначити співвідношення права на приватність та права на захист ПД;
- з'ясувати правові межі права на приватність;
- визначити критерії балансу між приватними та публічними інтересами;
- з'ясувати правила стосовно обробки ПД у міжнародних, регіональних та національних актах;
- виявити гарантії захисту ПД в законодавстві України та інших державах;
- визначити перспективи впровадження в Україні провідних положень щодо регулюванню ПД;
- проаналізувати процес зближення українського законодавства у сфері захисту ПД із провідними світовими практиками;
- з'ясувати суть даних, які обробляються при використанні ТРО.

Об'єктом дослідження є суспільні відносини, які пов'язані із реалізацією та захистом права на приватність, гарантіями захисту при обробці ПД зв'язку із впровадження ТРО.

Предметом дослідження є правове регулювання механізмів та засобів захисту ПД та права на приватність в умовах застосування ТРО.

Методи дослідження. При дослідженні механізмів організаційно-правового забезпечення захисту права на приватність та захисту ПД було застосовано системно-структурний метод. Застосування формально-логічного методу дозволило провести аналіз чинних правових норм. Завдяки аналітичному та статистичному методу було досліджено реальну ситуацію та правові наслідки впровадження ТРО. Застосування герменевтичного методу допомогло при розумінні основних термінів (право на приватність, ПД, ТРО). В роботі було застосовано також такі загальнонаукові методи дослідження, як аксіологічний та антропологічний, адже тема безпосередньо пов'язана із правами людини.

Під час написання цієї роботи було використано таку *нормативну базу*: міжнародно-правові акти, рішення іноземних судів, національне законодавство, наукова праці.

Теоретична база. В науковій доктрині України питання застосування ТРО, захист ПД та право на приватність при використанні ТРО не досліджувалась комплексно. Тому в роботі в основному використано дослідження європейських та американських вчених, зокрема: Рашіди Річардсон, Алессандро Аквісті, Мішель Фінк, Бієга Асія, Кейт Кроуфорд, Маріко Хіросе. При цьому праці українських науковців, зокрема, Погребняка С.П., Дахової І.І., Размєтаєвої Ю.С. були основою для аналізу меж втручання держави у право на приватність.

Наукове значення даної роботи полягає в тому, що в ній з нової точки зору розглядається класичне для прав людини співвідношення права на приватність, тісно з яким пов'язано право на захист ПД, та права на безпеку.

Практичне значення полягає в тому, що надані в роботі висновки можуть бути застосовані органами влади для забезпечення гарантій індивідів при використанні ТРО.

РОЗДІЛ 1. ТЕХНОЛОГІЇ РОЗПІЗНАВАННЯ ОБЛИЧ ЯК ІНСТРУМЕНТ ВСТАНОВЛЕННЯ БЕЗПЕКИ В СУСПІЛЬСТВІ

1.1. Поняття технологій розпізнавання облич та мета їх застосування

Невпинний технічний розвиток вносить корективи у всі сфери життя. Нові технології своїми прогресивними функціями та можливостями цілком виправдано викликають схвалення суспільства. Але позитивний на перший погляд ефект впровадження та застосування нових технологій, може приховувати ризики, які у випадку їх не виявлення та/або нехтування можуть спричинити втручання у права осіб та їх порушення. Однією із таких популярних і в той же час суперечливих технологій є технологія розпізнавання облич.

Найперше вважаю за необхідне, визначити суть ТРО. Кембриджський словник визначає розпізнавання облич, як «технологію, яка дозволяє комп'ютеру розпізнавати цифрове зображення чийогось обличчя»[1] [2]. Тобто штучний інтелект аналізує особливості зовнішності згідно наявних зображень, завдяки чому відбувається ідентифікація особи. Особливість ТРО визначають два процеси: «запис до певної бази осіб та знаходження співпадінь» [3, с. 95]. Основна задача для здійснення ідентифікації – отримати зображення і безумовно, що чим кращою буде його якість, тим точнішою буде ідентифікація. Ідентифікація за зображенням є особливістю ТРО, адже дає змогу не залучати особу безпосередньо в процес, а навпаки здійснювати ідентифікацію на відстані.

Як пише у своєму дослідження Еліас Райта, першочергова мета, яка покладалась на ТРО, – «допомога військовим виявити на відстані конкретних осіб противника» [4, с. 617]. На даному етапі сфера застосування ТРО розширились, основні завдання, які покладають на ці технології охоплюють забезпечення громадського порядку, становлення національної безпеки, запобігання злочинності. «ТРО використовуються в портах в'їзду та в системах

[1] Тут і далі, якщо не зазначено інше, переклад авторки.

громадського транспорту. У Китаї такі технології інтегровані в автобусні та залізничні транзитні пункти для сканування облич пасажирів замість фізичних квитків або цифрових кодів квитків, подібне використання пілотно застосовується в Казахстані» [5, с. 4]. «Сполучені Штати та держави Європейського Союзу проводять різний ступінь моніторингу мережі, масового аналізу даних, збору та каталогізації в режимі реального часу з метою розвідки та безпеки» [6, с. 5]. Постійний процес удосконалення ТРО «забезпечує потужний аналітичний інструмент для прогнозування потенційного насильства та потенційно може допомогти у запобіганні конфліктам» [7, с.3]. Що в свою чергу означає безпрецедентну можливість здійснювати автоматизований аналіз поведінки особи завдяки якісним процесам об'єднання різних технологій. Є можливість реалізувати два процеси, які можуть бути взаємопов'язані: моніторинг та поведінковий аналіз.

Для держави – це спосіб вирішувати питання встановлення безпеки, які періодично потребують перегляду у зв'язку із викликами національній безпеці та громадському порядку. Терористичний акт 9 вересня 2001 р. в Сполучених Штатах Америки гостро поставив питання безпеки. «Агентство національної безпеки США почало збирати та зберігати телефонні дзвінки, електронні листи та здійснювати інші цифрові дії щодо громадян США без попередніх гарантій після прийняття «Патріотичного акту» 2001 р.» [5, с.10].

Теракт в США привернув увагу до обговорення посилення заходів безпеки та легітимності таких заходів і в інших державах. Дебати щодо співвідношення права на приватність та права на безпеку постали з новою силою. Сенатор Рон Вайден, аналізуючи обидві сторони медалі, підкреслював, що найперше потрібно розуміти те, що це не взаємовиключні явища, тому вони можуть і повинні існувати паралельно [8, с. 331].

Все ж таки перевага була надана встановленню безпеки та захисту від терористичних актів. Декількома роками пізніше після терористичного акту, Агентством національної безпеки США почала застосовуватись система Інтернет-спостереження за даними під назвою PRISM, про що писало видання

«The Washington Post» [9]. У статті зазначеного видання йшла мова про те, що система PRISM почала застосовуватись із 2007 р., коли до програми приєднався Microsoft, і окрім даних про онлайн активність осіб, використовувалась для здійснення спостережень у режимі реального часу [9]. Постійний моніторинг дав можливість Агентству національної безпеки США сформувати базу фотографій користувачів. Видання «The New York Times» писало про те, що АНБ США перехоплює «мільйони зображень на день» - у тому числі близько 55 000 «якісних зображення для розпізнавання облич» [10]. Що в свою чергу сприяло успіху в роботі АНБ США над створенням програмного забезпечення для розпізнавання обличчя.

Викриття, зроблене Едвардом Сноуденом (американський програміст, колишній працівник АНБ США, який передав документи про систему PRISM виданням «The Guardian» і «The Washington Post», а також інформацію про стеження АНБ США за інформаційними системами багатьох країн світу [11]), викликало шквал обговорень. Адміністрація тодішнього президента США Барака Обами наголошувала на необхідності таких заходів та підкреслювали, що кожен американський президент підтримав б такі заходи задля становлення безпеки [12].

З такою позицією важко погодитись, адже населення взагалі не підозрювало про заходи впровадженні державою. Ідентифікувати того, хто спостерігає, є важливим етапом для того, щоб потенційні суб’єкти даних мали змогу реагувати на таке спостереження, висловлювати свої думки щодо таких дій державних органів. Правозахисники навіть ведуть мову про ознаки злочинності в запровадженні державою заходів спостереження та ідентифікації без повідомлення про це населення. Лаура Фінлей та Луїджі Еспосіто стверджують, що широке та загальне спостереження за громадянами США, які не підозрюються у вчиненні будь-якого кримінального правопорушення, слід розглядати як злочинну діяльність, яка відбувається внаслідок змови державних та корпоративних структур [13].

При цьому обізнаність населення про застосування камер спостереження та камер з модулем ідентифікації осіб не виключає порушення прав громадян. Серйозним посяганням на громадянські свободи видання «Старший брат спостерігає» («Big Brother Watch») визначає використання ТРО у Великобританії службою столичної поліції Лондона, наводиться статистика, що з 13 000 людей, які піддавались спостереженню заарештували лише одну людину. Також виявилося, що схема спостереження не змогла ідентифікувати правильного підозрюваного сім із восьми разів [14]. Тому досягнення точних результатів ідентифікації є першочерговим питанням, яке повинно бути опрацьованим та вирішеним, перш ніж вдаватись до застосування ТРО.

Технологічний прогрес дає можливість здійснювати аналіз все більшого обсягу даних. Алессандро Аквісті, дослідник технологій розпізнавання обличчя з Університету Карнегі-Меллона виданню «The New York Times» зазначав, що «розпізнавання обличчя може бути дуже інвазивним. Поки є певні технічні обмеження, але обчислювальна потужність продовжує зростати, бази даних постійно розширюються, а алгоритми вдосконалюються» [10].

Ряд важливих елементів, які постійно вдосконалюються, можуть допомогти досягнути точних результатів. По-перше, Кевін В. Бовер зазначає про те, що система може розпізнавати лише осіб, зображення яких були занесені до бази даних [15, с. 11]. Цей елемент звертає до етапу формування бази даних зображень. У випадку із ТРО діє правило, що чим більше зображень у базі даних, тим легше віднайти необхідне зображення, щоб з’єднати його із отриманим за допомогою ТРО. Ще один момент полягає в тому, що система повинна мати можливість отримувати зображення обличчя достатньої якості [15, с. 11]. Недостатня освітленість фотографії або інші негативні характеристики щодо якості створюють складнощі для функціонування ТРО.

Неочевидним на перший погляд моментом, котрий повинен бути врахованим є «поріг чутливості» [15, с. 11]. Кевін В. Бовер веде мову про те, що занадто низький поріг призведе до занадто великої кількості помилкових позитивних результатів, а занадто високий поріг призведе до занадто великої

кількості помилкових негативів - терорист не визнається через відмінності у зовнішності між галереєю та зображеннями терориста [15, с. 11].

Із зазначеного, приходжу до висновку, що розпізнавання обличчя не завжди здатне точно з'єднати дані із камер із наявними у базі даних зображеннями. Помилки зазвичай трапляються через погані зображення або брак інформації в базі даних або ж недостатню якість зображення і ведуть до негативного результату та ускладнюють точне співставлення. Це все призводить до помилки в ідентифікації та ставить питання ефективності. Відомості чи сукупність відомостей зберігаються в базі даних, а практичний результат не завжди досягається і тому визначати ТРО стовідсотково точною технологію поки що рано. Та все ж постійний розвиток дає можливість мінімізувати можливі недоліки систем та робить аналіз більш точним.

Науковці Національного інституту стандартів та технологій США на постійній основі проводять дослідження досягнень точності розпізнавання облич. У 2020-2021 роках дослідження були зосередженні в основному на випробуванні застосування алгоритмів при використанні захисних масок. Тому наведу показники за попередні роки, а про ефективність системи ТРО для розпізнавання облич у захисних масках буде зазначено в останньому розділі цієї роботи. Отже, у 2018 р. дослідники зазначали, що «за останні п’ять років (2013-2018) було досягнуто значного збільшення точності. Принаймні 28 алгоритмів розробників перевершують найточніший алгоритм з кінця 2013 року, та все ж залишається широкий спектр можливостей для удосконалення» [16, с.2]. Дослідники бачать значні досягнення у зв’язку із істотним покращенням якості фотографій і зазначають у своєму аналізі, що завдяки якісним портретним фотографіям найточніші алгоритми можуть знайти відповідні записи (попередньо зібрані фотографії) у галереях із коефіцієнтом помилок нижче 0,2% [16, с.2]. Тут варто зробити примітку, що такого низького коефіцієнту помилок можна досягти шляхом застосування найбільш досконалих та точних алгоритмів. Більшість систем досягають нижчого рівня точності та ефективності.

На законодавчому рівні точність даних стає все поширенішою вимогою, яка ставитись до обробки ПД загалом та в частині обробки ПД, отриманих завдяки ТРО зокрема. В українському законодавстві щодо захисту ПД закріплено: «Персональні дані мають бути точними, достовірними та оновлюватися в міру потреби, визначеної метою їх обробки» (ч.2 ст. 6 Закону України «Про захист персональних даних») [17].

«Точність» закріплено як принцип в Загальному регламенті про захист даних. Згідно п.1d ст.5 Загального регламенту про захист даних: «Персональні дані необхідно: вважати точними і, за необхідності, оновлювати; необхідно вживати усіх відповідних заходів для того, щоб забезпечити, що неточні персональні дані, зважаючи на цілі їхнього опрацювання, було стерто чи виправлено без затримки («точність»)» [18].

Точність зображень, або, як на мою думку більш вдалим по відношенню до фото- та/або відеозображень буде термін релевантність зображень, сприяють уникненню помилок при ідентифікації. Відбувається природний процес старіння особи, тому навіть системи з високою роздільною здатністю, засновані на відповідному алгоритмі для досягнення позитивного результату повинні застосовувати найновіші зображення особи. Таким чином, бази даних із зображенням повинні піддаватись періодичному оновленню, задля виконання законодавчих вимог щодо забезпечення точності даних та з метою уникнення помилок в ідентифікації особи.

1.2. Достатність, відповідність та доцільність як основні критерії застосування технологій розпізнавання облич

Визначення мети застосування ТРО є центральною ланкою для забезпечення та дотримання законодавчих вимог. Адже визначення мети означає (1) вказівку на сферу застосування ТРО, (2) зазначення контролера, який відповідає за те, в який спосіб та ким здійснюватиметься обробка ПД; (3) розвиток більш детальних вимог до застосування ТРО та обробки ПД, отриманих

з їх допомогою, таких як достатність, відповідність та необхідність, які в ЗРПЗД визначені як «принцип мінімізації даних» [18]. Даний принцип насамперед закладає практику обмеження збору та збереження тих ПД, що мають безпосереднє значення та необхідні для досягнення визначеної мети; тобто організації повинні збирати та зберігати наскільки це можливо щонайменшу кількість даних [19]. Інформація, що не має значення для конкретного аналізу, не повинна взагалі збиратись. Контролер ПД зобов'язаний оцінити рівень очікувань приватності фізичної особи в момент збору її персональних даних за допомогою ТРО. Це можна розуміти, як проведення оцінки законних інтересів, відповідно до якої розглядатиметься не тільки наскільки необхідним є використання розпізнавання обличчя для досягнення поставленої мети, а й те, що, можливо зробити, щоб мінімізувати втручання ТРО в приватність особи.

Однак ТРО є системою штучного інтелекту, основою належного функціонування якої є саме велика кількість даних. Звідси й основна мета системи – збір та використання якомога більшої кількості даних, без додаткового проектування ситуації, коли можна досягти тих самих цілей із меншою кількістю даних. Для мінімізації кількості зображень в базах даних на мою думку найперше необхідним є впровадження та застосування періодичного «перегляду» відповідних баз даних на предмет відповідності зображень, які ними використовуються.

Визначення відповідності даних в ЗРПЗД не надано, в українському законодавстві взагалі конкретно про принцип мінімізації даних не згадується. Науковці ж визначають відповідність як вимогу обробляти лише релевантні дані [20, с.26]. Мішель Фінк та її колега Бієга Асія наводять до прикладу ситуацію, коли здійснюючи покупку в через мережу інтернет, сайт вимагає вказати повну дату народження для того, щоб надати персоналізовані рекомендації щодо покупок. Якщо завдяки певним астрологічним знанням можна визначити вподобання, то так, такий збір ПД може мати місце, але в більшості випадків вказівка дати народження має значення для іншої мети, а ніж персоналізована підбірка [20, с.26]. Відповідно вимога відповідності даних порушується.

При застосуванні ТРО, випадки використання отриманих результатів за межами визначеної мети також можуть мати місце. Взагалі для особи знати, що за нею спостерігає камера, не є тотожним розуміти мету такого спостереження. Тобто пересічний громадянин, який потенційно піддається спостереженню, не може дати собі відповіді на питання чому, з якою метою і ким встановлена камера спостереження, буквально кажучи питання «хто спостерігає за особою» залишається відкритим. Коли особа перебуває на вокзалі, в аеропорту чи в будь-якому іншому громадському місці, можна зустріти патрульного або іншого представника органів державної влади чи місцевого самоврядування. Фізична ідентифікація дає змогу в більшості випадків припустити, що його обов'язок попередження порушень громадського порядку та забезпечення безпеки для осіб, які на даний момент знаходяться в полі його зору, та зрозуміти, представником якого органу є посадова особа. Відповідно особа може конкретно ідентифікувати, що за певних обставин її дані будуть зібрані та оброблені конкретним органом влади. Камера, яка встановлена на тому ж залізничному вокзалі чи в аеропорту не дає можливості ідентифікувати, хто спостерігає за особою і яка мета закладена в таке спостереження. Стандартом для контролерів даних повинно бути чітке та беззастережне визначення мети використання ТРО та збору ПД, для того, щоб уникати надмірності даних та не призводити до нагромадження бази даних.

Вимога відповідності тісно переплітається із вимогою достатності. Та все ж між обома поняттями є нюанс. Якщо критерій відповідності має суто обмежуючий вплив на збір даних, за певних обставин достатність може вимагати обробки більшої кількості даних [20, с. 27]. Отримані (зібрані) дані повинні забезпечити формування цілісної інформації для розуміння суті обставини та встановлення та ідентифікації осіб у конкретних обставинах. Вимога достатності виключає фрагментарність даних, адже це перешкоджатиме безпомилковому встановленню та ідентифікації осіб. При зборі ПД завдяки ТРО вимога достатності тісно пов'язана із якістю отриманих зображень. Одне чітке зображення може замінити всі неякісні, цим самим забезпечити позитивний

результат ідентифікації. Тому при використанні ТРО важливе значення відіграє застосування найновіших технічних можливостей.

Останньою вимогою принципу мінімізації даних є необхідність. На онлайн-платформі організації Управління комісара із питань інформації (Information Commisioners Office) зазначено, що вимога необхідності передбачає, що контролер не може зберігати більше даних, ніж потрібно для визначеної мети [21]. Не відповідатиме також вимозі необхідності збір ПД, якщо є припущення, що ПД можуть бути потрібними в майбутньому, за виключенням випадків, коли для цього є належне обґрунтування [21]. Європейський суд справедливості розглядав справу за заявою організації «Діджитал Райц Ірландія Лтд» (Digital Rights Ireland Ltd), справа C-293/12 [22]. З метою запобігання, виявлення, розслідування, переслідування злочинів та забезпечення безпеки держави, від постачальників послуг телефонного зв'язку вимагалось зберігати дані про трафік та місцезнаходження користувачів для відстеження та ідентифікації джерел зв'язку, тривалості та типу зв'язку, обладнання зв'язку користувачів, включаючи ім'я та адресу абонента, номер телефону протягом визначеного законодавством періоду [22].

Суд у висновку зазначив: «слід визнати, що боротьба з серйозною злочинністю, зокрема проти організованої злочинності та тероризму, дійсно є надзвичайно важливою для забезпечення громадської безпеки та її ефективність може значною мірою залежати від використання сучасних методик розслідування. Однак така мета загального інтересу, якою б фундаментальною вона не була, сама по собі не виправдовує такого заходу, як встановлений Директивою 2006/24 (прим. збирання даних про користувачів телекомунікаційних послуг), який вважається необхідним для цілей цієї боротьби» [22].

