

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: **«BIG DATA В ПУБЛІЧНОМУ АДМІНІСТРУВАННІ»**

Виконала: студентка 2-го року навчання,
Спеціальності
081 Право

Мацера Галина Вікторівна

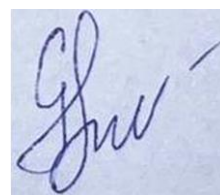
Керівник: Іщенко Юрій Вікторович,
кандидат юридичних наук, доцент

Рецензент _____

Магістерська робота захищена з
оцінкою _____

Секретар ЕК _____

«__» _____ 2022 р.



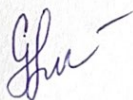
Київ-2022

**Декларація академічної доброчесності
студентки НаУКМА**

Я, Мацера Галина Вікторівна, студентка 2 року навчання факультету правничих наук, спеціальності 081 Право, адреса електронної пошти h.matsera@ukma.edu.ua:

- підтверджую, що написана мною магістерська робота на тему «Big data в публічному адмініструванні» 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 ознайомлена;
- підтверджую, що надана мною електронна версія роботи є остаточною і готовою до перевірки;
- 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 Unichек;
- даю згоду на архівування моєї роботи в репозитаріях та базах даних університету для порівняння цієї та майбутніх робіт.

17 червня 2022



Мацера Г. В.

ЗМІСТ

ВСТУП.....	4
РОЗДІЛ 1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ВЕЛИКИХ ДАНИХ.....	7
1.1. Big data як феномен сучасного світу.....	7
1.2. Підходи до визначення поняття «big data»	9
1.3. Характерні ознаки великих даних.....	13
Висновки до Розділу 1.....	14
РОЗДІЛ 2. ПРАВОВІ АСПЕКТИ ВИКОРИСТАННЯ ВЕЛИКИХ ДАНИХ У ПУБЛІЧНІЙ СФЕРІ.....	16
2.1. Публічне адміністрування: поняття та зміст.....	16
2.2. Держава – акумулятор великих даних.....	18
2.3. Сфери застосування big data в публічному адмініструванні.....	23
2.3.1. Надання державних послуг.....	23
2.3.2. Запобігання вчиненню правопорушень.....	26
2.3.3. Охорона здоров'я.....	29
2.3.4. Освіта та наука.....	33
2.3.5. Соціальний захист.....	36
2.3.6. Використання великих даних під час війни.....	39
Висновки до Розділу 2.....	43
РОЗДІЛ 3. ВПЛИВ ВЕЛИКИХ ДАНИХ НА ПРАВА ЛЮДИНИ.....	45
3.1. Порухення прав людини шляхом використання big data.....	45
3.2. Механізми захисту прав людини від неправового застосування big data.....	50
3.2.1. Міжнародне та національне законодавство у сфері кібербезпеки та захисту персональних даних.....	50
3.2.2. Суб'єкти публічної адміністрації з кібербезпеки та захисту персональних даних в Україні.....	56
Висновки до Розділу 3.....	61
РОЗДІЛ 4. СУДОВА ПРАКТИКА У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ.....	62

	3
Висновки до Розділу 4.....	69
ВИСНОВКИ.....	70
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	72

ВСТУП

Стрімкий розвиток технологій кардинально змінив канони сьогодення. Big data як важлива частина цифровізації відіграють надзвичайно важливу роль не лише в приватному житті людей, а й у державно-управлінських механізмах. Масштабне використання даних у діяльності корпорацій прискорило досягнення їхніх поставлених цілей. У свою чергу перейняття такого методу роботи органами публічної влади створює нові можливості для отримання ефективних результатів у забезпеченні загального блага громадян. Великі масиви інформації та їхнє бурхливе поширення удосконалюють різні сфери життєдіяльності, але водночас приносять нові проблеми та виклики у сфері приватності.

Дослідницьке питання роботи – у чому полягають особливості використання big data у публічному адмініструванні?

Актуальністю обраної теми є поступове впровадження big data в майже всі галузі бізнесу, науки, промисловості, економіки, побуту тощо. Як наслідок, застосування даних стало однією з основних напрямів державної політики, зокрема в Україні. Станом на сьогодні кількість технологічних інновацій, які використовуються в публічному адмініструванні, невпинно зростає, що підвищує інтерес до відповідних процесів. Зважаючи на те, що сфера регулювання big data є відносно новою та перебуває на стадії свого становлення, детальний розгляд взаємодії великих даних і органів державної влади дозволить краще зрозуміти переваги такої кореляції, а також застережить від її негативних наслідків.