Мета збору даних, визначена державним органами Ірландії, була дуже загальною. В той же час державні органи отримали доступ до збереження численної кількості даних, а користувачі стали постійними суб'єктами спостереження.

Необхідним видається впровадження процесів підзвітності, завдяки яким буде продемонстровано, що збираються та зберігаються тільки необхідні дані. Вміти ідентифікувати та обробляти мінімальну кількість даних є необхідним стандартом для контролерів.

Зберігання ПД, які не мають відношення до мети такого зберігання або втратили свою цінність для досягнення мети, є предметом серйозних штрафів. Державний орган Берліну із захисту даних оголосив 5 листопада 2019 року, що оштрафував компанію Deutsche Wohnen SE на 14,5 млн. євро за порушення ЗРПЗД після розслідування на місці [23]. Зазначалось, що компанія Deutsche Wohnen SE зберігала персональні дані орендарів, такі як відомості про заробітну плату, витяги з контрактів, дані про податки, соціальне страхування та медичне страхування та банківські виписки, в системі архівування, з якої неможливо було видалити такі дані, і що персональні дані орендарів зберігалися без перевірки чи дозволено та чи взагалі потрібно їх зберігати [23]. Видання «Compliance Week» повідомляє, що у лютому цього року дане рішення було скасовано в апеляції, зараз триває розгляд у вищій інстанції [24]. Незалежно від фінального результату, такі дії органів державної влади із захисту персональних даних свідчать про необхідність захисту від безпідставного зберігання та обробки ПД. В Україні також існує гостра потреба застосування вимог достатності, відповідності та доцільності при обробці ПД, особливо тих, які отримані без явної згоди суб’єктів даних, зокрема завдяки ТРО. Є потреба в конструктивному діалозі між органами державної влади, які в основному виступають контролерами та/або розпорядниками ПД, та спільнотою працівників сфери інформаційних технологій для розробки та впровадження алгоритмів, котрі можуть визначати, які дані необхідні, які фотозображення можуть бути використані для ідентифікації та забезпечення встановленої мети, а якими можна знехтувати та не нагромаджувати бази даних.

1.3. Необхідні гарантії при застосуванні технологій розпізнавання облич

У січні минулого року Європейська комісія розглядала заходи щодо тимчасової заборони використання ТРО на території Європейського Союзу, що застосовується як державними, так і приватними суб'єктами [25]. Тоді обговорювався проект «Біла книга про штучний інтелект – європейський підхід до високої якості та довіри» [25].

Зазначений проект визначив матеріальні та нематеріальні ризики застосування штучного інтелекту. У контексті цієї роботи значення мають саме нематеріальні ризики, до яких Європейська комісія віднесла втрату приватного життя, обмеження права на свободу вираження поглядів, гідність людини, дискримінації. У проекті зазначено, що для мінімізації та уникнення ризиків, повинна бути розроблена та імплементована нормативна база [26, с.10-11]. Регулювання штучного інтелекту, закріплення гарантій від безпідставного застосування штучного інтелекту загалом та ТРО зокрема, зможе мінімізувати ризики потенційної шкоди.

Кейт Кравфорд у статті із промовистою назвою «Припиніть використання технології розпізнавання обличчя, поки це не буде регульовано» зазначає: «Уряди не готові запобігти заподіяння шкоди від ТРО. (…) Системне законодавство повинно гарантувати обмеження щодо використання ТРО, а також прозорість, належну процедуру та інші основні права. Поки ці гарантії не будуть застосовані, потрібен мораторій на використання ТРО у громадських місцях» [27].

Частина науковців, органів державної влади виступають за повну заборону застосування ТРО [28]. Зупинити постійний технологічний розвиток не можливо, тому повна заборона ТРО на мою думку не видається реальною. Затвердження та впровадження належних гарантій для суб’єктів даних може сприяти мінімізації ризиків, які асоціюються із використанням ТРО.

Для мене, як для суб'єкта даних, важливим є чітке повідомлення про застосування ТРО на відповідній території та вказівка про мету такого застосування . Це підвищує обізнаність громадськості та дозволяє передбачити власний рівень приватності в громадських місцях.

В науці розроблена доктрина «розумних очікувань приватності», яка вперше була застосована у справі «Катз проти США» 1967 р. [29]. Маріко Хіросе зазначає про два фактори, які мають значення при посиланні на очікування приватності: «(…) з одного боку, очікування приватності є необґрунтованим, якщо інформація, яка підлягає захисту, піддається впливу громадськості або якщо вона вже була передана третім особам, з іншого боку, очікування конфіденційності є розумним, якщо воно відповідає соціальним нормам та законним намірам» [30, с. 1603]. Першим елементом, який повинен бути проаналізований є суб'єктивні очікування особи, чи могла вона передбачити, що в цьому місці будуть розташовані ТРО та отримані ПД будуть в подальшому використані.

Вартою уваги для розуміння позиції ЄСПЛ щодо «розумних очікувань приватності» є справа «Перрі проти Сполученого Королівства Великої Британії» (Perry vs. the United Kingdom). Заявник був заарештований за вчинення пограбування. Він відмовився взяти участь в пред'явленні для впізнання. Коли його привезли до відділення міліції його зняли на камеру спостереження, яка постійно працювала, і була розташована в місці, через який співробітники міліції та інші підозрювані приїжджали та проходили. Інженер відрегулював камеру, щоб гарантувати, що вона робила чіткі знімки під час візиту заявника. Була підготовлена нарізка відео фрагментів, в якій одинадцять добровольців імітували дії заявника, зафіксовані на негласному відео. Це відео було показано різним свідкам пограбувань, двоє з яких позитивно визначили заявника як причетного до другого та четвертого пограбувань. Ні заявнику, ні його адвокату не було повідомлено про те, що нарізка відео була виготовлена та використана з метою пред'явлення для впізнання, також не була надана можливість переглянути її до моменту її використання [31].

Уряд в свою чергу стверджував, що це [відділення поліції] не можна розглядати як приватне місце, і оскільки камери, які працювали в цілях безпеки, були на помітному для заявника місці, він, мабуть, усвідомив, що його знімають, без обґрунтованого очікування приватності за цих обставин [31].

ЄСПЛ погодився, що звичайне використання камер охорони як таких на громадських вулицях або в приміщеннях, таких як торгові центри чи поліцейські дільниці, де вони служать законним і передбачуваним цілям, не порушує питань відповідно до пункту 1 статті 8 Конвенції [31].

Однак тут поліція відрегулювала камеру безпеки, щоб вона могла зняти чіткі кадри заявника в приміщенні для тримання під вартою та вставила їх у відео нарізки, щоб показати свідкам, щоб ті побачили та ідентифікували заявника як винуватець розбійних нападів. Відеозапис також було показано під час судового розгляду справи над заявником у громадській залі суду [31]. Саме тому, як підкреслює ЄСПЛ, постало питання, чи являло собою таке використання камери та відеозаписів обробку чи використання особистих даних, що мають характер втручання у повагу до приватного життя [31].

Суд наголосив, що незалежно від того, знав заявник чи ні про камери безпеки, які працювали в приміщенні для тримання під вартою, немає жодних ознак того, що заявник мав сподівання на те, що в поліцейському відділенні робилися фотозображення з ним для використання в процедурі ідентифікації та, можливо, як доказ, що завдає шкоди його захисту під час судового розгляду. Такі дії поліції суд розцінив, як вихід рамки звичайного або очікуваного використання камер цього типу, що справді демонструє той факт, що поліція повинна була отримати дозвіл (…). Кадри, про які йдеться у цій справі, не були отримані добровільно або за обставин, коли можна було б обґрунтовано передбачити, що вони будуть записані та використані для ідентифікації. Отже, Суд дійшов висновку, що запис та використання відеозаписів заявника у цій справі є втручанням у його право на повагу до приватного життя [31].

Конкретно визначена мета збору та обробки ПД для суб’єкта даних сприяє розумінню, чи може відбутись втручання в приватне життя, а також дає змогу

проаналізувати, як ПД будуть в подальшому використані і в разі порушень мати можливість оскаржити обробку ПД. Тому, на мою думку, першочерговою гарантією є точне повідомлення про застосування ТРО та мету такого застосування. Для реалізації даної гарантії можливим вбачається, наприклад, визначення в мобільному додатку, який створений для відповідного населеного пункту, точок, де встановлено ТРО. Зараз наша держава прагне до створення так званих «розумних міст». Для цього розробляються мобільні додатки, які можуть стати платформою для зв'язку органів державної влади, місцевого самоврядування та громадськості. В мобільному додатку пропоную впровадити карту відповідного населеного пункту, на які буде позначено території, де розташовано ТРО. Громадськість матиме можливість безперешкодно ознайомитись із такою інформаційною картою і припускати, чи будуть обмежені її права на конкретній території. Варто наголосити на уникненні політичних маніпуляцій. На мою думку, органи державної влади, відповідальні за впровадження ТРО, розробку правил їх використання, повинні вступати в діалог з населенням для аналізу впливу ТРО на звичний стиль поведінки та приватного життя кожного індивіда, намагаючись дійти балансу інтересів.

Також доречним видається окрім загальної мети – встановлення безпеки, більш детально на місцевому рівні прописати конкретні цілі, які мають та можуть бути досягнуті завдяки використанню ТРО, та протягом періоду застосування ТРО не відступати від першочергової мети. Цілком погоджуюсь із Бенджаміном Дж. Гулд, який у своєму дослідженні пише: «…камери слід використовувати лише для тих цілей, які були спочатку визначені, коли було прийнято рішення про їх встановлення: слід уникати поступової «повзучості функцій» [32, с. 29].

Звідси випливає ще один фактор, котрий повинен враховуватись: «системи повинні бути відкритими та прозорими, а особи, відповідальні за їх використання, безпосередньо підзвітні громадськості» [32, с. 29], - йдеться у роботі Бенджаміна Дж. Гулд. Керівникам систем спостереження та розпізнавання, які по суті виступають розпорядниками та/або володільцями ПД,

варто надавати звіти діяльності. Адже «Найгіршою практикою демократії, здається, є надцентралізація рішень щодо національної безпеки в невеликій групі осіб, які приймають рішення, без встановлення механізмів підзвітності» [32, с. 16-17]. Такі звіти повинні містити результати, яких було досягнуто за поточний період, наприклад, впродовж одного кварталу. Під результатами мається увазі кількісні показники, які заходи негативного впливу на населення вдалось попередити завдяки ТРО, чи було затримано осіб, які намагались вчинити злочини та порушити громадську безпеку. Тоді громадськість усвідомлюватиме необхідність впровадження ТРО.

Наступне, про що варто вести мову, це строки зберігання фотозображень, відеозображень та інших ПД у базах даних та їх видалення або знищення. Український законодавець не приділяє уваги строку зберігання ПД. Строк зберігання даних згадується виключно у контексті видалення або знищення ПД: «Персональні дані підлягають видаленню або знищенню у разі закінчення строку зберігання даних, визначеного згодою суб'єкта персональних даних на обробку цих даних або законом» (п.1 ч.2 ст.15 ЗУ «Про захист персональних даних») [17]. У зазначеному законодавчому положенні йде мова про строк зберігання даних, коли суб’єкт даних надавав згоду на обробку цих даних. Які строки є прийнятними для зберігання ПД, коли суб’єкт даних не був залучений до безпосереднього надання згоди законодавець не вказує.

В ЗРПЗД визначено: «Персональні дані необхідно зберігати в формі, що дозволяє ідентифікацію суб'єктів даних не довше, ніж це є необхідним для цілей їхнього опрацювання; персональні дані можна зберігати протягом більш тривалих періодів, доки їх опрацьовують виняткова для досягнення цілей суспільних інтересів, цілей наукового чи історичного дослідження або статистичних цілей відповідно до статті 89(1) за умов вжиття відповідних технічних і організаційних заходів, передбачених цим Регламентом для гарантування прав і свобод суб'єкта даних («обмеження зберігання») [18]. Тобто, період зберігання даних має бути пропорційним меті такого зберігання. Визначення строку зберігання ПД є практично настільки ж важливим як і

визначення мети обробки ПД. Європейська рада захисту даних досліджує застосування ЗРПЗД щодо обробки ПД відео пристроями. В останній Інструкції №3/2019 щодо цього питання від 10.07.2019 р. зазначено, що контролер даних у вузькі терміни повинен визначити, чи необхідно зберігати отримані ПД чи ні [34, с.28]. В документі йде мова про те, що ідеальний в розумінні забезпечення прав суб'єктів даних період зберігання ПД в більшості випадків це декілька днів (наприклад, з метою виявлення вандалізму) [34, с.28]. Укладачі документу пропонують застосовувати автоматичне видалення ПД протягом кількох днів, якщо ПД не становлять жодного інтересу для контролера. Чим довший строк зберігання встановлюється (особливо коли більше 72 годин), тим більш обґрунтованим повинно бути аргументування щодо законності мети та необхідності зберігання ПД. Якщо контролер має намір зберігати дані, він повинен переконатися, що зберігання насправді необхідне для досягнення мети. Якщо так, то строк зберігання повинен бути чітко визначений та індивідуально встановлений для кожної конкретної мети. Контролер відповідає за визначення строку зберігання ПД відповідно до принципів необхідності та пропорційності [34, с.28].

У Сполученому Королівстві у червні 2013 р. було прийнято Кодекс правил відеоспостереження, який закріпив 12 принципів використання камер спостереження відповідними органами. Варто звернути увагу на шостий принцип, а саме на його третій пункт, згідно якого: «Хоча зображення та інша інформація не повинна зберігатися довше, ніж це потрібно для досягнення цілей їх запису, іноді оператору може знадобитися зберігати зображення довше, наприклад, коли правоохоронний орган розслідує злочин, щоб дати їм можливість переглянути зображення для розслідування» [35]. Дане твердження можна трактувати таким чином, що зображення ПД можуть зберігатись протягом більш довгого періоду тільки у випадках, коли планується їх подальше використання і воно обов'язково відповідає першочергово визначеній меті обробки ПД. Якщо ж контролер розуміє, що ПД не мають жодного відношення, наприклад, до розкриття злочину чи не тягнуть за собою подальших активних

дій із боку органів державної влади та/або місцевого самоврядування такі ПД повинні бути знищені. Тому завдання, яке стоїть перед контролером, полягає в чіткому розумінні необхідності ПД для подальших дій. Як уже неодноразово було зазначено ТРО застосовуються в більшості для становлення безпеки та розкриття злочинності. Випадок, наприклад, крадіжки, є доволі очевидним і може бути вирішений протягом короткого періоду, мається на увазі відповідні відео-, фотозображення можуть бути опрацьовані в той же день або в найближчі дні протягом інциденту. Тому потреба в зберіганні ПД може існувати не більше декількох днів. Ті ж ПД, які стосуються інциденту, будуть використані як доказ. В органів державної влади, які проводять заходи запобігання та розслідування злочинів є розуміння того, ПД якого періоду можуть бути необхідні. На основі такого розуміння та із застосуванням математичних розрахунків, можна визначити орієнтовні строки зберігання ПД, які відповідатимуть меті збирання та обробки ПД.

Протягом періоду зберігання ПД суб’єкт даних має право на доступ до своїх ПД. Таке право закріплено зокрема в п.3 ч.2 ст.8 ЗУ «Про захист ПД», також у ст. 16 зазначеного закону визначено порядок доступу до ПД. Подаючи запит про доступ до ПД, суб’єкт даних має можливість отримати копію ПД, які обробляє конкретний розпорядник даних. «Суб'єкт даних повинен (окрім того, що ідентифікує себе) у своєму запиті до контролера вказати, коли - протягом розумного періоду пропорційно до кількості зареєстрованих суб'єктів даних - він або вона потрапляють у зону, що контролюється» [34, с.22]. Право на доступ допомагає суб’єкту даних зрозуміти, які категорії даних обробляються, чи здійснюється передача даних, якщо так, хто є одержувачем, а також ряд інших критеріїв, завдяки яким можна визначити, чи законною є обробка ПД.

Варто більш детально зупинитись на передачі даних. Як неодноразово уже було зазначено, ПД збираються з конкретною метою. Якщо пізніше ПД передаються іншим органами та установам для їх власних цілей, такі дії можуть визнаватись порушенням. Має бути чітке обґрунтування підстав передачі ПД, третя сторона повинна зазначити, чому саме ці дані необхідні та яких законних

цілей буде досягнуто завдяки їх аналізу. Володільці баз даних повинні встановлювати стандарти обробки та гарантії, яких має дотримуватись третя сторона перш, ніж здійснити передачу даних. ЗРПЗД містить вимогу про необхідність договору або іншого нормативно-правового акту, який пов'язує оператора зобов'язальними відносинами з контролером та встановлює предмет і тривалість опрацювання, специфіку і цілі опрацювання, тип персональних даних і категорії суб'єктів даних, обов'язки і права контролера [18]. Це стосується випадків, коли ПД передаються в межах Європейського Союзу. Вимогу укладання договору можна спроектувати на передачу даних між різними органами державної влади в межах території України. Це виключить безпідставну передачу ПД та забезпечить захист від незаконної обробки.

Та все ж, якщо буде виявлено, що при обробці ПД відбулись певні порушення, суб’єкт даних може пред’являти вмотивовану вимогу володільцю ПД із запереченням проти обробки своїх ПД (п.5 ч.2 ст.8 ЗУ «Про захист ПД»), пред'являти вмотивовану вимогу щодо зміни або знищення своїх ПД будь-яким володільцем та розпорядником ПД, якщо ці дані обробляються незаконно чи є недостовірними (п.6 ч.2 ст.8 ЗУ «Про захист ПД»). Ці гарантії не є абсолютними і можуть бути застосовані за наявності відповідних підстав, зокрема ПД підлягають видаленню, якщо закінчився строк зберігання ПД, припинено правовідносини між суб’єктом ПД та володільцем чи розпорядником [17]. В будь-якому випадку суб’єкт даних має засоби реагування реагує на загрози його ПД різними інструментами захисту.

***

Для цілей даної роботи суть ТРО визначено як технологію спостереження, мета якої розпізнавання обличчя. Сфера застосування ТРО характеризується широким колом використання. В цій роботі визначаються основи, підстави застосування ТРО органами державної влади та місцевого самоврядування.

З огляду на природу ТРО важливими аспекти для їх належного функціонування є найперше точність зображень, їх якість, достатність зображень

в базах даних, які піддаються порівнянню обробляються контролерами, адже саме від них залежить досягнення результату.

У розділі зазначається, що ПД мають оброблятись відповідно до принципу «мінімізації даних». Вбачається необхідним закріплення даного принципу та його ключових вимог (достатність, відповідність та доцільність) в українському законодавстві. Визначено, що при застосуванні ТРО висловлення особою згоди на обробку даних практично виключається. Тому необхідно чітко зазначати, встановлювати оголошення-попередження про використання ТРО на відповідній території, пропонується використовувати для цього додатки, які функціонують за принципом «розумного міста», в яких на карті встановлювати місця встановлення ТРО.

РОЗДІЛ 2. ОБРОБКА ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ПРИ ВИКОРИСТАННІ ТЕХНОЛОГІЙ РОЗПІЗНАВАННЯ ОБЛИЧ

2.1. Загальні принципи обробки персональних даних

Конвенція № 108 Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» [36] від 28 січня 1981 р. стала першим документом у сфері захисту ПД, в якому викладено основні принципи обробки ПД, зазначено перелік прав особи у зв'язку з обробкою її ПД, а також базові норми щодо транскордонної передачі даних. Пізніше було прийнято Додатковий протокол (8 листопада 2001 р.) до Конвенції [37], в якому основні положення стосуються деталізації норм, щодо транскордонної передачі даних та йде мова про важливість створення наглядового органу. У Конвенції визначено принципи, які є актуальними і сьогодні. Вони стосуються, зокрема, сумлінного та законного отримання та обробки, зберігання ПД для визначених і законних цілей. Конвенція вимагає також, щоб ПД були адекватними, відповідними та ненадмірними стосовно цілей, для яких вони зберігаються [36].

Постійний розвиток визначає все нові напрямки удосконалення Конвенції та впровадження інструментів захисту ПД. Публічні обговорення в 2011 р. визначили два головних напрямки роботи: посилення захисту приватності в цифровій сфері та зміцнення контрольного механізму Конвенції 108 [38]. Протокол CETS № 223, який було прийнято за результатами обговорень у 2018 р., є модернізованою версією Конвенції. Україна поки не приєдналась до Протоколу CETS № 223.

Примітно, що Протокол CETS № 223 було прийнято в той же ж період, що ЗРПЗД у ЄС. Тому важливо, що більша частина положень обох актів узгоджені. Оновлення зберегло загальний гнучкий характер Конвенції та зміцнило її потенціал як універсального інструмента для захисту ПД. Внаслідок оновлення було підтверджено та закріплено важливі принципи і введено нові права фізичної особи [39, с.29].

Детально ті більш широко принципи обробки даних прописано і в рекомендаційних актах, зокрема у частині ІІ Резолюції про міжнародні стандарти конфіденційності [40], розробленій під час Міжнародної конференції уповноважених із захисту даних, що відбулася 03.01.2011 р.

Одним із першочергових принципів визначено принцип законності та справедливості обробки ПД, згідно якого «ПД мають оброблятися з додержанням національного законодавства, прав і свобод людини, а також у відповідності до цілей та принципів, викладених у Загальній декларації прав людини та Міжнародному пакті про громадянські та політичні права» [40].

Окремо в Резолюції конкретизується визначеність цілей обробки, – «обробка ПД має обмежуватися виконанням конкретної, явної та законної мети відповідальної особи» [40]. У попередньому розділі було звернено увагу, що суб'єкти даних мають бути попередженні про визначену мету, задля якої збираються ПД. Що важливо: ця мета не може змінюватись протягом періоду, на який дана згода на обробку.

Наступним принципом, який випливає із визначеності цілей обробки визначається «принцип пропорційності – обробка ПД повинна бути адекватною, пропорційною та не надмірною щодо її цілей» [40]. Тобто, якщо у конкретній ситуації немає необхідності обробки всіх ПД, на обробку яких надав згоду суб'єкт ПД, то варто обмежуватись виключно рівнем обробки, який достатній у конкретній ситуації. Стосовно тесту на пропорційність правових положень, що дозволяють збирати ПД, Максиміліан із посиланням на німецьку судову практику визначає, кілька критеріїв: по-перше, кого і скількох осіб стосується збирання ПД; по-друге, за яких обставин збираються дані, наприклад, чи вказали особі причину чи ні, чи збирання даних відбувається таємно чи відкрито; і по-третє, інтенсивність порушення [41, с.167]. Окремої уваги потребує третій наведений Максиміліаном критерій. Для визначення останнього критерію до уваги має братись, наскільки актуальною є інформація для особистості, зокрема, якщо вона поєднується з іншими даними; чи могла особа розраховувати, що дані про неї будуть оброблятися певним чином [41, с.168]. В цьому критерію визначається

рівень очікувань особи щодо збирання та обробки ПД по відношенню до неї, а також ставлення особи до того, що її дані можуть також бути передані і в подальшому використовуватись.

Наступний визначений у Резолюції принцип – це «принцип якості даних – відповідальна особа завжди має забезпечувати точність, достатність та своєчасне оновлення ПД для того, щоб досягнути цілей, з якими вони обробляються» [40].

Останні два принципи, про які йде мова у Резолюції спрямовані на забезпечення гарантій прозорості. Перш за все «принцип відкритості – будь-яка відповідальна особа повинна проводити прозору політику відносно обробки ПД. Відповідальна особа повинна надавати суб'єктам даних як мінімум інформацію про відповідальну особу, цілі обробки, одержувачів цих даних, про те, яким чином вони будуть використовуватись, а також будь-яку іншу додаткову інформацію» [40]. Його доповнює принцип «звітності – відповідальна особа повинна вживати усіх необхідних заходів для додержання принципів та обов'язків, закріплених національним законодавством, та мати необхідні внутрішні механізми для демонстрації додержання цих принципів та обов'язків як суб'єктами даних, так і наглядовим органом при виконанні своїх обов'язків» [40].

Умовно ці принципи при обробці ПД розкриваються один за одним, доповнюючи та підсумовуючи попередній. Лінслей Дублетс виокремлює три категорії принципів від оцінки загальної допустимості обробки даних до адекватного використання інформації, що складаються з механізмів забезпечення якості даних, а також захисту прав суб'єктів даних визначаються у більшості міжнародних актів, хоча можуть по різному визначатись [42, с. 550].

Виокремлені принципи є основою, фундаментальними засадами при обробці ПД та повинні враховуватись всіма контролерами та розпорядниками ПД для забезпечення прав суб'єктів ПД. Належне тлумачення та глибоке розуміння принципів є важливим механізмом впровадження систем захисту ПД.

2.2. Українське законодавство у сфері захисту персональних даних

З 2011 р. в Україні діє закон «Про захист персональних даних» [17], який в більшій мірі відображає Конвенцію «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних».

Закон визначає загальні вимоги, принципи обробки ПД, про які йшла мова у попередньому підрозділі, окреслює коло прав та обов'язків суб'єктів ПД та встановлює порядок обробки ПД, тобто дію або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення ПД, у тому числі з використанням інформаційних (автоматизованих) систем [17]. Вимоги до кожного з етапів обробки ПД встановлюються Законом додатково.

Український законодавець окремо встановлює особливі вимоги до обробки ПД про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних [17]. За загальним правилом ч. 1 ст. 10 ЗУ «Про захист персональних даних» такі дані заборонено обробляти [17]. Встановлено виключний перелік підстав для їх обробки, серед яких однозначна згода на обробку таких даних, необхідність використання даних у трудових відносинах та інші. Примітно, що в цьому переліку немає підстави обробки ПД в цілях національної безпеки та для становлення громадського порядку, також не згадується про презумпцію згоди на обробку в публічних місцях. На ці підстави часто посилаються при обробці біометричних даних.

В той же час Цивільний кодекс України [43] у ч. 1 ст. 307 визначає: «Фізична особа може бути знята на фото-, кіно-, теле- чи відеоплівку лише за її згодою». А в публічних місцях: «згода особи на знімання її на фото-, кіно-, теле- чи відеоплівку припускається». Зйомка, на мою думку, є більш простим процесом, якщо порівнювати із функціонуванням ТРО. Тому, як зазначено у

статті «Україна: Регулювання технології розпізнавання обличчя»: «ці положення не обов'язково застосовуються для розпізнавання обличчя» [44]. Тобто припущення згоди на запис особи на камеру не обов’язково означає припущення згоди на застосування ТРО та обробку біометричних даних.

Визначення ж біометричних даних міститься тільки в Законі України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» і розуміється як сукупність даних про особу, зібраних на основі фіксації її характеристик, що мають достатню стабільність та істотно відрізняються від аналогічних параметрів інших осіб (біометричні дані, параметри - відцифрований підпис особи, відцифрований образ обличчя особи, відцифровані відбитки пальців рук) [45]. Безумовно дана дефініція дає розуміння поняття біометричних даних, але зазначений закон не має відношення до законодавства України у сфері ПД та не є таким, що встановлює гарантії при обробці біометричних даних. Вбачається необхідність саме в комплексному підході до захисту ПД, в тому числі біометричних. Мається на увазі зведення положень у сфері захисту ПД в один нормативно-правовий акт. Поряд з цим, удосконалення законодавства у сфері захисту ПД тісно пов’язане із встановлення порядку використання технологій.

В Україні на даному етапі немає заборони використання ТРО, але й немає закріплених вимог до використання ТРО, не проаналізовано, наскільки такі технологій є необхідними у діяльності органів державної влади та/або місцевого самоврядування, в першу чергу органів Національної поліції. Це може призвести до численних зловживань та порушень вимог щодо обробки ПД з боку органів, що уже використовують ТРО або планують використання технології.

2.3. Європейське регулювання технологій розпізнавання облич та питань захисту персональних даних

ЗРЗПД [18] – це акт, мета якого «забезпечити вільний рух даних по всьому Європейському Союзу (ЄС) та встановити право на захист персональних даних всередині ЄС та за його межами до тих пір, поки дані суб'єкта обробляються» [46, с. 1159]. Регламент набрав чинності у травні 2018 року та запровадив чимало нових вимог зобов’язань щодо обробки ПД і в той же час розширив права суб’єктів персональних даних.

ЗРЗПД вводить важливе поняття – біометричні дані. Згідно п. 14 ст. 4 Регламенту «біометричні дані означає персональні дані, отримані в результаті конкретної технічної обробки, що стосується фізичних, фізіологічних або поведінкових характеристик фізичної особи, які дозволяють або підтверджують унікальну ідентифікацію цієї фізичної особи, наприклад зображення обличчя або дактилоскопічні дані» [18]. ЗРЗПД відносить біометричні дані разом із ПД, що розкривають расову чи етнічну приналежність, політичні переконання, релігійні чи філософські вірування, чи членство в професійних спілках, і опрацювання генетичних даних, даних стосовно стану здоров'я чи даних про статеве життя фізичної особи чи її сексуальної орієнтації до спеціальної категорії – «чутливі дані» [18].

«Обробка біометричних даних, включаючи зображення обличчя, вважається особливо чутливою для цілей Регламенту і підпадає під більш жорсткі правила як одна із «спеціальних категорій даних» [47], – зазначає Кларе Селларс. Таким чином, якщо дані є спеціальною категорією, обробка повинна підпадати під виняток відповідно до статті 9 (2) ЗРЗПД.

Так, у статті 9 (2) ЗРЗПД визначає ряд законних підстав, відповідно до яких може здійснюватися обробка чутливих ПД, в тому числі біометричних даних: (a) суб'єкт даних надав явну згоду на опрацювання таких ПД, (b) опрацювання є необхідним для цілей виконання обов'язків і здійснення спеціальних прав контролера або суб'єкта даних у сфері зайнятості (…) (c) опрацювання є

необхідним для захисту життєво важливих інтересів суб'єкта даних або іншої фізичної особи, якщо суб'єкт даних фізично чи юридично неспроможний надати згоду; (d) опрацювання здійснюють в ході відповідної законної діяльності з необхідними гарантіями (…); (e) опрацювання стосується ПД, що відкрито оприлюднені суб'єктом даних; (f) опрацювання є необхідним для формування, здійснення або захисту правових претензій або якщо суди діють як судові органи;(g) опрацювання є необхідним з причин суттєвого суспільного інтересу, на підставі законодавства Союзу або держави-члена, що має бути пропорційним цілі, якої прагнуть досягти, поважати сутність права на захист даних і передбачати належні та спеціальні заходи для захисту фундаментальних прав та інтересів суб'єкта даних; (h) опрацювання є необхідним для цілей превентивної медицини чи гігієни праці (…); (i) опрацювання є необхідним з причин суспільного інтересу в сфері охорони суспільного здоров'я (…); (j) опрацювання є необхідним для досягнення цілей суспільного інтересу, цілей наукового чи історичного дослідження або статистичних цілей [18].

Варто звернути увагу, що не всі дані, що стосуються фізичних, фізіологічних або поведінкових характеристик фізичної особи, що дозволяють перевірку або ідентифікацію фізичної особи, вважаються біометричними даними згідно з ЗРЗПД. Просто збирання та зберігання таких даних без будь-якої конкретної біометричної обробки не підпадає під згаданий вище спеціальний захист [48, с.530]. У продовження цієї думки Кіндт у статті про новий правовий режим біометричних даних наводить приклад із зображеннями облич або відбитками пальців. Автор зазначає, що база даних, із зображеннями обличчя або відбитками пальців без біометричної обробки, не вважатиметься базою даних з біометричними даними або біометричною базою даних. Таким чином, створення або ведення такої бази даних також не підпадає під конкретні правила для обробки біометричних даних, крім загальних правил захисту даних, які застосовуються до всіх ПД [48, с.530]. Отже, спеціальний захист та особливі гарантії до біометричних даних застосовуються тоді, коли ці дані безпосередньо використовується для ідентифікації. Мета ТРО саме встановлення особи, дані

збираються та використовуються саме з метою ідентифікації. Тому можна припустити, що при використанні ТРО в більшості випадків будуть поширюватись гарантії захисту для чутливих даних. Тут якраз можна провести істотну різниця між ПД, отриманими із камер відеоспостереження та завдяки ТРО. У випадку із зображенням із камер відеоспостереження вони не обов'язково будуть використані для ідентифікації. Тоді як камери із функцією розпізнавання облич за своєю суттю передбачають ідентифікацію, тому до ПД, отриманих в цей спосіб варто застосовувати більш широке коло гарантій.

ЄСПЛ також звертає особливу увагу на обробку та зберігання біометричних даних. У справі M.K. v. FRANCE (Application no. 19522/09) заявник скаржився на збереження даних стосовно нього в комп'ютеризованій базі даних відбитків пальців. У зв'язку з двома розслідуваннями у заявника двічі брали відбитки пальців. Відповідно до статті 1 французького указу, оцінка якому надається ЄСПЛ, комп'ютерна обробка відбитків пальців і долонь покликана сприяти зусиллям національної поліції та жандармерії з метою виявлення та встановлення винних у серйозних злочинах та інших серйозних правопорушеннях та забезпечення судового переслідування, розслідування та розгляд справ, переданих до судових органів. Пізніше заявник просив видалити його дані із бази відбитків пальців. Прокурор, до якого заявник подавав звернення наказав видалити лише відбитки пальців, зняті під час першого провадження. Він стверджував, що збереження одного зразка відбитків пальців заявника є виправданим в його ж інтересах. Заявник не погодився із такою позицією і подав оскарження до суду. Суд підтримав позицію сторони обвинувачення. На його думку зберігання відбитків пальців відповідає інтересам слідчих органів. Крім того, цей захід не завдав шкоди заявникові завдяки конфіденційності бази даних, яка запобігла будь-якому впливу на приватне чи соціальне життя заявника [49].

ЄСПЛ не погодився із такою позицією національних органів. Суд звернув увагу, що захист ПД має фундаментальне значення для здійснення особою свого права на повагу до приватного та сімейного життя. Тому, національне

законодавство повинно забезпечити відповідні гарантії для запобігання будь-якому такому використанню ПД, яке може суперечити гарантіям цієї статті [49]. Суд також вважає, що потреба у таких гарантіях ще більша, якщо це стосується захисту ПД, що проходять автоматичну обробку, не в останню чергу при використанні таких даних для поліцейських цілей. Національне законодавство повинно, зокрема, забезпечити, щоб такі дані були доречними та не надмірними щодо цілей, для яких вони зберігаються, і зберігалися у формі, яка дозволяє ідентифікувати суб'єктів даних не довше, ніж це потрібно для цілей, для яких ці дані зберігаються [49]. Суд підкреслює необхідність додаткових гарантій, коли це біометричні дані, які піддаються автоматичній обробці і завдяки яким здійснюється ідентифікація особи. Таких додаткових гарантій законодавство Франції не передбачало. А період зберігання ПД, який становить 25 років згідно указу, Суд окреслив як строк рівнозначний на практиці невизначеному збереженню [49]. Дана справа також є ілюстрацією того, що зберігання даних, особливо біометричних даних, незалежно від того, чи вони будуть використані, саме по собі уже може визнаватись втручанням у приватне життя особи та ставити під питання дотримання основних вимог захисту ПД. Національне законодавство повинно ретельно визначати вимоги до етапів обробки ПД, особливо до зберігання біометричних даних. Тому що бази біометричних даних зростають, підкреслює Кіндт та акцентує увагу на тому, що для зберігання зображень облич потрібно переглядати політики конфіденційності [50].

ЗРПЗД у надає державам-членам право мати або вводити деталізовані умови, в тому числі, обмеження, у зв'язку з опрацюванням генетичних даних, біометричних даних або даних стосовно стану здоров'я (пункті 4 статті 9 ЗРПЗД) [18]. Не вдаючись до деталей поширення ЗРЗПД на Великобританію на етапі її виходу з Європейського Союзу, відзначу Закон Великобританії «Про захист даних» від 2018 р., який встановлює деталізований підстави, умови обробки спеціальних категорій ПД, до яких даний закон також відносить біометричні дані.

У частині 2 додатку 1 зазначеного Закону деталізується, що таке умови значного суспільного інтересу. До таких Закон відносить законодавчі та інші державні цілі, відправлення правосуддя та парламентські цілі, запобігання або виявлення протиправних дій, захист громадськості від нечесності та ряд інших умов [51]. При цьому кожна умова має свої підстави для обробки ПД. Наприклад, умова запобігання або виявлення протиправних дій виконується, якщо обробка - (а) необхідна для запобігання або виявлення протиправного діяння, (б) повинна проводитися без згоди суб'єкта даних, щоб не зашкодити цим цілям, і (в) необхідна з міркувань, що становлять значний суспільний інтерес [51]. Поняття суспільного (громадського) інтересу з’являється не в одній умові, але у кожній має свій сенс. На платформі Управління Уповноваженого Великобританії з питань інформації зазначено: «Суспільні інтереси охоплюють широкий спектр цінностей та принципів, що стосуються суспільного блага або того, що відповідає інтересам суспільства. Це повинно бути реальним і суттєвим. З огляду на властиві спеціальним категоріями даних ризики, недостатньо наводити нечіткий або загальний аргумент щодо суспільних інтересів» [52].

Деталізації категорії «суспільний інтерес» має важливе значення для захисту прав суб’єкта даних. Часто використання оціночних категорії, якою є «суспільний інтерес», є безпідставним та маніпулятивним з боку органів державної влади та місцевого самоврядування. Закон Великобританії на мою думку мінімізує ризики безпідставного апелювання до категорії «суспільний інтерес» та вимагає від розпорядників/володільців даних конкретизації – вказівки, які саме блага порушуються/можуть зазнати порушень та яким чином конкретні інструменти, для використання яких необхідною є обробка ПД, можуть сприяти запобіганню порушень.

Питання потенційних переваг застосування ТРО було поставлено для вирішення у вересні 2019 р. у Вищому суді в місті Кардіфф. Позивач посилався на те, що використання ТРО передбачає збір та подальшу обробку унікальних біометричних даних великої кількості людей для чого немає підстав. Він порівнював біометричні дані обличчя та відбитки пальців та біометричних даних

ДНК та подальше використання таких даних. Позивач звернув увагу суду, що використання відбитків пальців та ДНК підкріплені статутом та предметом детальних вказівок, що встановлюють ряд критеріїв про те, коли і як дані можна брати та обробляти. По відношенню до біометричних даних облич конкретно встановлених критеріїв обробки немає, тому поліцією Уельсу було порушено його право на приватність та захист ПД [53].

Позивач без його згоди двічі потрапив під запис відеокамер – одного разу, здійснюючи покупку, а наступного під час відвідування політичної акції. Система відеоспостереження була влаштована таким чином, що відеокамери, які сканують обличчя в натовпі, порівнювали зображення з поліцейською базою розшуку людей. Коли система знаходить відповідність, вона надсилає попередження офіцерам командного центру, які потім зв'язуються з іншими офіцерами, щоб затримати особу. Такий спосіб використовувався поліцією Уельсу на різноманітних заходах, де було велике скупчення людей [53].

Суд вирішив, що використання таких систем є прийнятним, а той факт, що технологія є новою, не означає, що вона виходить за рамки існуючого регулювання або що для неї завжди необхідно створити спеціальну правову базу [53]. У п. 159 рішення судом зроблено висновок: «чинний правовий режим є достатнім для забезпечення належного та небезпідставного використання автоматизованого розпізнавання обличчя, і що використання Поліцією Південного Уельсу на сьогоднішній день автоматизованого розпізнавання обличчя відповідає вимогам закону про права людини та законодавству про захист даних» [53].

Такі висновки не підтримав апеляційний суд, який побачив ряд ризиків у використанні ТРО. Найпершим з яких є те, що існуюче законодавство та місцева політика не дають чітких вказівок щодо параметрів, які слід застосовувати при використанні ТРО. Суд також зазначив, що окремим працівникам поліції було надано занадто багато повноважень, щоб вирішувати, кого включати до списку осіб, за якими ведеться спостереження, також не встановлено і не було ясно, чи

існують будь-які критерії для визначення місця, де є необхідність у застосовуванні ТРО [54].