Наукове значення проведеного дослідження полягає у визначенні наявного теоретичного та законодавчого базису для використання великих даних у публічному адмініструванні, виокремленні існуючих прогалин і наданні рекомендацій щодо їх подолання.

Практичне значення роботи полягає в тому, що її матеріали та висновки сприятимуть популяризації теми big data в публічному адмініструванні України, а також можуть використовуватися задля створення нового правового механізму захисту персональних даних і кіберпростору. Результати дослідження можуть

лягти в основу розробки оновлених механізмів правомірного впровадження великих даних у публічну сферу.

Об'єктом дослідження є великі дані як явище, яке активно асимілюється в публічно-правову сферу.

Предметом дослідження є практика використання великих даних органами державної влади України, переваги та недоліки такого використання в Україні та світі, а також його вплив на права людини.

Мета дослідження полягає в здійсненні комплексного аналізу феномену великих даних через особливості їх використання суб'єктами публічного адміністрування та їхнього впливу на права людини.

Завданнями дослідження є:

- сформулювати дефініцію big data;
- виокремити характерні ознаки великих даних;
- визначити основні сфери використання великих даних органами державної влади;
- з'ясувати, яким чином порушуються права людини у зв'язку з вільним доступом до інформації та її швидкого поширення;
- проаналізувати міжнародне та вітчизняне законодавство у сфері захисту персональних даних;
- охарактеризувати наявні в Україні органи виконавчої влади, що забезпечують дотримання прав людини шляхом правомірного використання big data;
- опрацювати наявну українську та міжнародну судову практику щодо дотримання законодавства у сфері захисту персональних даних і захисту права на приватне життя.

Станом на сьогодні тема роботи не є достатньо дослідженою в науковій спільноті. До іноземних учених, які розглядали питання великих даних у публічній сфері, належать Даг Ланей, Клаус Шваб, Кліффорд Лінч, Ханнес Грассеггер, Мікаель Крогерус, Сесілія Фредріксон, Фарук Мубарак, Марія Туохіма, Мінг Жан, Ювал Ной Харрарі, Шошана Зубофф, Генрі Саттон. Серед українських науковців важливий внесок у розвиток теми дослідження внесли

Маркіян Бем, Іван Городинський, Дмитро Самофалов, Антоніна Митко, Ірина Кольцова, Уляна Шадська, Володимир Батчаєв. Натомість велика кількість українських і міжнародних нормативно-правових актів допомагають краще осягнути всі питання та прогалини теми, а також знайти відповіді на них.

Методологічну основу дослідження складають як загальнонаукові, так і спеціально-правові методи правових досліджень. Зокрема, у роботі було використано такі методи: аксіологічний, антропологічний, аналітичний, формально-логічний, статистичний, герменевтичний, конкретно-соціологічний, формально-юридичний і метод порівняльного правознавства.

РОЗДІЛ 1

ЗАГАЛЬНА ХАРАКТЕРИСТИКА ВЕЛИКИХ ДАНИХ

1.1. Big data як феномен сучасного світу

Big data у своєму теперішньому розумінні не є чимось украй новим і незвичним для людства. Століттями люди використовували аналітичні методи даних для процесу прийняття рішень, ведення воєнних дій і підтримання державного ладу. Зокрема, державні органи влади Римської імперії ретельно аналізували статистику своїх військових задля визначення оптимального розподілу армій [1].

Поява Інтернету в кінці минулого століття кардинально змінила всі канони життя людства. Поступовий розвиток технологій істотно вплинув і на еволюцію великих даних. Завдяки швидкості, вседоступності та відкритості, які пропонує нам мережа Інтернет, поширення big data стало ще легшим.

Раніше інформація була вкрай обмеженим ресурсом, доступ до якого був відкритий лише невеликій кількості компаній або окремим представникам органів державної влади. Наразі потік інформації є надзвичайно великим, що й надає даним особливої цінності. Поява big data зробила життя людей простішим і мобільнішим, відкрила нові можливості та перспективи, а також дозволила економити час і зусилля при провадженні різноманітних видів діяльності.