Дане рішення підкреслює, що ТРО містить ряд відмінностей від інших технологій ідентифікації, тому потребує окремого правового регулювання. Загальні принципи обробки ПД, гарантії захисту від порушень у сфері ПД не є достатніми, коли йде мова про ТРО. Це окрема технологія, яка має свою специфіку використання, в першу чергу пов’язану із поширенням на невизначене коло людей.

Апеляційний суд відзначив також належні елементи функціонування системи. Зокрема, звернено увагу на те, що дані тих, хто не відповідає особі в списку спостереження, автоматично видаляються без будь-якого перегляду та втручання людини і що це відбувається майже миттєво. Апеляційним судом вбачається необхідність в закріплені даної процедури видалення; висловлено сподівання, що ця особливість поточної схеми не буде просто викладена в політичному документі шляхом опису, а що буде чітко вказано, що такі автоматичні та майже миттєві видалення є потрібними, щоб забезпечити існування адекватної правової база для використання ТРО [54].

Це рішення є важливим не тільки для Великобританії, а й для інших європейських країн, адже виражає чітку позицію, що використання ТРО можливе лише після врегулювання, встановлення процедури, забезпечення гарантій саме для використання ТРО. Питання стоїть не тільки в забезпеченні дотримання заходів обробки ПД, але й у встановленні та дотриманні вимог використання ТРО. Із рішення прочитується висновок, що до моменту визначення законодавчих меж для застосування ТРО, використання технології є незаконним.

Примітно, що на рівні ЄС на початку 2020 р. обговорювалась пропозиція на даному етапі заборонити використання ТРО в громадських місцях на найближчі п'ять років [55]. В основі такого відтермінування ідея, що «тимчасова заборона дасть дослідникам та розробникам політики час вивчити технологію та з'ясувати, як найкраще її регулювати» [55].

А уже у квітні 2021 р. ЄС запропонував проект Регламенту, який обмежуватиме або заборонятиме деякі види використання штучного інтелекту в межах ЄС [56], – пише видання The New York Times. У проекті Регламенту «Встановлення гармонізованих правил щодо штучного інтелекту (Закон про штучний інтелект)» йде мова про те, що використання штучного інтелекту із його специфічними характеристиками, серед яких можна виділити непрозорість, складність, залежність від даних, автономна поведінка може негативно вплинути на низку основних прав, зокрема на право на приватність та захист ПД. Тому мета проекту Регламенту – забезпечити високий рівень захисту основних прав, оцінити ризики, які тягне за собою застосування штучного інтелекту та визначити підходи для уникнення таких ризиків [57]. Маргрете Вестагер, європейська комісарка з питань конкуренції, вважає підхід застосований у проекті Регламенту цілком послідовним та таким, що заснований на оцінці ризиків, тому його можна обґрунтувати простою логікою: «Чим вищий ризик, тим жорсткіше правило», йдеться у статті Джордже Ліборейро [58].

Використання системи розпізнавання, ідентифікації згідно проекту Регламенту можна зрозуміти як діяльність із високим ризиком. У тексті проекту Регламенту використовується поняття дистанційна система біометричної ідентифікації у реальному часі [57]. Аналізуючи використання даного поняття у проекті акту можна дійти висновку, що до таких систем відносяться ТРО.

Згідно проекту Регламенту, за загальним правилом, використання дистанційної системи біометричної ідентифікації у реальному часі заборонено (параграф 1d стаття 5 розділ 2), адже вважається особливим видом втручання у права та свободи зацікавлених осіб в тій мірі, яка може вплинути на приватне життя значної частини населення, та викликає у населення відчуття постійного нагляду і опосередковано перешкоджає здійсненню права на свободу зібрань та реалізації інших основних прав. Крім того, безпосередність впливу та обмежені можливості подальших перевірок або виправлень щодо використання таких систем, що працюють у режимі реального часу, несуть підвищений ризик для прав і свобод осіб, до яких застосовуються правоохоронні заходи [57].

Використання системи є можливим тільки у певних, регламентованих випадках. Кожне використання системи в загальнодоступних приміщеннях для правоохоронних цілей повинно бути предметом чіткого та конкретного дозволу судового органу або незалежного адміністративного органу [57]. Фактично перед наданням дозволу відповідний орган повинен провести попередню оцінку застосування технології, визначити, чи є пряма необхідність у такому застосуванні і тільки тоді, якщо є підстави для застосування, надати відповідний дозвіл.

До використання технології без попереднього дозволу проект Регламенту встановлює додаткові вимоги та визначає, що таке використання є можливим лише у випадку належним чином обґрунтованих ситуацій терміновості. У проекті Регламенту визначено, що обґрунтовані ситуації терміновості – це ситуації, коли необхідність використання розглянутих систем така, що робить ефективним та об'єктивно неможливим отримання дозволу до початку використання [57]. Для використання систем у термінових ситуаціях потрібно дотримуватись вимоги мінімізації, тобто використання повинно бути обмежене до необхідного мінімуму, і підлягати належним гарантіям та умовам, визначеним національним законодавством та зазначеним у контексті кожного окремого випадку невідкладного використання самим правоохоронним органом [57]. Крім того, правоохоронний орган повинен у таких ситуаціях прагнути отримати дозвіл якомога швидше, при цьому вказуючи причини неможливості подати клопотання про такий дозвіл раніше [57].

Фрідеріке Реінхолд, аналізуючи проект Регламенту, відзначає велику кількість винятків та зачіпок, які можуть привести до безпідставного використання систем штучного інтелекту. Одним із найперших недоліків авторка відзначає неврегульованість використання дистанційних систем біометричної ідентифікації у реальному часі іншими державними органами, окрім правоохоронних органів [59]. Цілком погоджуюсь із даною позицією. У проекті Регламенту, йде мова виключно про використання систем правоохоронними органами. Проте, як уже зазначалось у даній роботі, системи

розпізнавання облич можуть використовуватись не тільки в правоохоронних цілях. Відповідно інші органи державної влади, а також органи місцевого самоврядування можуть вдаватись до застосування технологій розпізнавання та ідентифікації. Проект Регламенту не містить вказівки, яка б дала підстави презюмувати, що інші органи не можуть використовувати технологію. Тому потребує уточнення положення про заборону використання технологій відносно органів держаної влади та місцевого самоврядування, окрім правоохоронних органів.

Наступне на, що звертає увагу Фрідеріке Реінхолд, це низка виключень із заборони застосування систем. Встановлення широкого кола виключень створює прогалини, які органи влади можуть спробувати використати на свою користь [59]. До прикладу авторка коментує можливість використання систем ідентифікації для запобігання конкретній, суттєвій та безпосередній загрозі життю або фізичній безпеці фізичних осіб або теракту, підкреслюючи, що дане положення залишає широке коло дискреційних повноважень для органів влади. Гарантією є отримання дозволу на використання технології, але знову ж таки є випадки, про які було зазначено вище у цьому розділі, коли можна відкласти отримання дозволу [59]. Таким чином, із врахуванням усіх винятків, за яких технології розпізнавання можуть бути використані, залишається вузька сфера реальної заборони біометричної ідентифікації в режимі реального часу.

Варто відзначити, що проект Регламенту розділяю розпізнавання та ідентифікацію на дві групи: в режимі реального часу та подальша (пост) ідентифікація. Дистанційну систему біометричної ідентифікації в режимі реального часу визначено як віддалену систему біометричної ідентифікації, за допомогою якої збір біометричних даних, порівняння та ідентифікація відбуваються без значних затримок. Це включає не тільки миттєву ідентифікацію, але й обмежені короткі затримки, щоб уникнути труднощів в ідентифікації [57]. Решта випадків, які не підпадають під режим реального часу, розглядаються як подальша (пост) ідентифікація. Обидві групи ідентифікації слід класифікувати як групи технологій високого ризику, і з огляду на це вони

повинні підпорядковуватися строгим вимогам. Проте проаналізована вище стаття 5, яка встановлює випадки заборони використання штучного інтелекту, поширюється тільки на системи ідентифікації в режимі реального часу. Тобто подальша ідентифікації з використанням вже зібраних фото-, відеозображень не підпадає під заборону, встановлену статтею 5. Цим самим залишаючи можливість для застосування технологій спостережень.

Не зважаючи на певні прогалини, проект Регламенту оцінюється як позитивний крок на шляху регулювання штучного інтелекту, тому є потреба в його обговоренні та подальшому прийнятті [59].

2.4. Досвід США в регулюванні технологій розпізнавання облич та питаннях захисту персональних даних

В одному із найбільших американських міст – Сан-Франциско – місцева влада у травні 2019 р. заборонила використання ТРО, які у своїй діяльності використовували багато поліцейських для розшуку злочинців у справах від найменшої тяжкості до масових вбивств [28].

Професор філософії Еван Селінджер, який разом із професором правничих та комп'ютерних наук Вудроу Хартзог вивчали питання прозорості використання технологій розпізнавання обличь підтримує заборону використання таких технологій і в інтерв'ю «USA.TODAY» таким чином висловився щодо позиції заборони використання ТРО: «Якщо американський спосіб життя збережеться – свобода висловлювань, свобода асоціацій та вільний рух - найкращий шлях уперед - це визнати, що в даний час технологія розпізнавання обличчя є унікальним загрозливим інструментом пригнічення, якому не може бути місця в традиційному управлінні» [60]. Із зазначеного, приходжу висновку, що професори наголошують не тільки на втручанні в право на приватність, також йде мова про загрозу порушення ряду інших свобод, які є не менш важливими в демократичному суспільстві. Скоріш за все вплив на перелічені авторами свободи не настільки прямо простежується, як втручання

через ТРО у право на приватність, але це не означає, що цими правами можна знехтувати. Оцінка впливу ТРО має відбуватись комплексно – із розгляду всіх прав людини і громадянина, яким потенційно може бути завдана шкода.

Наприклад, Тіберіу Драгу змодельвував декілька варіантів взаємодії між терористичними та антитерористичними організаціями, для того щоб проаналізувати як обмеження приватності впливає на безпеку, як йде мова у дослідженні, від терористичних нападів. Автор дійшов висновку: «зниження приватності не обов'язково підвищує безпеку від тероризму» [61, с. 75].

Щодо законодавчого закріплення можливості використання ТРО в США варто зазначити, що регулювання здійснюється на рівні кожного штату. На федеральному ж рівні не існує закону, який би спеціально регулював технологію, що розвивається, в той же час є пропозиції численних законопроектів [62].

Зазначаючи про акти окремих штатів, варто звернути увагу на Каліфорнійський закон «Про приватність споживачів» [63] від 2018 року, який набрав чинності у січні 2020 року. Закон оперує поняттям споживач, а не суб’єкт даних, як, наприклад, ЗРЗПД, із яким часто порівнюють цей закон. «Споживачем визнається фізична особа, яка є резидентом Каліфорнії» [63]. Таким чином, усі інші особи під дію Каліфорнійського закону не попадатимуть і відповідно ніяким чином не зможуть захистити свої права.

У Каліфорнійському законі застосовується достатньо широке визначення персональної інформації. Примітно, що саме категорія «персональна інформація» використовується у даному законі. Каліфорнійський закон наводить перелік інформації, яку варто розглядати як персональну, і відносить сюди окрім звичних із інших актів загальних даних (прізвище, ім’я, електронна адреса і т.д.), інформацію про діяльність в Інтернеті, а також біометричну інформацію. Закон деталізує поняття біометричної інформації. «Біометрична інформація означає, – фізичні, біологічні або поведінкові особливості людини, включаючи дезоксирибонуклеїнову кислоту (ДНК), яку можна використовувати окремо або в поєднанні один з одним або з іншими ідентифікаційними даними для встановлення особи. Біометрична інформація включає, але не обмежуючись

ними, зображення райдужної оболонки, сітківки, відбитків пальців, обличчя, руки, долоні, венних візерунків і записів голосу, з яких складається ідентифікаційний шаблон, такий як відбиток обличчя, шаблон дрібниць або голосовий відбиток , можуть бути вилучені, і натискання клавіш або ритмів, схеми ходи або ритми, дані про сон, здоров'я та фізичні вправи, які містять ідентифікаційну інформацію» [63].

Згідно закону є загальні інструменти захисту персональної інформації, які включають можливість надати повний звіт про всі дані, які система має про споживача, який запитав їх інформацію, також право «бути забутим», згідно якого буде видалено усі асоційовані зображення обличчя та ідентифікатори [63]. В основному цей закон стосується «бізнесу», але все ж є актуальним для розуміння підходу до визначення поняття персональної та біометричної інформації.

Можна сказати, що Каліфорнійський закон спрямований більше не на тотальний захист прав і інтересів суб'єктів даних (як, наприклад, ЗРЗПД), а швидше на те, щоб викорінити в компаній елемент розхлябаності до питань захисту ПД. Проте в будь-якому випадку даний акт має на меті посилення контролю щодо захисту ПД [64].

В США окрім дискусій навколо втручання ТРО в право на приватність та захист ПД, гостро також стоїть проблема застосування ТРО для ідентифікації афро-американців та осіб азіатської зовнішності [65]. Рон Уайден в коментарі виданню «The Washington Post» звернув увагу: «Будь-яка компанія чи уряд, що застосовує нові технології, несе відповідальність за перевірку свого продукту на предмет упередженості та дискримінації принаймні настільки ретельно, наскільки вони шукають помилки у програмному забезпеченні» [65].

Виокремлення проблеми, дискусія навколо шляхів її вирішення не запобігли помилковій ідентифікації особи у зв’язку із особливостями зовнішності. Видання «The New York Times» повідомляло, що Роберт Вільямс, житель штату Мічиган, був помилково арештований у зв’язку з неналежним

функціонування ТРО [66]. Пізніше виявилось, що технологія, розроблена для поліції міста Детройт, майже ніколи не призводить до прямого поєднання і майже завжди неправильно ідентифікує людей [67]. Органи поліції, розуміючи із наявної у них статистичної інформації помилковість ідентифікації, продовжували використовувати ТРО, цим самим нехтуючи правами осіб, які є потенційними суб'єктами даних [67]. Практично стовідсоткова помилковість системи, відсутність дії, спрямованих на уникнення помилкових ситуацій із боку органів поліції, викликає недовіру населення до технології та виявляє, як недосконаліть самої технології так і неспроможність державних органів забезпечити її належне застосування.

Окреслена ситуація є демонстративним прикладом того, як використання ТРО може призвести до помилкової ідентифікації, призвести до серйозного вторгнення в приватне життя, призвести до незаконних арештів та/або затримання та перешкоджати принципам та вимогам належного судочинства та процесуальної справедливості [68].

У позові проти органів поліції представники Роберта Вільямса акцентують на тому, що відомості, отримані завдяки ТРО не могли служити належною підставою для арешту, політика, встановлена у відділі поліції стосовно використання ТРО була невідповідною [69]. Основною вимогою у позовній заяві, на мою думку, є прийняття рішення, що забороняє використовувати ТРО як метод розслідування, якщо вони невірно ідентифікують осіб із суттєво різними показниками залежно від раси, етнічної приналежності або кольору шкіри [69].

Рішенню у даній справі може бути рушійним. На перший погляд очевидним видається порушення поліцейськими органами вимог до застосування ТРО. Проте суду необхідно буде вирішити, в якій мірі поліцейські органи можуть нести відповідальність, адже, на мою думку, не варто виключати халатність розробників технології, які здійснюють продаж та розповсюдження технології.

***

Виокремлено загальні принципи обробки ПД, до яких, згідно міжнародних актів відносяться законність та справедливість обробки ПД, якість даних визначення цілей обробки, , пропорційності, а також прав суб'єктів даних. Надано аналіз українського законодавства у сфері захисту персональних, звернено увагу, що в Україні на даному етапі немає ані заборони, ані дозволу на використання ТРО, тому запропоновано законодавчо закріпити вимоги до обробки персональних даних, отриманих завдяки використанню ТРО.

Окреслено європейський підхід до обробки персональних даних, проаналізовано основні положення GDPR, згідно яких біометричні дані, включаючи зображення обличчя, є спеціальною категорію даних, тому підпадають під більш жорсткі правила обробки. У розділі також звернено увагу, що в Європейському Союзі обговорюється питання заборони використання ТРО до встановлення правил та умов їх використання.

В США розвиток та регулювання ТРО залежать від штату, наведено до прикладу один із найновіших актів Каліфорнійський закон «Про приватність споживачів», згідно якого визначається поняття біометричної інформації.

Таким чином, у цьому розділі проаналізовано підхід до обробки ПД згідно декількох актів. Можна підсумувати, що без належного правового регулювання ТРО не повинні використовуватись, адже існує великий ризик зловживань. Врегулювання порядку використання ТРО є одним із аспектів регулювання застосування штучного інтелекту. Тому вбачається необхідними розвиток національного законодавства у двох паралельних сферах: доопрацювання наявних актів, що регулюють питання обробки ПД та встановлення вимог до застосування ТРО, як системи штучного інтелекту.

РОЗДІЛ 3. ОБСЯГ ПРАВА НА ПРИВАТНІСТЬ ТА СПІВВІДНОШЕННЯ ІЗ ПРАВОМ НА ЗАХИСТ ПД

3.1. Обсяг права на приватність

Аналіз права на приватність варто вести від міжнародних актів про права людини, які забезпечують універсальний базис, на основі якого слід оцінювати будь-яке втручання в право на приватність.

Загальна декларація прав людини 1948 р. вперше на міжнародному рівні закріпила право на приватність. Згідно статті 12 Загальної декларації прав людини: «Ніхто не може зазнавати безпідставного втручання у його особисте і сімейне життя, безпідставного посягання на недоторканність його житла, таємницю його кореспонденції або на його честь і репутацію. Кожна людина має право на захист закону від такого втручання або таких посягань» [70].

Практично у такий же спосіб право на приватність визначається у статті 17 Міжнародного пакту про громадянські та політичні права від 1966 р.: «Ніхто не повинен зазнавати свавільного чи незаконного втручання в його особисте і сімейне життя, свавільних чи незаконних посягань на недоторканність його житла або таємницю його кореспонденції чи незаконних посягань на його честь і репутацію. Кожна людина має право на захист закону від такого втручання чи таких посягань» [71].

У ч. 1 ст. 8 Конвенції про захист прав людини і основоположних свобод 1950 р. право на приватність сформульовано наступним чином: «Кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції» [72]. У Конвенції, на відміну від Декларації та Міжнародного пакту, не тільки визначено суть права на приватність, його складові, у ч. 2 ст. 8 передбачено випадки, коли держава може втручатись у здійснення цього права. Тобто право на приватність не є абсолютним і в обґрунтованих випадках, з додержанням законодавчих вимог, може піддаватись обмеженням: «Органи державної влади не можуть втручатись у здійснення цього права, за винятком

випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб» [72].

Зазначені акти стали основою для розробки поняття права на приватність на національних рівнях. У Конституції України формула приватності закріплена у статті 32: «Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України» [73]. Але обмежувати право на приватність тільки статтею 32 не варто. Гарантія недоторканності житла, про що йде мова у статті 30 Основного Закону України, та гарантія таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції [73], що визначається статтею 31 Конституції України, також є важливими аспектами права на приватність. Тому за своє суттю право на приватність не обмежується одним спрямуванням, а може включати ряд ознак, звідси і різноманітні підходи до тлумачення на доктринальному рівні.

Размєтаєва Ю. С наголошує: «Визначення самого права містять спектр розумінь – від недоторканості приватного життя особи, яке охоплює фізичну та душевну недоторканість, та захищеної індивідуальності до можливості поділитися інформацією із самостійно обраними особами, права бути залишеним у спокої, контролю над персональною інформацією тощо» [74, с. 235]. Право на приватність виходить за межі виключно захисту від незаконного втручання. Поняття цього феномену може включати й неконкретизований перелік інших складових.