Починаючи з 1990-х років держави почали активно використовувати збережені та кодифіковані дані для своїх «практичних, правових та адміністративних цілей» [2, с. 44]. Уже станом на початок 21 століття вебсайти, онлайн-портали, соціальні мережі та блоги стали настільки поширеними, що органи державної влади змогли вільно використовувати інформацію з відкритого доступу для прийняття рішень [2, с. 44].

Цікаву позицію щодо стрімкого поширення великих даних у XXI столітті висловив ізраїльський історик Ювал Ной Харарі у своїй книзі «Homo deus: за лаштунками майбутнього». Автор презюмує, що через стрімкий розвиток технологій такі інститути як «вибори, політичні партії і парламенти можуть стати непотрібними,

тому що вони не можуть достатньо ефективно обробляти інформацію» [3, с. 458]. Харарі також пропонує власну еволюцію становлення системи обробки даних, яка пройшла такі чотири стадії як когнітивна революція, що дала «можливість об'єднати велику кількість людей, які мислять в одну мережу обробки даних» [3, с. 464], аграрна революція, завдяки якій сільське господарство створило «щільні локальні мережі» [3, с. 465], винайдення письма та грошей, які встановили політичні та торговельні зв'язки між людьми, та відкриття Колумбом Америки, що призвело до масштабної глобалізації даних [3, с. 466].

Чарлі Страйкер, видатний підприємець у галузі обробки даних, ще в 2014 році наголошував на тому, що щоденно обробляється 5 мільярдів гігабайт даних [4]. Він запевняв, що протягом наступних 5 років не існуватиме жодної сфери життя, яка не була б піддана впливу великих даних [4]. Як бачимо, він мав рацію, адже наразі Інтернет контролює майже всі галузі діяльності та існування людини. Страйкер, досліджуючи концепцію великих даних, виокремив 4 характерні елементи big data: їхній великий обсяг, можливість їх структурувати, можливість їх легко знайти та поширювати [4].

Відомий німецький економіст Клаус Шваб характеризує сьогодення як четверту технологічну революцію – епоху цифрових інновацій, «великих можливостей і водночас потенційної небезпеки» [5, с. 9]. У своїй праці під назвою «Четверта промислова революція» Шваб наголошує на тому, що технології впливатимуть не лише на економіку, бізнес і соціум, а й на державний лад загалом. Зокрема, застосування вебтехнологій сприятиме ефективнішому управлінню. Відповідно органи публічної влади зможуть оновити закоренілі системи та функції, щоб «покращити загальну результативність, починаючи зі зміцнення процесів електронного управління до більшої прозорості, відповідальності та взаємодії між урядом і громадянами» [5, с. 55].

Вклад Шваба в розуміння феномену big data є колосальним, адже крізь призму розгляду всеосяжності Інтернету та технологій, їхнього визначального місця в житті суспільства, учений наголошує на великих даних як невід'ємному компоненті цифрової революції. Той масив інформації, який щоденно можна

отримати в мережі Інтернет, поширюється з неймовірною швидкістю та є доступним для кожного користувача. До того ж для отримання послуг та благ, які пропонує Інтернет, люди добровільно віддають свої дані. Такий взаємообмін має як свої переваги, так і недоліки. З одного боку, він економить час, адже завантаживши одного разу свої дані в мережу, вони зберігатимуться там завжди, а тому не потрібно щоразу вводити їх при здійсненні будь-якої операції онлайн. З іншого боку, така відкритість може призвести до маніпулювання та неправомірних дій з боку представників керівних органів влади держави.

Концепція big data є надзвичайно актуальною та водночас недостатньо досліджуваною через її недавнє виникнення та стрімкий розвиток. Щодня люди спостерігають за появою нових джерел інформації, соціальних мереж та Інтернет-додатків, які так чи інакше потребують наших даних. Регулярно в новинах можна довідатися про технологічні відкриття, які удосконалять ту чи іншу сферу життєдіяльності.

В Україні феномен великих даних не врегульовано належним чином, зокрема й з правової точки зору. Незважаючи на масштабне використання big data органами державної влади, законодавство і суспільство загалом потребує певної уніфікації всієї інформації щодо цього явища в публічній сфері.

1.2. Підходи до визначення поняття «big data»

Наразі як в Україні, так і в усьому світі немає загальноприйнятого визначення терміну «big data» як на доктринальному, так і на законодавчому рівні.

Загалом відсутні конкретні відомості навіть щодо часу виникнення та автора цього словосполучення. Більшість науковців схиляються до думки, що першим формулювання «big data» було вжито американським вченим Джоном Р. Маші ще в 1990-х роках [1; 6].

Водночас його запровадження в науковий обіг і так зване поширення в маси було здійснено професором Каліфорнійського університету Кліффордом Лінчем у його статті «Big data: How do your data grow?» у 2008-му році [7]. Лінч не пропонує

власного визначення big data, однак пояснює, що прикметник «великі» є доречним для пояснення цього феномену у зв'язку зі швидкістю обміну будь-яких даних, їх тиражування, поєднання та можливості повторного використання [7, с. 28].

Згідно з версією Рамеш Донти термін big data уперше вжили дослідники Nasa Майкл Кокс і Девід Елсворс ще в 1997-му році [8]. Водночас віце-президент SoftElegance Data Андрій Старжинський наголошує на тому, що поняття big data ввів в обіг аналітик Даг Ланей [9]. Відповідно сталої думки щодо зачинателя терміну big data станом на сьогодні немає, однак це не заперечує той факт, що цей феномен виник досить давно та з часом ставав усе більш вживаним.

Американський фінансовий вебсайт Investopedia пропонує таке визначення поняттю «big data» як «різноманітні набори інформації, що збільшуються з постійно зростаючими темпами» [10].

Наприклад, комерційна компанія TechTarget, яка пропонує свої маркетингові послуги саме на основі великих даних, визначає big data як певне поєднання зібраних компаніями «структурованих, напівструктурованих і неструктурованих» даних, видобування яких здійснюється для отримання інформації та використовується в «машинному навчанні, прогнозному моделюванні та інших передових методах аналітики» [11]. Беручи до уваги цю позицію, можна зрозуміти, що феномен big data має все ж статистичну та технологічну природу.

Ханнес Грассеггер та Мікаель Крогерус у своїй статті, присвяченій впливу великих даних і, зокрема, соціальних мереж на перемогу Дональда Трампа в боротьбі за президентство, характеризують термін big data як «усе, що ми робимо в мережі Інтернет або поза нею, залишає свої цифрові сліди» [12]. Автори коротко та чітко пояснюють читачам головну особливість big data: неможливість завантаженої в Інтернет інформації безслідно зникнути.

Томас Дейвенпорт зазначає, що big data – це дані, які є «занадто великими, щоб помістити їх на одному сервері, занадто неструктуровані, щоб вмістити їх в базу даних рядків і стовпців або занадто непостійні, щоб вміститися в статичному сховищі даних» [13, с. 1].

Наприклад, дослідники Фонду Рокфеллера визначають великі дані завдяки їхнім характеристикам. У своїй доповіді про теперішній вплив big data вони стверджують, що великі дані – це явище, що «має величезний об'єм, генерується досить швидко та збирається цілодобово та безстроково» [14, с. 6]. Зокрема, на думку авторів, big data настільки «великі», що їх неможливо проаналізувати на одному девайсі [14, с. 6].

Віктор Майєр-Шенбергер і Кеннет Кук'єр розглядають великі дані як «операції, які можна виконувати виключно у великому масштабі» [15, с. 14]. Учені наголошують на тому, що поява великих даних була вимушеною через масштабне збільшення об'єму інформації та як наслідок «потребу модернізації інструментів для аналізу всіх даних» [15, с. 14]. У своїй праці, присвяченій big data, автори зіставляють великі дані з «трьома кроками до нового способу аналізу інформації» [15, с. 20]. Ними є кількість, яка є величезною для даних у теперішньому світі [15, с. 20], точність, перевірку якої потребують ці масиви інформації [15, с. 21], а також причинність, яку станом на сьогодні можна замінити на «кореляцію між даними» [15, с. 22].

Ласло Бок, колишній віце-президент Google з роботи з персоналом, у своєму інтерв'ю для The New York Times зазначає, що одним із застосувань big data є «надання людям фактів та розуміння того, що їхні критерії до прийняття рішень не ідеальні» [16]. Він вважає, що «таке переконання у свою чергу змушує їх змінити свою поведінку» [16].