Примітно, що ЄСПЛ у своїй практиці не вдається до визначення вичерпного змісту поняття права на приватність, про що зазначається у п. 29 рішення «Німіц проти Німеччини»: «…було б надто обмежуюче звужувати це поняття «внутрішнім колом», в якому індивід може жити власним особистим життям, яке він вибирає, і виключити з нього цілком зовнішній світ... право встановлювати та розвивати стосунки з іншими людьми» [75]. Із зазначеного рішення ЄСПЛ можна дійти висновку, що приватність – це не тільки про

можливість відокремити себе від навколишнього світу, це й про певне інтегрування у суспільство. Тому, варто залишити простір для тлумачення цього права. Адже, надавши поняттю конкретного визначення, є загроза протилежних явищ: надмірного узагальнення, або надмірного обмеження. Як розширення, так і звуження суті може призвести до складнощів застосування. Доречним видається закріплення саме меж втручання держави у право на приватність, а не суті цього поняття. Це може сприяти більш широкому захисту індивідів в конкретній ситуації.

3.2. Зв'язок між правом на приватність та правом на захист персональних даних

Право на приватність, як було зазначено у попередньому розділі, включає ряд окремих складових, які можуть розглядатись як самостійні права та на них поширюються окремі (додаткові) гарантії. Широке коло аспектів, яке визначає право на приватність, на перший погляд робить очевидним, що право на захист даних має тісний зв'язок із правом на приватність, тому є складовою частиною права на приватність. Однак існує значна академічна дискусія щодо зв'язку або його відсутності між правом на приватність та правом на захист даних [76, с.23-24], - зазначає Шрадха Кульхарі із посиланням на наукові праці Глорії Гонзалес Фустер, Рафаеля Галлерт, Сержа Гатвірз, а також ряду інших дослідників. В українському законодавстві та міжнародних актах, до яких Україна приєдналась, зокрема у згадуваній Конвенції та Пакті про політичні права право на захист ПД окремо від права на приватність не виділяється. Натомість в Хартії основних прав Європейського Союзу є дві окремі статті, які незалежно одна від одної визначають право на повагу приватного життя та право на захист інформації особистого характеру, тобто ПД. Стаття 7 Хартії закріплює право на приватність: «Кожна людина має право на повагу до його приватного і сімейного життя, на недоторканність житла і таємницю кореспонденції» [77]. У статті 8 окремо

йдеться про те, що: «Кожна людина має право на захист інформації, що стосуються особистого характеру» [77].

Глорія Гонзалес, робота якої присвячена аналізу походження права на захист ПД, вважає, що розробка Хартії дала змогу на рівні ЄС посилити систему захисту основних прав та закріпити деякі права, які вважалися «неіснуючими», але були необхідними у світлі тодішніх потреб. У цьому контексті побачило світло право на захист ПД, встановлене у 2000 році у Хартії [78, с.206].

Виокремлення права на захист ПД дала поштовх для його детального окремого аналізу. Ивонн Мак-Дермотт стверджує, що право на захист ПД пов'язано із цілим рядом фундаментальних прав, в першу чергу із правом на приватність, а також правом на свободу думки, совісті та релігії; свободи самовираження та іншими, але для права на захист ПД характерними є окремі елементи, які притаманні виключно йому, що і виправдовують його виокремлення як самостійного право [79, с.2]. Такими елементами із посиланням на ч.2 ст. 8 Хартії авторка визначає основні вимоги до обробки ПД: відповідність меті, згода особи або законні підстави для обробки ПД, право на доступ до ПД [79, с.2]. Я погоджуюсь із тим, що право на захист ПД варто сприймати як таке, що пропонує додаткові гарантії для особи, тому може розглядатись як самостійне.

ЄСС розглядалась об'єднана справа «Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen», в якій було надано оцінку праву на приватність та праву на захист ПД [80].

Обоє заявників займаються сільськогосподарським бізнесом і обидва заперечували проти публікації їхніх даних, як отримувачів сільськогосподарських субсидій. У даній справі було проведено аналіз взаємозв'язку права на приватність і права на захист ПД. У висновку зазначено, що у справі посилаються на два окремі права: класичне право (захист приватності згідно зі ст. 8 ЄКПЛ) та більш сучасне право (Конвенції № 108). З точки зору Хартії, подібні права визначені відповідно у статтях 7 та 8. Суд визнав тісний зв'язок між основним правом на приватне життя та правом на захист

даних» [80]. На жаль, у даному рішенні не було з’ясовано відмінності між «класичним правом» та «більш сучасним правом», та все ж важливим є зазначення, що ці два права не є повністю тотожними. Дуже влучно відзначено «більш сучасне право». Генеральний Адвокат нібито підкреслює, що право на захист ПД є відповіддю на нові виклики, які постають у зв’язку із суспільним розвитком, але в той же час пов’язане із «класичним правом».

3.3. Межі втручання держави у право на приватність

У попередньо зазначених статтях Загальної декларації прав людини, Конвенції про захист прав людини і основоположних свобод визначення права на приватність сформульовано через категорію «має право на повагу», «має право на захист закону». У світлі зазначених формулювань науковці часто зазначають, що структурно положення, котрі визначають право на приватність, до прикладу стаття 8 Конвенції, складаються з двох частин: у першій визначено свободи, які підлягають захисту; у другій викладено умови, за яких держава може правомірно втручатися у здійснення права (тобто мету та умови його легітимного обмеження) [81, с.230-231]. Ключовим фактором у другій частині є саме правомірність втручання держави у право на приватність. Тому держава має право обмежити право на приватність виключно за певних умов.

Одним із найпоширеніших підходів при визначенні можливості обмеження права на приватність та правомірності такого обмеження є застосування «трьохступеневого»/«трьохскладового тесту». Дахова І. І. у своїй роботі «Обмеження реалізації прав і свобод людини: конституційне регулювання та практика Європейського суду з прав людини» виокремлює основні складові зазначеного тесту: по-перше, чи була можливість обмеження реалізації права передбачена законом; по-друге, чи є легітимною мета такого обмеження і, по-третє, чи є таке обмеження необхідним у демократичному суспільстві» [82, с. 18].

Розглянемо більш детально складові трискладовго тесту. Категорія «передбачений законом», «згідно із законом» набула широкого тлумачення у

практиці ЄСПЛ. У справі «Олександр Волков проти України» (Заява № 21722/11) Суд, посилаючись на свої попередні дослідження щодо категорії «згідно із законом» зазначив:

«Вислів «згідно із законом» вимагає, по-перше, щоб оскаржуваний захід мав певне підґрунтя у національному законодавстві; він також стосується якості закону, про який йдеться, вимагаючи, щоб він був доступний для зацікавленої особи, яка, окрім того, повинна мати можливість передбачити наслідки його дії щодо себе, та відповідав принципові верховенства права. (…) ця фраза передбачає, inter alia, що формулювання національного законодавства повинно бути достатньо передбачуваним, щоб дати особам адекватну вказівку щодо обставин та умов, за яких державні органи мають право вдатися до заходів, що вплинуть на їхні конвенційні права» [83].

Із зазначеного доходжу висновку, що категорія «згідно із законом» має такі ознаки: (1) чіткість процедури, яка підлягає дотриманню при її застосуванні; (2) передбачуваність для застосування.

Забезпечення передбачуваності застосування правових норм, встановлюваних обмеженнями згідно Рішення Конституційного Суду України від 29 червня 2010 року № 17-рп/2010 означає, що обмеження будь-якого права повинне базуватися на критеріях, які дадуть змогу особі відокремлювати правомірну поведінку від протиправної, передбачати юридичні наслідки своєї поведінки [84].

Другий елемент трискладового тесту легітимність мети обмеження, втручання [82, с. 18]. Згідно ст. 8 Конвенції легітимним може визнаватись втручання в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров’я чи моралі або для захисту прав і свобод інших осіб [72]. При обмеженні права на приватність держава захищає певні цінності, які також є вагомими та важливими у демократичному суспільстві. Однак це не означає, що перелічені суспільні цінності повинні превалювати над правом окремої особи на приватність.

Легітимність мети обмеження повинна визначатись через оцінку пропорційність заходів. Дахова І.І. підкреслює, що пропорційність визначає сумірність між здійсненням основного права та необхідністю його обмежень. Саме принцип пропорційності забезпечує обґрунтований і легітимний характер обмежень основних прав [82, с.20]. Деякі автори визначають пропорційність як сукупність норм, що визначають необхідні та достатні умови для обмеження захищеного права. Інші визначають його як принцип, що обмежує здійснення державних повноважень. Отже, принцип виконує подвійну роль: він захищає основні права та забезпечує обґрунтування для їх обмеження [85, с.117].

Проаналізувати, чи дотримано критерій пропорційності можна завдяки чотирьом запитанням: 1. Чи відповідає дія щодо втручання у сферу основного права, законній меті? (Попереднє запитання) 2. Якщо так, чи адекватна дія для досягнення цієї мети? 3. Якщо так, то чи потрібна дія для цієї мети, іншими словами, чи не існує жодної іншої дії, яка б однаково ефективно використовувалась для досягнення законної мети та відбулось менше втручання у сферу основного права? 4. Якщо так, то чи є дія [втручання] пропорційною стосовно основних прав, що обмежуються? [41]. Усі ці питання, завдяки яким можна визначити, чи дотримано тест на пропорційність, слід розглядати послідовно у рамках загальної оцінки, яка повинна збалансувати інтереси держави, суспільства та конкретного індивіда/індивідів, у права яких здійснюється втручання.

Переходячи до останнього критерію трискладового тесту – необхідності втручання. Необхідність можна розуміти як негайну, крайню потребу держави. Справа Шабо та Віші проти Угорщини від 12 січня 2016 року [86] є яскравим прикладом визначення дотримання умов необхідності втручання.

Згідно обставин справи у 2011 р. в Угорщині було створено Антитерористичну групу, особливість повноважень якої становили пошук та спостереження за будинком, відкриття листів та посилок, а також перевірка та запис вмісту електронних чи комп’ютеризованих комунікацій. Проблема полягала в тому, що всі ці дії здійснювались без згоди осіб, яких це могло

стосуватись. Заявники, працівники неурядової, контролюючої організації, скаржились, що вони можуть бути піддані таємному нагляду, який здійснюється в цілях національної безпеки. Вони наголошували, що в цій ситуації є простір для зловживань, адже таємний нагляд може бути необґрунтованим і також немає належних гарантій судового захисту [86].

У рішенні по цій справі судом встановлено порушення статті 8 Конвенції. Суд у пункті 68 Рішення не заперечує впровадження новітніх технологій з міркувань безпеки, зазначаючи: «Для Суду закономірним наслідком форм сучасного тероризму є те, що уряди вдаються до передових технологій для попередження таких атак, включаючи масовий моніторинг комунікацій» [86].

Але в пункті 73 Рішення Суд наголошує на дотриманні вимог необхідності: «…міра таємного нагляду може бути визнана такою, що відповідає Конвенції тоді, коли в цілому необхідна із загальних міркувань для захисту демократичних інститутів, і більше того, якщо це вкрай необхідне із конкретних міркувань для отримання життєво важливої інформації в окремій ситуації» [86]. Суд встановив, що мотиви застосування заходів спостереження не були виправданими, адже не було «крайньої необхідності» для їх застосування. Примітно, що суд вдається до виправдання застосування захисту саме для «демократичних інститутів». Тим самим підкреслюючи, що не задля кожної мети держава може вдаватись до обмежень, а виключно, коли є потреба у захисті демократичних інститутів [86].

Важливими є також гарантії захисту від порушення прав, в першу чергу завдяки судовому нагляду. «Однак в угорському законодавстві жодних повідомлень про будь-які заходи не передбачено. Цей факт у поєднанні з відсутністю будь-яких формальних засобів захисту у разі зловживань свідчить про те, що законодавство не відповідає забезпеченню належних гарантій» [86], – підсумовується у рішенні Суду. Таким чином, держава повинна приймати пропорційні рішення про обмеження права на приватність та визначати гарантії захисту права на приватність до початку виконання такого рішення.

Застосування заходів пост фактум може бути ускладнене та не ефективне. Також виникає ризик розширеного тлумачення органами державної влади

принципу пропорційності застосованих заходів. Після впровадження обмежувальних заходів органи державної влади можуть вдатись до виправдання своїх дій та відповідно до свободи тлумачення необхідності заходів, згідно чого певні обмеження будуть позиціонуватись як менш інвазивні.

ЄСПЛ у справі A.-M.V. v. FINLAND (Application no. 53251/13) звернув увагу на те, що процесуальні гарантії, доступні для особи, будуть особливо суттєвими при визначенні того, чи держава, встановлюючи нормативно-правову базу, залишалась у межах своєї свободи розсуду. Зокрема, Суд повинен перевірити, чи був процес прийняття рішень, що призводить до заходів втручання, справедливим та таким, щоб забезпечити належну повагу інтересам, захищеним особою статтею 8 [87].

У даній справі Суд звернув увагу, що він не намагається перебрати на себе функції держави, свобода розсуду неминуче повинна залишатися за національним органам влади, котрі через прямий і постійний контакт із важливими інструментами своїх країн в принципі мають кращі можливості, ніж міжнародний суд, для оцінки місцевих потреб та умов. Та все ж Суд буде здійснювати оцінку межі свободи розсуду, яка може змінюватися залежно від характеру права, про яке йдеться в Конвенції, його значення для людини та характеру обмеженої діяльності, а також характеру мети, яку переслідують обмеження [87]. Підхід до врахування свободи розсуду національних органів стає ще сильнішим у тих випадках, коли заходи вводяться з метою захисту національних інтересів. У таких ситуаціях Суд неодноразово повторював, що національні органи влади повинні судити самостійно про те, що необхідно для захисту внутрішніх інтересів. Суд у таких справах зосереджений на аналізі правових гарантій. Наявність належних гарантій проти зловживань з боку державних органів – це спосіб забезпечити захист прав людей [85, с.118].

Не втручання у питання встановлення та застосування обмежувальних заходів також має сенс з тієї позиції, що лише в рідкісних випадках вжиті заходи є абсолютно ірраціональними і завжди можливо стверджувати, що вони придатні і необхідні для досягнення законної мети [88, с.296], зазначає Погребняк С.П.,

аналізуючи думки з цього приводу в літературі. По суті, набагато поширенішими є випадки, в яких перевірка пропорційності заходів зводиться до порівняння інтенсивності втручання з метою, яка переслідується. Іншими словами, інтенсивність обмежень не повинна бути надмірною щодо легітимних потреб та інтересів, до забезпечення яких прагне конкретне обмеження [88, с.296]. Використання ТРО буде, на мою думку, надмірним, коли метою такого застосування проголошується забезпечення громадського порядку. При цьому, за аналізом попередніх звітів, ТРО встановлюються у містах із мінімальним рівнем злочинних проявів. Населення ж відповідної місцевості буде піддаватись постійному нагляду. Звідси встановлені заходи обмежень є надмірними у наведеній ситуації.

Адже, як цілком слушно зазначає Акін Унвер у роботі «Політика цифрового спостереження, національна безпека та приватність», що демократії, зрештою, повинні створити баланс конфіденційності нагляду, який відповідає політичній культурі країни [33, с. 16-17]. Увага до політичних умов не є випадковою. За останні десять років, наприклад, Франція неодноразово ставала жертвою терактів, що мало за собою загибель сотні людей. Тому й питання безпеки в цій державі може стояти більш гостро, а відповідно заходи забезпечення можуть бути суворішими у порівнянні із іншими державами.

Важливим є саме попередження злочинних актів. Коли ж органи державної влади вдаються до запровадження заходів безпеки, зокрема, впровадження ТРО постфактум, після певних подій, які призвели до втручання в національну чи громадську безпеку постає питання необхідності та доцільності таких заходів. Я схильна до думки, що в більшості випадків таке застосовування не виправдовує себе.

Складні події, що призводять до жертв, викликають загальну стурбованість та страх повторності чергової атаки. Тому в такі періоди органи державної влади можуть вдаватись до більш широкого застосування запобіжних заходів в місцях, де мали місце жахливі події, зокрема до використання ТРО. Хоча як пише професорка кримінології Рашель Армітаж: «використання технологій

відеоспостереження та розпізнавання обличь блокує для злочинців тільки певний простір можливості для злочинів, і тому злочинці автоматично виберуть ціль в іншому місці. Іншими словами, злочинність рухається, а не зменшується» [89, с. 3]. Тому для ефективної боротьби зі злочинністю видається необхідним вдаватись також і до інших попереджувальних заходів, які при цьому можуть в меншій мірі мати вплив на приватну сферу життя або хоча б вплив на істотно меншу кількість населення.

Безумовно «…у демократичному суспільстві не існує простого рішення для вирішення конфліктів між суспільними інтересами та особистими претензіями (…). Головне, щоб рішення органів влади в кінцевому підсумки «не призвели або до якоїсь форми диктатури з одного боку, або до анархії з іншого» [90].

***

У розділі окреслено підходи до закріплення поняття приватності у міжнародних актах, зокрема, у Загальній декларації прав людини, Міжнародному пакті про громадянські і політичні права, Конвенції про захист прав людини і основоположних свобод, також проаналізовано практику ЄСПЛ та національне законодавство.

Наведено аналіз підходу до визначення права на приватність в доктрині. Зазначено, що не варто вдаватись до визначення вичерпного переліку складових права на приватність, більш доречно встановити межі втручання держави у приватність індивіда.

Запропоновано вдаватись до трискладового тесту на визначення необхідності втручання держави та меж такого втручання, та брати до уваги баланс між приватними та публічними інтересами.

Акцентовано увагу на важливості забезпечення прозорості ТРО та підзвітності населенню про результати їх впливу на становлення безпеки.

Зазначено, що приватність не виключається тільки власною домівкою, а може мати місце і в публічних місцях. Безумовно рівень приватності в публічних

місцях є відмінним. Для визначення рівня приватності в публічних місцях пропонуємо звернутись до американської доктрини «розумні очікування приватності».

РОЗДІЛ 4. РОЛЬ ТЕХНОЛОГІЙ РОЗПІЗНАВАННЯ ОБЛИЧ В ПЕРІОД COVID-19

4.1. Запровадження заходів відстеження та спостереження для виявлення та карантину осіб, заражених COVID-19

Якщо попередньо технології розпізнавання обличь в основному використовувались з метою запобігання злочинним діями та становленню безпеки, то у зв’язку з пандемією вони також набули нового завдання – запобігання поширенню коронавірусної хвороби. Тому не дивно, що пандемія і зростання технологій розпізнавання обличчя, а також ряд інших технологій стеження зараз тісно переплітаються, та останні використовуються як частина протидії першим.

В Україні популярністю користується технологія відстеження даних про місцезнаходження особи. Для цього було запущено застосунок «Дій вдома», завдяки якому визначається місцезнаходження особи в момент, коли вона робить фото. Кабінет Міністрів України зазначає, що використання застосунку здійснюється тільки за згодою користувача. В основному даний застосунок використовується для перевірки дотримання особою правил ізоляції [91].

Держави-члени ЄС також запровадили національні програми стеження [92]. Європейська комісія впроваджує застосунок щодо взаємодії, що зв’язує національні програми в ЄС, має на меті повністю використати потенціал мобільних застосунків для відстеження та попередження контактів, щоб допомогти зупинити поширення COVID-19 у Європі [93].

8 квітня 2020 року Європейська Комісія видала Рекомендацію 2020/5189, пропонуючи низку кроків та заходів для у вироблення загального підходу до використання цифрових технологій та даних у відповідь на кризу [94]. В Рекомендації зазначено, що цей підхід повинен бути ефективним для підтримки компетентних національних органів, зокрема охорони здоров'я, влади та політиків, надаючи їм достатньо точних даних, щоб зрозуміти поширення вірусу

COVID-19, а також його наслідки. Подібним чином ці технології можуть надати громадянам змогу брати участь ефективні та більш цілеспрямовані заходи соціального дистанціювання [94]. Водночас Європейська комісія наголошує, що запропонований підхід має на меті підтримати цілісність єдиного ринку та захист основних прав і свобод, особливо прав на приватне життя та захист персональних даних [94].

Європейською Комісією встановлено також і вимоги до застосування застосунків, зокрема вимоги прозорості налаштувань, цілісності, автентичності та конфіденційності даних, гарантії, що забезпечують повагу основних прав та запобігання стигматизації, технічні вимоги щодо відповідних технологій, закінчення терміну вжитих заходів та видалення персональних даних, отриманих за допомогою цих заходів та ряд інших вимог [94].

Окрім впровадження застосунків відстеження місцезнаходження осіб, популярністю користується і розробка технологій вимірювання температури. З самого початку стрімкого поширення коронавірусної хвороби висока температура визначається основною ознакою захворювання [94]. Тому звичною процедурою для того, що потрапити в заклад, установу, продуктовий магазин та ряд інших установ та організацій є проходження перевірки температури. Поряд із використанням звичних термометрів, застосовуються також камери спостереження з контролем температури.

В Києві минулого року на початковому етапі впровадження заходів запобігання поширенню коронавірусної хвороби, ряд видань писали про те, що столиця закупила камери, які розпізнають обличчя і вимірюють температуру тіла [95]. Така закупівля дозволила б оперативно визначати людей з підвищеною температурою тіла у супермаркетах, аптеках та інших місцях масового скупчення людей [95]. Але декількома днями пізніше на офіційному майданчику електронної системи публічних закупівель України ProZorro з’явилась інформація, що при моніторингу закупівлі виявлено порушення, тому договір було розірвано [96].

У лютому цього року на онлайн-платформі «Офіційний портал Києва» знову з'явилась інформація про закупівлю камер відеоспостереження для київського метрополітену. У релізі зазначається, що нові камери мають інтелектуальний функціонал: 140 оглядових камер, 90 – із функцією розпізнавання облич, 75 камер з функціями розпізнавання облич та термального скринінгу [97]. Техніка слугуватиме як для розшуку людей, розкриття та попередження злочинів, так і для моніторингу дотримання киянами та гостями столиці вимог профілактичних та протиепідемічних заходів під час пандемії COVID-19 [97]. Які наслідки матиме виявлення підвищеної температури у особи, не зрозуміло. Інформація на онлайн-платформі «Офіційний портал Києва» є надто стислою, жодної відсилки до актів, які б регулювали обробку ПД, отриманих завдяки технологіям з функціями розпізнавання облич та термального скринінгу немає. Таке хаотичне встановлення нової технології є прямим порушенням права особи на приватність та права на захист ПД. На жодному офіційному ресурсі органів державної влади та місцевого самоврядування м. Києва немає зазначення про те, на яких саме станціях київського метрополітену буде встановлено нові технології. Пересічний користувач метрополітену позбавлений можливості знати, що він перебуває в постійному моніторингу з боку органів державної влади та місцевого самоврядування, яким чином будуть використані ПД залишається також відкритим питанням.

Потребує також уточнення питання на скільки точними є технології, свідчень про це на інформаційному ресурсі взагалі немає. Зважаючи на карантинні обмеження, в метрополітені особи постійно перебувають в масках, це дещо інший, очевидно складніший рівень розпізнавання облич. Деякі частини обличчя залишаються все ж таки відкритими, можливо алгоритм працює таким чином, що може провести розпізнавання особи за відкритою частиною обличчя. Але це тільки здогадки. Тому обов'язковим вважаю розробку Рекомендацій, в яких буде розкрито технічні характеристики технологій, а також буде встановлено процедуру обробки та захисту ПД.

Отже, в період карантинних обмежень в першу чергу набули поширення технології відстеження місцезнаходження осіб та ТРО із здатністю визначати температуру тіла людини.

Чи ймовірно, що ці широко застосовні технологічні ресурси будуть зменшені, коли загроза пандемії пройде, або вони залишаться частиною нового «звичного життя» з метою превентивних заходів щодо безпеки?

Джое Масоді пише: «Технологічні компанії можуть використовувати страх, що виникає внаслідок кризи, щоб поширити більше технологій спостереження, пропонуючи їх урядам як рішення для контролю за поширенням вірусу» [98]. Я погоджуюсь із тим, що страх може виступати тригером прийняття необґрунтованих рішень. Проте в більшості видається, що такі дії (встановлення технологій спостереження загалом та ТРО зокрема) є цілеспрямованими і держави чітко усвідомлюють, що з допомогою технологій спостереження та зокрема ТРО зможуть відслідковувати дії, поведінку населення. Карантинні ж обмеження стали тільки підставою для їх впровадження та подальшого застосування.

4.2. Особливості та тенденції регулювання технологій розпізнавання облич та інших технологій відстеження в окремих державах в період встановлення карантинних обмежень

У попередньому розділі на прикладі України зазначено, що регулювання нововведених технологій відсутнє або воно є мінімальним. На рівні ЄС прийнято Рекомендації. Згідно ст.288 Договору про функціонування ЄС: «Рекомендації та висновки не є зобов'язальними» [99]. Тобто Рекомендації прийняті Європейською комісією не мають обов'язкової сили для держав членів, тому в питанні регулювання превентивних заходів у зв'язку з коронавірусною хворобою значення мають саме встановлені державами стандарти.

Італія була однією із перших європейських країн, яка стикнулась із випробуванням коронавірусною хворобою, відповідно їй одній із перших

довелось реагувати на загрозу поширення коронавірусної хвороби шляхом прийняття актів, які регулюють процедури впровадження карантинних обмежень та запровадження заходів безпеки.

На початку березня 2020 р. орган захисту даних Італії опублікував прес-реліз, в якому наголосив, що за стеження та збір інформації щодо симптомів, характерних для коронавірусу, та про останні пересування кожної людини відповідають медичні працівники та система цивільного захисту, тобто суб'єкти, яким доручено забезпечити відповідність нещодавно прийнятим правилам охорони здоров'я [100]. Таким чином, орган захисту даних Італії визначив відповідальних за обробку ПД та уповноважених збирати та обробляти дані про стан здоров’я, а також інші дані, пов’язані з поширенням коронавірусної хвороби. Епідемічна криза тільки посилювалась, тому уряд Італії змушений був вдаватись до впровадження технологічних рішень – застосування програми відстеження контактів.

30 квітня 2020 р. уряд Італії видав Декрет №28, як зазначено у ст. 6 цього Декрету, з єдиною метою захищати людей, їх здоров'я через заплановані заходи профілактики та створити єдину національну платформу для управління системою попередження суб’єктів завдяки добровільному встановленню спеціального застосунку на телефоні [101]. В Декреті чітко прописано, що ПД, зібрані за допомогою мобільного застосунку належатимуть Міністерству охорони здоров’я, яке координуватиме з суб’єктами, які працюють у Національній службі цивільного захисту, з Вищим інститутом охорони здоров’я та з акредитованими державними та приватними структурами, що діють у складі Національної служби охорони здоров’я, відповідно до відповідних інституційних повноважень та не будуть оброблятися для інших цілей, за винятком єдиної обробки в сукупній або анонімній формі для наукових або статистичних цілей [101]. Згідно Декрету також гарантується, що ПД будуть зберігатися протягом встановленого Міністерством охорони здоров'я строку, суворо необхідного для відстеження, і, згодом, автоматично видалятися. Однак цей період не триватиме більше, аніж до 31 грудня 2020 року [101]. У ч.2 ст.6

Декрету визначено, що перш ніж активувати програму користувачі отримують чітку та прозору інформацію для досягнення повної обізнаність, зокрема, про цілі та операції обробки, про методи псевдонімізації та період зберігання даних; на постійній основі гарантується конфіденційність, цілісність, доступність та стійкість систем та гарантуються права суб'єктів, визначені ЗРПЗД [101].

Уряд Італії встановив чіткі рамки для впровадження заходів відстеження контактів з метою швидкого та безпечного врегулювання епідеміологічної ситуації, що склалась. Прийнятий Декрет визначив основні вимоги, які повинні застосовуватись під час обробки ПД.

Але не всі впроваджені в Італії заходи були прозорими та відкритими. В муніципалітеті Комо почали встановлювати ТРО, які не мали законних підстав для використання [102]. Варто зазначити, що ці технології планували використовувати безвідносно до коронавірусної хвороби [103]. Та все ж складна епідеміологічна ситуацію тільки пришвидшила тестування та впровадження ТРО. В кінцевому результаті, як зазначає видання Privacy International із посиланням на місцеві засоби масової інформації тестування ТРО в муніципалітеті Комо не дало очікуваних результатів, камери не змогли розпізнати обличчя, проте не зрозуміло, наскільки довго діяло тестове випробування ТРО [102]. Але сам факт впровадження та тестування ТРО в період критичної епідеміологічної ситуації звертає знову ж таки до думки, що в кризових ситуаціях обмеження прав людини може позиціонуватись, як допустимі кроки і тому не сприймається так гостро.

Більшість європейських держав вдались до розробки та впровадження застосунків для відстеження контактів. В основному при використанні застосунків збирались дані про місце перебування особи або взагалі не було потреби вказувати свої дані [104]. Та є ряд держав, які впроваджували застосунки для моніторингу дотримання карантинних обмежень і окрім геолокації, використовували також функцію розпізнавання облич. Наприклад, польський застосунок «Kwarantanna domowa» (домашній карантин) повинен використовуватись особами, які перебувають на карантині, зазначається в Акті

від 2 березня 2020 року [105]. Обов'язок встановлення та використання застосунку не поширюється тільки на осіб з вадами зору або осіб, котрі зробили заяву, що не є абонентом або користувачем мережі телекомунікацій або не мають мобільного пристрою, що дозволяє встановлення цього програмного забезпечення. Заява про неможливість встановити застосунок складається із умовою про повне розуміння кримінальної відповідальності за неправдиве повідомлення [105].

Завдяки цьому застосунку польські органи влади мають можливість відстежувати місцезнаходження осіб та періодично вимагати від них завантажити селфі, щоб підтвердити свою присутність у будинку, де особа має перебувати на карантині. Неможливість зробити та завантажити селфі або виконати інші дії, які вимагає застосунок, автоматично відправляє сповіщення органам влади, які мають право перевірити, чи особа перебуває за визначеним нею місцем карантину [105].

З Інструкції використання застосунку випливає, що право на доступ до ПД мають органи поліції (центральні та місцеві), воєводи та виключний перелік організації, що працюють над програмним забезпеченням, і Центр здоров’я [106]. Мета застосунку перевірити дотримання карантинних вимог. Перевірку дотримання карантинних вимог здійснюють органи поліції, моніторинг вчасності направлення фотографії також здійснюється органами поліції. З якою метою доступ до ПД, право обробляти ПД надається іншими інституція не є очевидним.

При цьому володільцем даних є Міністерство діджитизації Польщі, яке уповноважене зберігати ПД протягом строку позовної давності, який в Польщі становить 6 років. Зберігаються ПД за винятком фотографій, які видаляються при деактивації облікового запису [106]. Період зберігання ПД чітко прописаний, проте протягом 6 років доцільності використання застосунку вже може не бути, правовідносини між суб’єктами можуть бути припинені, проте дані продовжуватимуть зберігатись. Застосунок не збирає дані, які стосується стану здоров’я особи, симптомів коронавірусної хвороби, які в подальшому

могли б становити інтерес для наукових, дослідницьких, статистичних цілей. Тому 6 років для зберігання даних є занадто розширеним періодом і видається не релевантним встановленій меті використання ПД.

Аналізуючи застосунок з точки зору надання прав суб'єктам даних, варто зазначити, що згідно Інструкції суб'єкт даних наділений широким колом гарантій для захисту ПД, зокрема має право в будь-який час отримати доступ до ПД, вимагаючи їх виправлення, подавати запити проти обробки даних, запити на обмеження їх обробки, подавати скарги до контролюючого органу [106].

При всіх гарантіях, правах, якими наділяється суб'єкт даних, визначеній меті застосування застосунок зазнав критики щодо його транспарентності. Александра Бартожко звертає увагу, що застосунок має ширше коло функції, ніж зазначено в нормативних актах на урядовому веб-сайті або тих, що додаються до програми. Ці функції можна визначити на основі аналізу з дозволів у онлайн-магазині Google Play/App Store та від ІТ-експертів, які читають коди [107, с.9]. Із посиланням на фахівців у сфері ІТ-технологій зазначається про те, що програма інтегрована з бібліотеками Facebook та медіаплеєром. Міністерство ж не надало відповідь, чи додаток якимось чином взаємодіє з інфраструктурою Facebook [107, с.9].

Критиці піддається саме технологічне рішення використання застосунку. Пояснюється це тим, що використання застосунку робить громадян, які живуть у і без того тривожній ситуації, більш напруженими та тривожними. Пропонуючи новий інструмент контролю, демократичні уряди повинні врахувати, чи є нав'язливі засоби єдиним способом досягнення цілей. Польський уряд ще не надав жодних доказів того, що «Kwarantanna domowa» є розумною та ефективною формою боротьби із коронавірусною хворобою. Наскільки свідчить досвід користувачів, замість того, щоб сприяти боротьбі з пандемією, це ускладнює повсякденне життя поліції та громадян, які перебувають у карантині, підкреслюючи, що держава ставиться до них із реальною підозрою. Відзначається також і велика кількість помилок, які допускає застосунок, а зі збільшенням помилок зростає і недовіра до впровадженого урядом заходу та до

його спроможності та готовності вирішити епідеміологічну кризу [107, с.12-13]. З огляду на зазначене можна дійти висновку, що системі бракує прозорості, точного розуміння суспільством можливостей та функцій технології і врахування громадської думки щодо ефективності та необхідності технології.

Деякі держави пішли далі відстеження завдяки застосункам. У Франції, Сполученому Королівстві, США та Італії, як повідомляє видання «Financial Times», почали використовувати дрони для відстеження, чи дотримується населення соціального дистанціювання [108]. Безпілотники зазвичай обладнані камерами, що дозволяють пілотам керувати ними. Запис безпілотниками зображень людей може становити вторгнення в приватне життя. Більше того на безпілотник також може бути встановлена низка інших програм та бортових пристроїв, здатних збирати та обробляти ПД, що призводить до потенційно серйозних порушень права громадян на захист їхнього приватного життя та їх даних [109, с.185]. Потенційно безпілотник може бути обладнаний і камерами із функцією розпізнавання облич.

У правозахисних організацій та органу захисту даних у Франції застосування поліцією безпілотників викликало занепокоєння та призвело до ініціації процедури заборони даного пристрою [110]. Дані щодо технічних характеристик пристрою неможливо знайти у вільному доступі, відповідно населення, яке піддається спостереженню завдяки безпілотникам не має жодних відомостей про функціонал технології і що більш критично не має інформації, як використовуються їх дані.

Президент органу захисту даних у Франції ініціював проведення перевірки використання безпілотників. Для цього ним було направлено ряд запитів до Міністерства внутрішніх справ, а також поліцейських відділень різних рівнів Франції. Міністерства внутрішніх справ у своїй відповіді зазначило, що ними використовуються безпілотники, оснащені камерами, і основна мета такого використання це перевірка дотримання встановлених заходів обмежень для запобігання поширенню коронавірусної хвороби. Також у відповідь йшла мова про те, що безпілотники використовуються для спостереження за

демонстраціями, а також виконання інших функції поліції, пов’язаних зокрема із запобіганню торгівлі людьми, наркотиками та в загальному для посилення заходів безпеки у країні. Пізніше Президент органу захисту даних у Франції випробував безпілотник, здійснивши на ньому політ [110]. Висновок, якого він дійшов: «можна встановити осіб, яких знімали за допомогою пристроїв цього типу. (…) ця обробка ПД не базується на якій-небудь правовій основі» [110].

Правозахисні організації звернулись до суду для вирішення питання, чи все ж таки було втручання держави у право на приватність шляхом використання безпілотників. Суд у своєму рішенні звернув увагу на принцип пропорційність заходів, які можуть бути застосовані і пункті 4 рішення зазначив, що у поточний період надзвичайної ситуації з охороною здоров’я різні компетентні органи влади повинні вжити будь-яких заходів, які можуть запобігти або зменшити наслідки епідемії, для захисту здоров’я населення. Ці заходи, які можуть обмежити реалізацію основних прав і свобод, повинні, бути необхідними, відповідними та пропорційними меті охорони здоров'я населення, яку вони переслідують [111].

У процесі аналізу інструкції до безпілотників Судом було встановлено, що безпілотники не мають функції ідентифікації осіб, а також було підтверджено, що жодного відео чи зображень, які містять будь-яку персональну інформацію, не зафіксовано та не збережено. Проаналізувавши Директиву та національне законодавство Суд зазначив, що спірна система нагляду, яка полягає у зборі даних, захопленні зображень безпілотним апаратом, передачі їх, у певних випадках, до центру префектури поліції для перегляду в режимі реального часу та використання їх для виконання функцій поліції - це обробка ПД у значенні Директиви. Тому Суд все ж таки заборонив застосування безпілотних апаратів, звернувши також увагу, що для їх використання не було прийнято спеціального акту, розпорядження чи указу компетентного міністра, який повинен бути затверджений після обґрунтованого та опублікованого висновку державного органу захисту даних [111]. Головною у цьому рішенні є теза про те, що порушенням права на приватність та захист ПД може бути виключно збирання

ПД, навіть, якщо ПД в подальшому не використовуються і практично одразу після отримання видаляються. В будь-якому випадку збирання ПД – є одним із аспектів, етапів обробки ПД. Звідси і необхідність врегулювання процесу використання ПД новим технологіями, що стрімко впроваджуються в період коронавірусної хвороби та вплив яких на права людини не завжди моментально піддається оцінці.

При цьому, варто розділяти безпілотники згідно мети їх потенційного використання в період коронавірусної хвороби, адже від цього може залежати і необхідність та детальність врегулювання їх використання. По-перше, безпілотники можуть бути використані для сприяння виконання правил соціального дистанціювання. По-друге, безпілотники можуть бути обладнані термодатчиками для ідентифікації людей з температурою. По-третє, безпілотники можуть бути обладнані ТРО для відстеження людей, з якими хворий був у контакті [112]. Найбільш очевидним є збирання та обробка ПД осіб у третій ситуації. Стурбованість викликає не стільки запис інформації про конкретних осіб, вжиття до них карантинних заходів, скільки те, що інформація зберігатиметься необмежений час, передаватиметься правоохоронним органам у цілях, що не стосуються громадського здоров'я, або іншим чином відбуватимуться зловживання [112].

Безпілотники з функцією розпізнавання облич не є окремим явищем, пов’язаним із встановленням особи. За своїми функціями та рівнем втручання у права осіб вони можуть розглядатись як доповнення до широкого спектру інструментів, які використовуються для спостереження та встановлення осіб. Важливість становить встановлення правил для впровадження та застосування ТРО, як самої функції, через яку відбувається обробка ПД, безвідносно до того, яке саме технологічне рішення при цьому використовується, статична камера на розі будівлі, безпілотник чи інше.

Штат Вашингтон у США взяв напрямок на комплексне врегулювання ТРО. Саме в період коронавірусної хвороби, коли відбувається стрімке впровадження

технологій, у штаті Вашингтон було прийнято Закон, що стосується використання послуг розпізнавання обличчя.

Найперше в пункті 3а розділу 2 зазначеного Закону наступним чином визначено суть технології: «Функція розпізнавання обличчя» означає технологію, яка аналізує риси обличчя та використовується державним або місцевим органом влади для ідентифікації, перевірки або постійного відстеження осіб на фото або відеозображеннях» [113].

Із визначення випливає, що ТРО можуть використовуватись тільки державним або місцевим органом влади, про використання у приватному секторі не йдеться. Далі акт встановлює фундаментальні вимоги до впровадження ТРО. «Державна установа чи орган місцевого самоврядування, які використовують або мають намір розробити, придбати або використовувати ТРО, повинні подати до законодавчого органу повідомлення про намір розробити, придбати або використовувати ТРО та вказати мету, для якої ця технологія має бути використана» [113]. Дана вимога встановляє принцип відкритості та забезпечує інформування громадськості, починаючи із першого, початкового етапу процесу впровадження технології.