Жан-П'єр Дейкс, продакт менеджер корпорації з програмного забезпечення Oracle, розділяє великі дані на три групи: «традиційні підприємницькі дані – включають дані з CRM-систем, транзакційні дані з ERP-систем, транзакції з вебмагазину; дані від машин і датчиків – включає дані з CDR, вебблогів, розумних лічильників, торгових систем; соціальні дані – сайти відгуків клієнтів, мікроблог як Twitter, соціальні платформи як Facebook» [17, с. 3].

У контексті дослідження дефініції big data варто також звернути увагу на статтю, присвячену огляду літератури на тему великих даних у державній сфері, підготовлену учасниками дослідницького проєкту «Big Cities meet Big Data».

Автори статті зазначають, що сталого визначення big data немає, натомість використання тієї чи іншої дефініції залежить від «напрямку дослідження» [2, с. 45]. Окрім цього, великі дані характеризуються як процес, який «втілює нові ідеї та поєднує в собі мережі технологій, уряду, промисловості, ринків, користувачів і суспільства» [2, с. 45]. На підставі всіх проаналізованих визначень автори пропонують власне визначення big data – «великий обсяг даних зі специфічними властивостями, що призводить до нових ідей, а також проблем для сучасних технологій» [2, с. 52]. Зокрема, вони наголошують на тому, що дефініцію великим даним можна надати завдяки виокремленню їхніх характеристик.

Запропоновані варіанти визначення великих даних наводять на думку, що по-перше, big data – явище ілюзорне, це великий масив конкретної інформації про конкретну подію, істоту, предмет, факт тощо. По-друге, великим даним притаманні постійне збільшення, надзвичайна швидкість поширення, вільний доступ до них і цінність інформації, яку вони несуть. Незважаючи на відсутність чіткої доктринальної та законодавчої дефініції цього феномену, загальне уявлення та розуміння великих даних притаманні сьогодні кожному індивіду, так як щодня люди стикаються з big data як в професійній сфері, так і в повсякденному житті.

Звичайно, розглядаючи big data в контексті публічного адміністрування не можна не згадати про українські нормативно-правові акти, сфера яких поширюється на великі дані, а саме: Закон України «Про доступ до публічної інформації», ч. 1 ст. 1 якого визначає публічну інформацію як відображену та задокументовану будь-якими засобами та на будь-яких носіях інформацію, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом [18] та Закон України «Про захист персональних даних» (далі – Закон), абз. 10 ч. 1 ст. 2 якого надає визначення персональним даним, а саме: відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [19]. Персональні дані можна вважати вагомою складовою великих даних як таких, адже вони допомагають встановити ту чи іншу

особу шляхом виокремлення та обробки певної інформації про неї. Відповідно для дослідження феномену big data це визначення допомагає краще досягнути особливості концепції, адже згаданий вище нормативно-правовий акт є одним із небагатьох в українському законодавстві, що розкриває тему великих даних.

1.3. Характерні ознаки великих даних

Незважаючи на певну розбіжність у поглядах щодо першості Дага Ланея в застосуванні терміну «big data», сумнівів щодо запропонованих ним характерних ознак великих даних немає. Відповідно саме Даг Ланей виокремив такі три загальновживані особливості big data як обсяг, швидкість та різноманітність, так звані три V (з англійської мови: volume, velocity, variety) [20, с. 4; 21].

Що стосується обсягу, зрозумілим є те, що масив великих даних є нескінченним. Щодня різні публічні структури та приватні організації можуть збирати інформацію з різноманітних джерел, до яких відносяться, зокрема, соціальні мережі, мобільні додатки, онлайн бізнес-транзакції, вебблоги тощо. Один клік на будь-якому вебсайті вже передає інформацію про людину, яка зробила його. Ця характерна ознака великих даних допомагає їх збирати, структурувати та аналізувати [20, с. 6], а також виокремлювати від іншої інформації. Важливою складовою цієї ознаки є те, що люди самостійно «віддають» свої дані так званій системі.

Velocity – швидкість, з якою дані поширюються в усьому світі. Ця характеристика неподільно пов'язана з об'ємом, так як швидкість поширення даних сприяє їх збільшенню.