Транспарентність системи має бути забезпечено також завдяки встановленню вимоги підзвітності щодо використання ТРО. Кожен звіт повинен містити щонайменше чіткі та зрозумілі твердження про такі аспекти: найменування ТРО, постачальника та версії; опис загальних можливостей та обмежень технології, види ПД, які використовує технологія; як ці дані генеруються, збираються та обробляються, інформацію про частоту помилкових збігів, та про те, як державна установа чи орган місцевого самоврядування буде вирішувати коефіцієнт помилок, визначений самостійно, що становить більше одного відсотка, а також ряд інших аспектів, які повинні бути обов’язково зазначені у звіті [113].

До процедури прийняття та опублікування звіту також встановлено відповідні умови: (1) остаточний звіт повинен бути прийнятий та повідомлений громадськості принаймні за дев'яносто днів до застосування ТРО, (2) остаточний

звіт повинен бути розміщений на публічному веб-сайті органу, що використовуватиме ТРО, (3) остаточний звіт також передається до законодавчого органу та публікується на його загальнодоступному веб-сайті [113]. Перелічені заходи дають можливість громадськості, потенційним суб'єктам даних розуміння того, хто оброблятиме дані, куди вони можуть звернутись у разі порушення їхніх прав на захист ПД, проаналізувати із доступної інформації, наскільки технологія є безпомилковою та в яких випадках в основному може бути похибка та що основне, мати розуміння для якої саме мети застосовується ТРО.

Закон встановлює випадки, коли може застосовуватись ТРО: (a) отримано ордер, що дозволяє використання ТРО для цілей нагляду та ідентифікації; (b) існують невідкладні обставини; або (c) отримано судовий наказ, який дозволяє використовувати ТРО з єдиною метою виявлення або встановлення зниклої особи або встановлення особи померлої особи. Суд може видати наказ ex parte згідно з підпунктом (c), якщо працівник правоохоронних органів засвідчить це і суд виявить, що інформація, яка, можливо, буде отримана, має значення для пошуку або встановлення зниклої особи або встановлення померлої особи. В інших випадках Закон забороняє використовувати ТРО для здійснення постійного нагляду, проведення ідентифікації в режимі реального часу або в режимі майже реального часу, або для постійного відстеження [113]. Ця норма встановлює рамки з метою захисту населення від тотального, масового спостереження та ідентифікації.

Останнім важливим введенням, на що варто звернути увагу, є обов'язок державного органу або органу місцевого самоврядування, який використовує ТРО для прийняття рішень, що спричиняють юридичні наслідки стосовно фізичних осіб або подібні суттєві наслідки щодо осіб, забезпечити, щоб ці рішення підлягали суттєвому перегляду з боку людини. Рішення, що спричиняють юридичні наслідки стосовно фізичних осіб або подібні суттєві наслідки для фізичних осіб, означають рішення, що призводять до надання або відмови у фінансових та позичкових послугах, житлі, страхуванні, зарахуванні

до освіти, кримінальному судочинстві, можливості працевлаштування, медичних послуг або доступу до предметів першої необхідності такі як їжа та вода, або які впливають на громадянські права людей [113]. При використанні ТРО державний орган або орган місцевого самоврядування повинен забезпечити також і відповідний персонал, який буде відповідальний за перевірку відомостей, встановлених технологіями. Із даного пункту чітко можна зрозуміти, що кінцеве рішення приймається виключно завдяки людському фактору, відповідно і відповідальність несе людина, яка працює із ТРО та тлумачить отримані результати. Перевірка отриманих завдяки ТРО відомостей людиною потенційно може зменшити кількість помилкових рішень, підставою для яких були хибні результати встановлені технологією.

Відійшовши від повної заборони використання ТРО, штат Вашингтон встановив чіткий алгоритм та забезпечив правову основу використання технології державними органами або органами місцевого самоврядування. Згідно виокремлених положень, можна дійти висновку, що Закон встановлює достатньо транспарентний підхід до застосування ТРО, закріплює гарантії для населення та забезпечує їх права та свободи.

Прийняття цього Закону в період епідеміологічної кризи має особливий сенс, зокрема тому, що в період коронавірусної хвороби держава (США) виділяє кошти для створення систем спостереження та збору даних з метою боротьби із поширенням хвороби [114]. Згідно Закону «Про економічну допомогу під час коронавірусу» передбачено фінансування Центру з контролю та профілактики захворюваності в США, і одним із напрямків використання Центром коштів є створення систем спостереження [114]. Тому Закон штату Вашингтон можна розглядати як послідовний крок, який був необхідним як із точки зору реакції на складні епідеміологічні обставини, так і у зв’язку із необхідністю закріплення правової позиції щодо дискусії чи варто взагалі дозволяти використання ТРО.

Ситуація з поширенням коронавірусу стала також тригером і створила ще більше можливостей для функціонування ТРО в Китайській Народній Республіці. Мартін Полрад у виданні «Reuters» пише, що китайська компанія

Hanwang Technology Ltd (Hanvon) заявила, що розробила першу в країні ТРО, яка може ідентифікувати людей, коли вони носять маску, як більшість населення в ці дні через коронавірусну хворобу [115]. У статті Мартіна Полрада також зазначається, що замовником розробки нових технологій є Міністерство суспільної безпеки, у підпорядкуванні якого знаходиться поліція КНР [115]. Тобто, новітні технології можуть мати функції, що дозволяють їм розпізнати обличчя, коли, умовно кажучи є перешкоди, як у даному випадку захисна маска. Більше того, це наводить на думку, що є сформована база зображень індивідів у захисних масках, адже у будь-якому разі захоплене зображення із камер піддається порівнянню із наявним у базі даних.

В Китайській Народній Республіці новітні технології дуже стрімко впроваджуються, як пише видання Deutsche Welle: «Багато нових програм з охорони здоров'я використовують персональні дані та геодані, за допомогою яких можна визначити, де перебуває або перебував громадяни. Це означає, що держава має доступ до інформації дедалі приватнішого характеру і може використовувати її для зміцнення своєї влади» [116].

Таким чином, ТРО в КНР – це рішення, яке виступає інструментом встановлення тотального контролю. Такий підхід не відповідає провідним практикам врахування та запобігання будь-яким ризикам правам людини.

Китайські регулятори почали визнавати проблеми конфіденційності та безпеки, що виникають із швидким розширенням системи ТРО [117]. Національний технічний комітет зі стандартизації інформаційної безпеки оприлюднив пропозицію щодо отримання згоди від суб’єктів даних. Хоча проект, як правило, рекомендує володільцям ПД отримувати чітку згоду від осіб до початку збору даних, у проекті зазначено, що такий підхід недоцільний для збору даних у громадських місцях, як це характерно для розпізнавання обличчя. У цих випадках орган зі стандартів рекомендував власникам ТРО просто визначати характер та мету збору інформації [117]. Такі пропозиції не мають системного характеру та у зв’язку з рекомендаційною функцією не покладають зобов’язань на суб’єктів, котрі використовують ТРО.

Гостра потреба у цілісному законодавчому регулюванні у КНР почала поступово вирішуватись у жовтні 2020 р., коли китайським урядом було оприлюднено законопроект «Про захист персональної інформації». Джемі П. Хорслі зазначає, що загалом зазначений законопроект узгоджується із світовими тенденціями на шляху забезпечення конфіденційності. Безумовно, розбіжна позиція КНР щодо суверенітету даних, повсюдне використання систем нагляду та ряд інших, поки не розв'язаних питань, ускладнюють перспективу досягнення відповідності глобальним, міжнародним правилам щодо управління даними. Проте законопроект передбачає, що КНР серйозно ставиться до захисту ПД [118].

***

В період поширення коронавірусної хвороби особливої популярності набули технології відстеження та ТРО із функцією скринінгу температури. Складна епідеміологічна ситуація стала тригером для використання ТРО. Фактично, посилаючись на необхідність впровадження заходів, що стримують поширення коронавірусної хвороби, деякі держави, окремі населені пункти почали широку кампанію впровадження ТРО. Окремо звернено увагу на безпілотники із функцією розпізнавання облич, застосування яких також набуло популярності протягом останнього року.

На європейському рівні та в США, де законодавство про конфіденційність суворіше, державні органи вдались до розробки політик, інструкцій захисту даних та порядку використання технологій стеження та ідентифікації. В державах, де увага питанням конфіденційності приділяється меншою мірою, впровадження належного рівня захисту ПД та права на приватність тільки починає обговорюватись.

ВИСНОВКИ

У даній роботі відповідно до поставлених завдань було зроблено наступні висновки:

1. ТРО є однією із систем ідентифікації осіб, унікальність якої полягає в тому, що немає необхідності в прямій участі осіб при використанні технологій, тобто відбувається дистанційна ідентифікація. Відмінність ТРО від інших систем ідентифікації полягає також в тому, що в поле зору цієї технологій попадає невизначене коло осіб, які в більшості не вчиняли жодних протиправних дій. Зважаючи на це, органи державної влади повинні надавати звіти про кількість попереджених правопорушень та/або затриманих осіб за вчинення правопорушень завдяки застосуванню ТРО. В іншому випадку використання ТРО може розглядатись як безпідставне втручання у права суб'єктів даних.

2. При застосуванні ТРО та інших технологій спостереження необхідно чітко визначати та дотримуватись мети застосування, принципу мінімізації даних, який включає вимоги достатності, відповідності та доцільності. Важливою гарантією є також, окрім загальної мети, встановлювати конкретні цілі, які мають та можуть бути досягнуті завдяки використанню ТРО та протягом періоду застосування ТРО не відступати від першочергової мети.

3. Важливим аспектом для належного застосування ТРО є встановлення обмежених строків зберігання даних. Володілець ПД, виходячи із мети використання ПД, повинен визначити, протягом якого періоду буде необхідність у обробці даних. При цьому такий строк має бути належним чином обґрунтованим.

4. Вимоги, які застосовуються до використання звичайних камер відеоспостереження, розглядаються вужче, а ніж ті, що повинні бути впровадженні для застосування ТРО, адже це система, яка охоплює ширше коло процесів. Презюмування згоди особи на зйомку в публічних місцях, передбачене ЦК України, не може розцінюватись як припущення згоди на обробку ПД при застосуванні ТРО.

5. Безпосереднє надання згоди суб'єктом даних при застосуванні ТРО практично виключається, тому органам державної влади варто вдаватись до обґрунтування інших законодавчо визначених підстав обробки ПД.

6. На рівні ЄС, в ЗРПЗД надається особлива увага біометричним даним, до яких відносять і зображення обличчя. Тому для наближення українського законодавства до провідних практик у сфері захисту ПД варто також визначити поняття біометричних даних, як особливої категорії, у законодавстві про захист персональних даних та деталізувати питання захисту таких даних.

7. Дуже обмежено в українському законодавстві йдеться також про відповідальність за порушення порядку обробки спеціальних категорій даних та й взагалі питанню відповідальності за порушення вимог до обробки ПД не надано належної уваги. На даний час в нашій державі відсутній спеціальний орган, діяльність якого була б спрямована на впровадження заходів забезпечення прав суб'єктів даних, удосконалення існуючих положень та впровадження нових умов.

8. Право на захист ПД тісно пов'язане із правом на приватність та розцінюється як складова останнього. Визначення спеціального регулювання щодо ПД дає підстави стверджувати, що дане право в певних випадках може захищатись більш широко, а ніж виключно статтею 8 Конвенції та іншими актами, що визначають право на приватність. В практиці ЄСС розрізняється право на приватність та право на захист ПД. Останнє позиціонується, як більш новий механізм. Тому для повного захисту прав осіб, окрім загальних вимог щодо обмеження права на приватність, варто аналізувати специфічні вимоги саме до обробки ПД.

9. Перш ніж вдаватись до впровадження ТРО, в кожному конкретному випадку необхідно проаналізувати таке впровадження згідно критеріїв принципу пропорційності.

10. Застосування ТРО органами державної влади відбувається в публічних місцях. Рівень захисту права особи на приватність відповідно може розцінюватись як дещо нижчий, а ніж в приватному будинку. Для визначення

рівня приватності у публічних місцях пропонується вдаватись до американської доктрини «розумні очікування приватності».

11. Внесення змін до законодавчих актів у сфері захисту ПД повинно бути органічно пов'язано із регулюванням новітніх технології. Приклад проекту Регламенту про регулювання штучного інтелекту є прогресивним кроком для встановлення комплексних засад використання новітніх технологій загалом та ТРО зокрема.

12. Окрім становлення безпеки, ТРО використовуються в цілях забезпечення права на охорону здоров'я під час коронавірусної хвороби (COVID-19). Країни ЄС та США, де стандарт захисту ПД є вищим, встановили правила мінімізації втручання технологій відстеження та розпізнавання у приватне життя. В США було прийнято закон, що закріпив суть технології та визначив фундаментальні вимоги до провадження ТРО. Таким чином, складна епідеміологічна ситуація стала підставою для підвищеної уваги до застосування ТРО та інших технологій відстеження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. У рамках проекту «Безпечне місто» запущено новий аналітичний модуль відеоспостереження, що прискорить пошук правопорушників. Офіційний портал КМДА - Головна. URL: https://kyivcity.gov.ua/news/u_ramkakh_proektu_bezpechne_misto_zapuscheno_noviy_analitichniy_modul_videosposterezhennya_scho_priskorit_poshuk_pravoporushnikiv.html (дата звернення: 19.05.2020).

2. Facial recognition. Cambridge Dictionary | English Dictionary, Translations & Thesaurus.

URL: https://dictionary.cambridge.org/ru/словарь/английский/facial-recognition (date of access: 05.02.2021).

3. Nakar S., Greenbaum D. Now you see me. Now you still do: facial recognition technology and the growing lack of privacy. Journal of Science & Technology Law - Boston University. 2017. 23:88. P. 89–123

URL: https://www.bu.edu/jostl/files/2017/04/Greenbaum-Online.pdf

4. Wright Elias. The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector. Fordham Intell. Prop. Media & Ent. L.J.. 2019. P. 611-684.

URL: https://ir.lawnet.fordham.edu/iplj/vol29/iss2/6/

5. Richardson R. Facial Recognition in the Public Sector: The Policy Landscape. *The German Marshall Fund of the United States*. URL: https://www.gmfus.org/publications/facial-recognition-public-sector-policy-landscape (date of access: 20.03.2021).

6. Ünver, H. Akın. Artificial Intelligence, Authoritarianism and the Future of Political Systems. Centre for Economics and Foreign Policy Studies, 2018

URL: www.jstor.org/stable/resrep26084 (date of access: 20.03.2021)

7. Pauwels, Eleonore. Artificial Intelligence and Data Capture Technologies in Violence and Conflict Prevention: Opportunities and Challenges for the

International Community. Global Center on Cooperative Security, 2020, www.jstor.org/stable/resrep27551 (date of access: 15.04.2021)

8. Ron Wyden, Law and Policy Efforts to Balance Security, Privacy and Civil Liberties in Post-9/11 America, vol 17 Stanford Law & Policy Review 331-352, 2006

URL: https://law.stanford.edu/publications/law-policy-efforts-balance-security-privacy-civil-liberties-post-9-11-america/ (date of access: 15.04.2021)

9. NSA slides explain the PRISM data-collection program. Washington Post. URL: https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (date of access: 15.04.2021).

10. Risen J., Poitras L. N.S.A. Collecting Millions of Faces From Web Images (Published 2014). The New York Times. URL: https://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html (date of access: 15.04.2021).

11. Учасники проектів Вікімедіа. Едвард Сноуден – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Едвард_Сноуден (дата звернення: 15.04.2021)

12. Kohen T. Data mining revelation opens political Pandora's box. CNN. URL: https://edition.cnn.com/2013/06/07/politics/data-mining-after-9-11/index.html (date of access: 04.05.2021).

13. Laura Finley, and Luigi Esposito. "'Digital Blackwater': The National Security Administration, Telecommunications Companies and State-Corporate Crime." State Crime Journal, vol. 3, no. 2, 2014, pp. 182–199. JSTOR, www.jstor.org/stable/10.13169/statecrime.3.2.0182 (date of access: 04.05.2021).

14. DAILY MAIL – 13,000 FACE SCANS LEAD TO JUST ONE ARREST BY MET POLICE – Big Brother Watch. URL: https://bigbrotherwatch.org.uk/2021/02/daily-mail-13000-face-scans-lead-to-just-one-arrest-by-met-police/ (date of access: 08.05.2021).

15. Kevin W. Bowyer. Face Recognition Technology: Security versus Privacy. IEEE TECHNOLOGY AND SOCIETY MAGAZINE. 2004. P. 9-20.

URL: http://www.cse.nd.edu/Reports/2004/TR-2004-21.pdf (date of access: 04.05.2021).

16. Grother P., Ngan M., Hanaoka K. Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification. URL: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf. (date of access: 17.03.2021).

17. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI : станом на 23 квіт. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 08.05.2021)

18. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) : Регламент Європ. Союзу від 27.04.2016 р. № 2016/679.

URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 08.05.2021).

19. Malek M. A. Imports of the Data Minimization Principle in the Big Data World. Medium. URL: https://towardsdatascience.com/imports-of-the-data-minimization-principle-in-the-big-data-world-9b2c85e1c14e (date of access: 08.05.2021).

20. Finck Michèle and Biega Asia. Reviving Purpose Limitation and Data Minimisation in Personalisation, Profiling and Decision-Making Systems, January 11, 2021, Max Planck Institute for Innovation & Competition Research Paper No. 21-04.

URL: https://ssrn.com/abstract=3749078 (date of access: 17.03.2021).

21. Principle (c): Data minimisation. Home | ICO. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/ (date of access: 08.05.2021).

22. Judgment of the Court of Court of Justice of the European Union of 08.04.2014 in Joined Cases C-293/12 and C-594/12. URL: https://eur-

lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293. (date of access: 06.05.2021).

23. Berlin Commissioner for Data Protection Imposes Fine on Real Estate Company | European Data Protection Board. *EDPB | European Data Protection Board*. URL: https://edpb.europa.eu/news/national-news/2019/berlin-commissioner-data-protection-imposes-fine-real-estate-company_en#:~:text=Berlin%20Commissioner%20for%20Data%20Protection%20Imposes%20Fine%20on%20Real%20Estate%20Company,-5%20November%202019&text=On%20October%2030th%202019,%20the,Data%20Protection%20Regulation%20(GDPR). (date of access: 06.05.2021).

24. Hodge N. GDPR dealt blow as German court drops $17.2M Deutsche Wohnen fine. *Compliance Week*. URL: https://www.complianceweek.com/gdpr/gdpr-dealt-blow-as-german-court-drops-172m-deutsche-wohnen-fine/30134.article (date of access: 08.04.2021).

25. Stolton S. LEAK: Commission considers facial recognition ban in AI 'white paper'. Euractiv.
URL: https://www.euractiv.com/section/digital/news/leak-commission-considers-facial-recognition-ban-in-ai-white-paper/ (date of access: 08.05.2021).

26. White Paper on Artificial Intelligence: a European approach to excellence and trust, 19.02.2020.
URL: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (date of access: 08.05.2021).

27. Crawford K. Halt the use of facial-recognition technology until it is regulated. Nature. URL: https://www.nature.com/articles/d41586-019-02514-7 (date of access: 08.05.2021).

28. Conger K., Fausset R., Kovaleski S. F. San Francisco Bans Facial Recognition Technology (Published 2019). The New York Times. URL: https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html (date of access: 05.04.2021).

29. Judgment of the Court of Supreme Court of 18.12.1967 in Charles KATZ v. UNITED STATES

URL: https://supreme.justia.com/cases/federal/us/389/347/ (date of access: 05.04.2021).

30. Mariko Hirose. Privacy in Public Spaces: The Reasonable Expectation of Privacy against the Dragnet Use of Facial Recognition Technology. Connecticut Law Review. 2017. No. 5. Issue 49. P. 1591-1620. URL: https://opencommons.uconn.edu/law_review/377 (date of access: 05.04.2021).

31. Judgment of the Court of European Court of Human Rights «Perry vs. the United Kingdom» of 17.07.2003 in no. Application no. 63737/00. URL: https://hudoc.echr.coe.int/fre#%7B"itemid":["001-61228"]%7D. (date of access: 17.03.2021).

32. J. Goold Benjamin CCTV and Human Rights. European Forum for Urban Security : CITIZENS, CITIES AND VIDEO SURVEILLANCE: TOWARDS A DEMOCRATIC AND RESPONSIBLE USE OF CCTV, Paris, 2010. P. 27-35. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1875060 (date of access: 17.03.2021).

33. Ünver Akın. Politics of Digital Surveillance, National Security and Privacy. Cyber governance and Digital Democracy. 2018. No. 2. P. 1-23. URL:https://www.jstor.org/stable/resrep17009?seq=1#metadata_info_tab_contents (date of access: 17.03.2021).

34. Guidelines 3/2019 on processing of personal data through video devices - version adopted after public consultation | European Data Protection Board. EDPB. 2020. URL: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en (date of access: 08.05.2021).

35. Surveillance camera code of practice : Code. 2013. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf. (date of access: 17.03.2021).

36. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних. Рада Європи; Конвенція, Міжнародний документ від 28.01.1981

URL: https://zakon.rada.gov.ua/laws/show/994_326 (дата звернення: 08.05.2021)

37. Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків [...]. Рада Європи; Протокол, Міжнародний документ від 08.11.2001

URL: https://zakon.rada.gov.ua/laws/show/994_363 (дата звернення: 08.05.2021)

38. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data : Treaty No.223 of 10.10.2018 no. 223.

URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223 (date of access: 17.03.2021).

39. Посібник з європейського права у сфері захисту персональних даних.Посібник. 2020. 432 с.

40. Резолюція «Про міжнародні стандарти конфіденційності». 2011р.

URL: http://khpg.org/index.php?id=1317623899 (дата звернення: 08.05.2021)

41. Maximilian Von Grafenstein. The Function of the Principle of Purpose Limitation in Light of Article 8 ECFR and Further Fundamental Rights. The Principle of Purpose Limitation in Data Protection Laws: The Risk-Based Approach, Principles, and Private Standards as Elements for Regulating Innovation, by, 1st ed., Nomos Verlagsgesellschaft MbH, Baden-Baden, Germany, 2018, pp. 109–596.

URL: https://www.jstor.org/stable/j.ctv941v5w.5?seq=1#metadata_info_tab_contents (date of access: 17.03.2021).

42. Dubbeld Lynsey. Protecting Personal Data in Camera Surveillance Practices. Surveillance & Society. 2005. P. 546-563.

URL: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3363/3326 (date of access: 17.03.2021).

43. Цивільний Кодекс України Відомості Верховної Ради України (ВВР). 2003. № 40-44, ст.356

URL: https://zakon.rada.gov.ua/laws/show/435-15 (дата звернення: 08.05.2021)

44. Podolyak Vladyslav, Maksymovych Tetiana. Ukraine: Regulation of facial recognition technology. URL: https://www.dataguidance.com/opinion/ukraine-regulation-facial-recognition-technology. (date of access: 17.03.2021).

45. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус: Закон України від 20.11.2012 р. № 5492-VI : станом на 23 квіт. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/5492-17 (дата звернення: 08.05.2021).

46. Staunton Ciara, Slokenberga Santa, Mascalzoni Deborah. The GDPR and the research exemption: considerations on the necessary safeguards for research biobanks. European Journal of Human Genetics volume. 2019. P. 1159–1167.

URL: https://www.nature.com/articles/s41431-019-0386-5 (date of access: 10.05.2021).

47. Sellars C. EU: EDPS comments on facial recognition technology. DataGuidance. URL: https://www.dataguidance.com/opinion/eu-edps-comments-facial-recognition-technology (date of access: 10.05.2021).

48. E. J. Kindt. Having yes, using no? About the new legal regime for biometric data. Computer Law & Security Review. 2017. Vol. 34, no. 3. P. 523–538. URL: https://www.sciencedirect.com/science/article/abs/pii/S0267364917303667. (date of access: 10.05.2021).

49. Judgment of the Court of European Court of Human Rights of 18.04.2013 in no. Application no. 19522/09. URL: https://hudoc.echr.coe.int/fre#%7B"itemid":["001-119075"]%7D. (date of access: 10.05.2021).

50. Kindt E. J. Transparency and Accountability Mechanisms for Facial Recognition. *The German Marshall Fund of the United States*. URL: https://www.gmfus.org/publications/transparency-and-accountability-mechanisms-facial-recognition (date of access: 08.05.2021).

51. Data Protection Act 2018: Act. URL: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

52. Lawful basis for processing. Home | ICO. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/#what (date of access: 08.05.2021).

53. Decision High Court of Justice Case No: CO/4085/2018 R -v- The Chief Constable of South Wales Police and others URL: https://www.judiciary.uk/judgments/r-v-the-chief-constable-of-south-wales-police-and-others/ (date of access: 08.05.2021).

54. Approved Judgment COURT OF APPEAL (CIVIL DIVISION) dated 11.08.2020 p. Case No: C1/2019/2670. URL: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf. (date of access: 08.05.2021).

55. Chen Angela. The EU might ban facial recognition in public for five years. URL: https://www.technologyreview.com/2020/01/17/238092/facial-recognition-european-union-temporary-ban-privacy-ethics-regulation/. (date of access: 10.05.2021).

56. Satariano A. Europe Proposes Strict Rules for Artificial Intelligence. The New York Times. URL: https://www.nytimes.com/2021/04/16/business/artificial-intelligence-regulation.html (date of access: 08.05.2021).

57. Artificial Intelligence Act: Proposal for a Regulation. URL: https://ec.europa.eu/newsroom/dae/items/709090. (date of access: 10.05.2021).

58. Liboreiro J. 'Higher risk, stricter rules': EU's new artificial intelligence rules. euronews. URL: https://www.euronews.com/2021/04/21/the-higher-the-risk-the-stricter-the-rule-brussels-new-draft-rules-on-artificial-intellige (date of access: 08.05.2021).

59. Reinhold F. AlgorithmWatch's response to the European Commission's proposed regulation on Artificial Intelligence – A major step with major gaps - AlgorithmWatch. AlgorithmWatch. URL: https://algorithmwatch.org/en/response-to-eu-ai-regulation-proposal-2021/ (date of access: 08.05.2021).

60. Collins Terry. Facial recognition: Do you really control how your face is being used?. USATODAY. 2019. URL: https://www.usatoday.com/story/tech/2019/11/19/police-technology-and-surveillance-politics-of-facial-recognition/4203720002/.(date of access: 10.05.2021).

61. Dragu Tiberiu. Is There a Trade-off Between Security and Liberty? Executive Bias, Privacy Protections, and Terrorism Prevention. American Political Science Review. 2011. No. 01. Issue 105. P. 64-78. URL: https://www.jstor.org/stable/41480827?seq=1 (date of access: 08.05.2021).

62. Sakin N. Will there be federal facial recognition regulation in the US?. IAPP. 2021 URL: https://iapp.org/news/a/u-s-facial-recognition-roundup/#:~:text=While%20there%20is%20no%20federal,examine%20potential%20facial%20recognition%20policies. (date of access: 10.05.2021).

63. California Consumer Privacy Act of 2018 [1798.100 - 1798.199] (Title 1.81.5 added by Stats. 2018, Ch. 55, Sec. 3.)

URL:https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article= (date of access: 10.05.2021).

64. Лясківський І. California Consumer Privacy Act: новий тренд США із захисту персональних даних у 2020 році. "ЮРИСТ&ЗАКОН". 2020. № 1. URL: https://uz.ligazakon.ua/ua/magazine_article/EA013372. (date of access: 08.05.2021).

65. Harwell D. Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expandinguse. The Washington Post. 2019. URL: https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/ (date of access: 08.05.2021).

66. Hill K. Wrongfully Accused by an Algorithm. The New York Times. URL: https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html (date of access: 08.05.2021).

67. Koebler J. Detroit Police Chief: Facial Recognition Software Misidentifies 96% of the Time. *Vice*. URL: https://www.vice.com/en/contributor/jason-koebler.

68. Wizner B. Facial recognition tech stories and rights harms from around the world. INCLO | International Network of Civil Liberties Organizations. URL: https://www.inclo.net/pdf/in-focus-facial-recognition-tech-stories.pdf (date of access: 08.05.2021).

69. CIVIL COVER SHEET. Case 2:21-cv-10827-GAD-APP ECF No. 1, PageID.1 Filed 04/13/21

URL: https://www.aclumich.org/sites/default/files/field_documents/001_complaint_1.pdf (date of access: 10.05.2021).

70. Загальна декларація прав людини (рос/укр). ООН; Декларація, Міжнародний документ від 10.12.1948

URL: https://zakon.rada.gov.ua/laws/show/995_015?lang=uk (дата звернення: 10.05.2021).

71. Міжнародний пакт про громадянські і політичні права ООН; Пакт, Міжнародний документ від 16.12.1966.

URL: https://zakon.rada.gov.ua/laws/show/995_043 (дата звернення: 10.05.2021).

72. Конвенція про захист прав людини і основоположних свобод : Конвенція Ради Європи від 04.11.1950 р. : станом на 2 жовт. 2013 р. URL: https://zakon.rada.gov.ua/laws/show/995_004 (дата звернення: 10.05.2021).

73. Конституція України // Верховної Ради України (ВВР). – 1996. – № 30, ст. 141

URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 10.05.2021).

74. Размєтаєва Юлія. Теоретичні аспекти зобов`язань бізнесу у сфері приватності: виклики цифрової епохи. Підприємництво, господарство і право. 2019. № 6. С. 235-239.

75. Німітц проти Німеччини (Niemietz v. Germany): Рішення Європейського Суду з прав людини від 16 грудня 1992 роки (скарга № 13710/88). URL: https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57887%22]} (date of access: 08.05.2021).

76. Shraddha Kulhari. Data Protection, Privacy and Identity: A Complex Triad. Building-Blocks of a Data Protection Revolution: The Uneasy Case for Blockchain Technology to Secure Privacy and Identity, by, 1st ed., Nomos Verlagsgesellschaft MbH, Baden-Baden, Germany, 2018, pp. 23–37. JSTOR, www.jstor.org/stable/j.ctv941qz6.7. (date of access: 08.05.2021).

77. Charter of Fundamental Rights of the European Union : no. 2012/C 326/02. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012P/TXT. (date of access: 08.05.2021)

78. Fuster G. G. The Emergence of Personal Data Protection as a Fundamental Right of the EU. Springer, 2016. 290 p.

79. McDermott Y. Conceptualising the right to data protection in an era of Big Data. *Big Data & Society*. 2017. Vol. 4, no. 1. URL: https://journals.sagepub.com/doi/10.1177/2053951716686994. (date of access: 08.05.2021)

80. Court of Justice of the European Union of 17.06.2010 in no. (C-92/09) and (C-93/09). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62009CC0092. (date of access: 08.05.2021)

81. ХРИСТОВА Г. О. ДОКТРИНА ПОЗИТИВНИХ ЗОБОВ'ЯЗАНЬ ДЕРЖАВИ У СФЕРІ ПРАВ ЛЮДИНИ. Харків, 2019. URL: http://nauka.nlu.edu.ua/download/diss/Xristova/d_Xristova.pdf (дата звернення: 17.03.2021).

82. Дахова Ірина Іванівна. Обмеження реалізації прав і свобод людини: конституційне регулювання та практика Європейського Суду з прав людини. Форум права. 2018. Вип. 4. С. 17-25.

83. Рішення Європейського Суду з прав людини у справі «Олександр Волков проти України» за Заявою № 21722/11. URL: https://zakon.rada.gov.ua/laws/show/974_947#Text . (дата звернення: 17.03.2021).

84. Рішення Конституційного суду України від 29.06.2010 р. у справі №1-25/2010. URL: https://zakon.rada.gov.ua/laws/show/v017p710-10#Text. (дата звернення: 17.03.2021).

85. Jonida Milaj. Privacy, surveillance, and the proportionality principle: The need for a method of assessing privacy implications of technologies used for surveillance, International Review of Law, Computers & Technology. 2015. 30:3, p. 115-130
URL:https://www.researchgate.net/publication/283565019_Privacy_surveillance_and_the_proportionality_principle_The_need_for_a_method_of_assessing_privacy_implications_of_technologies_used_for_surveillance (date of access: 08.05.2021)

86. Шабо і Віші проти Угорщини (SZABÓ AND VISSY v. HUNGARY): Рішення Європейського Суду з прав людини від 12 січня 2016 (скарга № 37138/14)
URL:
https://hudoc.echr.coe.int/eng#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-160020%22]} (дата звернення: 17.03.2021).

87. CASE OF A.-M.V. v. FINLAND Judgment of the Court of European Court of Human Rights of 23.03.2017 in no. Application no. 53251/13.
URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-172134%22]} (date of access: 08.05.2021)

88. Погребняк С. П. Принцип пропорційності в українській юридичній практиці та практиці ЄСПЛ. Правове забезпечення ефективного виконання рішень і застосування практики Європейського суду з прав людини. 2012. с. 294-310.

89. Armitage Rachel. To CCTV or not to CCTV? A review of current research into the effectiveness of CCTV systems in reducing crime. URL: https://epic.org/privacy/surveillance/spotlight/0505/nacro02.pdf. (date of access: 08.05.2021)

90. Irving Louis Horowitz. Privacy, publicity and security: the American context: Privacy is not only a right but also an obligation. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1490299/. (date of access: 08.05.2021)

91. Кабінет Міністрів України - Як працює застосунок «Дій вдома». *Головна | Кабінет Міністрів України*. URL: https://www.kmu.gov.ua/news/yak-pracyuye-zastosunok-dij-vdoma (дата звернення: 08.05.2021).

92. Mobile contact tracing apps in EU Member States. *European Commission*. URL: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en (date of access: 11.05.2021).

93. How tracing and warning apps can help during the pandemic. *European Commission - European Commission*. URL: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/how-tracing-and-warning-apps-can-help-during-pandemic_en (date of access: 11.05.2021).

94. Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems : Recommendation of 08.04.2020. URL: https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154.

95. Економічна правда. Київ закупив камери, які розпізнають обличчя і вимірюють температуру тіла. Економічна правда. URL: https://www.epravda.com.ua/news/2020/04/3/658959/ (дата звернення: 08.05.2021).

96. Система дистанційного вимірювання температури тіла. prozorro.gov.ua. URL: https://prozorro.gov.ua/tender/UA-2020-04-02-002335-a (дата звернення: 10.05.2021).

97. У метро встановлять додаткові камери відеоспостереження. Офіційний портал КМДА - Головна. URL: https://kyivcity.gov.ua/news/u_metro_vstanovlyat_dodatkovi_kameri_videosposterezhennya/ (дата звернення: 10.05.2021).

98. Masoodi Joe. Police and governments may increasingly adopt surveillance technologies in response to coronavirus fears. URL: https://theconversation.com/police-and-governments-may-increasingly-adopt-surveillance-technologies-in-response-to-coronavirus-fears-133737. (date of access: 08.05.2021)

99. Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union - : Treaty of 13.12.2007. Official Journal C 326 , 26/10/2012 P. 0001 - 0390. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012E/TXT. (date of access: 07.04.2021)

100. Coronavirus: Privacy Guarantor, no to "do it yourself" initiatives in data collection. Public and private entities must comply with the instructions of the Ministry of Health and the competent institutions. Home - Garante Privacy. URL: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9282117 (date of access: 11.05.2021).

101. DECREE-LAW “Urgent measures for the functionality of the systems of interception of conversations and communications, further urgent measures in the field of prison law, as well as supplementary and coordination provisions in the field of civil, administrative and accounting justice and urgent measures for the introduction of the Covid-19 alert system” dated 30.04.2020 p. № 28. URL: https://www.gazzettaufficiale.it/eli/id/2020/04/30/20G00046/sg. (date of access: 11.05.2021).

102. How facial recognition is spreading in Italy: the case of Como. Privacy International. URL: https://privacyinternational.org/case-study/4166/how-facial-recognition-spreading-italy-case-como (date of access: 11.05.2021)

103. ADM Systems in the COVID-19 Pandemic: Italy. Algorithmwatch. URL: https://algorithmwatch.org/en/automating-society-2020-covid19/italy/ (date of access: 11.05.2021).

104. Mobile contact tracing apps in EU Member States. *European Commission - European Commission*. URL: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en (date of access: 10.05.2021).

105. O szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych1) : USTAWA of 02.03.2020 no. Dz. U. 2020 poz. 374. URL: http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20200000374/T/D20200374L.pdf. (date of access: 10.05.2021).

106. Aplikacja Kwarantanna domowa - Koronawirus: informacje i zalecenia - Portal Gov.pl. Koronawirus: informacje i zalecenia. URL: https://www.gov.pl/web/koronawirus/kwarantanna-domowa (date of access: 10.05.2021).

107. Bartoszko A. Accelerating Curve of Anxiousness: How a Governmental Quarantine-App Feeds Society with Bugs. Journal of Extreme Anthropology. 2020. 4,, no. 1.

URL: https://www.researchgate.net/publication/340363404_Accelerating_Curve_of_Anxiousness_How_a_Governmental_Quarantine-App_Feeds_Society_with_Bugs (date of access: 10.05.2021).

108. McGee P. Lockdown crisis is a catalyst for novel drone deployment. *Financial Times*. URL: https://www.ft.com/content/7729851a-9363-11ea-899a-f62a20d54625 (date of access: 11.05.2021).

109. EUCHI J. Do drones have a realistic place in a pandemic fight for delivering medical supplies in healthcare systems problems?. *Chinese Journal of Aeronautics*. 2021. Vol. 34, no. 2. P. 182–190. URL: https://www.sciencedirect.com/science/article/pii/S100093612030279X?via=ihub. (date of access: 08.05.2021).

110. France: CNIL sanctions Ministry of Interior for unlawful use of drones. DataGuidance. URL: https://www.dataguidance.com/news/france-cnil-sanctions-ministry-interior-unlawful-use (date of access: 08.05.2021).

111. Decision of administrative court of Paris no. 440442. URL: https://www.legifrance.gouv.fr/ceta/id/CETATEXT000041897158. (date of access: 08.05.2021).

112. W. Savage C. USA: Pandemics, privacy, and drones. *DataGuidance*. URL: https://www.dataguidance.com/opinion/usa-pandemics-privacy-and-drones (date of access: 11.05.2021).

113. SENATE BILL 6280: Bill. Washington Privacy Act. URL: http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Bills/6280.pdf?q=20210511004904.

114. CARES Act Coronavirus Aid, Relief, and Economic Security Act. S.3548 116th Congress (2019-2020)

URL: https://www.congress.gov/bill/116th-congress/senate-bill/3548/text#toc-id41220d22025e45e3a4afb2cc7d640672 (date of access: 10.05.2021).

115. Pollard M. Even mask-wearers can be ID'd, China facial recognition firm says. U.S. URL: https://www.reuters.com/article/us-health-coronavirus-facial-recognition/even-mask-wearers-can-be-idd-china-facial-recognition-firm-says-idUSKBN20W0WL (date of access: 10.05.2021).

116. Зірен Ф. Коментар: Як коронавірус сприяє встановленню цензури та розвитку технологій в Китаї | DW | 17.03.2020. DW.COM. URL: https://www.dw.com/uk/yak-koronavirus-spryiaie-vstanovlenniu-tsenzury-ta-rozvytku-tekhnolohii-v-kytai/a-52797748 (дата звернення: 10.05.2021)

117. Dudley L. China’s Ubiquitous Facial Recognition Tech Sparks Privacy Backlash. The Diplomat. 2020. URL: https://thediplomat.com/2020/03/chinas-ubiquitous-facial-recognition-tech-sparks-privacy-backlash/ (date of access: 10.05.2021).

118. Horsley J. P. How will China’s privacy law apply to the Chinese state?. *Brookings*. URL: https://www.brookings.edu/articles/how-will-chinas-privacy-law-apply-to-the-chinese-state/#:~:text=China's%20highest%20law,%20the%20Constitution,foundational%20concepts%20supporting%20privacy%20protection; (date of access: 10.05.2021).