Різнорманітність big data полягає у варіації джерел їх виникнення. До них можна віднести як текстові, аудіо, відео повідомлення, публікації в соціальних мережах, так і фінансові операції, участь у судових процесах, заповнення декларації про майновий стан.

Окрім основоположних трьох характеристик великих даних, деякі вчені та дослідники концепції великих даних додають у цей перелік ще цінність і точність.

Таким чином іншим підходом до визначення характеристик big data є так звані п'ять V.

Value (з англійської мови «цінність»), на думку Жана-П'єр Дейкса, відображає «економічне значення даних» [17, с. 4], адже виокремлення з великої кількості інформації цінної та важливої є одним із етапів обробки даних. Відповідно від того, наскільки якісною є інформація, залежить і користь, яку вона зможе принести державі, корпораціям і суспільству загалом.

Veracity (з англійської мови «точність») є показником достовірності отриманих даних. Довіра осіб, які використовують інформацію для робочих, особистих, суспільних потреб, повинна бути високою [22, с. 21]. Зважаючи на кількість і різноманітність даних, особливо важливо звертати увагу на їхню правдивість, щоб досягнути бажаної мети обробки.

Керуючись запропонованими вище визначеннями та сталими ознаками big data, можна виокремити також такі характеристики цього явища як мінливість і легкодоступність, адже джерела інформації, її актуальність та новизна стрімко змінюються, а отримати бажані та необхідні дані в будь-який час та в будь-якому місті не є проблемою теперішнього.

Концепція big data не врегульована належним чином не лише в Україні, але й в усьому світі. На жаль, станом на сьогодні науковці не знайшли консенсусу щодо дефініції цього терміну, незважаючи на велику кількість запропонованих визначень. Завдяки визнаному науковою спільнотою переліку основних ознак великих даних можна осягнути суть і цінність цього феномену, а також сформулювати власний підхід до його змісту.

Що стосується законодавчого врегулювання big data, результат знову ж таки не є позитивним, адже великі дані не мають чіткого правового закріплення, що створює певне поле для особистого інтерпретування та потенційних ризиків маніпулювання.

Питання щодо дефініції, головних ознак і місця великих даних у сучасному житті є надзвичайно важливими задля подальшого розуміння їхнього впливу на сфери державного управління. Big data використовується не лише великими корпораціями та приватними компаніями, але й органами публічної влади. Крізь призму запропонованих у цьому розділі визначень і притаманних big data характеристик можна належним чином дослідити те, як саме застосовуються великі дані державою.

РОЗДІЛ 2

ПРАВОВІ АСПЕКТИ ВИКОРИСТАННЯ ВЕЛИКИХ ДАНИХ У ПУБЛІЧНІЙ СФЕРІ

2.1. Публічне адміністрування: поняття та зміст

Незважаючи на те, що феномен big data є ваговою складовою саме технологічної сфери, справжню користь для суспільства він приносить завдяки його застосуванню органами державної влади. Масове використання інструментів big data у державотворчих і правотворчих процесах є сьогодні частиною політичного курсу більшості урядів.

Адміністративне право, будучи галуззю публічного права, характеризується насамперед забезпеченням публічного інтересу як загального блага громадян. Саме публічний інтерес як складова адміністративного права відрізняє його від галузей приватного права. Роман Мельник у своєму навчальному посібнику з загального адміністративного права визначає публічні інтереси як такі, що містять у собі «інтереси, які однаковою мірою є важливими для кожного члена суспільства» [23, с. 36]. На думку Валентина Галуцького, публічний інтерес – це «інтерес соціальної спільності, що визнаний, задоволений державою» [24, с. 179]. Доктор юридичних наук, суддя Касаційного адміністративного суду Верховного Суду Семен Стеценко у своїй доповіді, присвяченій публічному інтересу, визначає це поняття як «об'єктивно існуючу сукупність взаємообумовлених інтересів суспільства і держави, що забезпечує задоволення домінуючих потреб пересічних громадян та відповідає стану розвитку суспільства» [25]. Доктори юридичних наук Колпаков і Кузьменко у своєму підручнику надають публічному інтересу визначення «інтереса соціальної спільності, що визнаний, задоволений державою» [26, с. 32]. Забезпечення таких потреб як чисті вода та повітря, продукти харчування, доступ до медицини та ліків, належна інфраструктура, надання робочих місць, приватна власність і територіальна цілісність є, на мою думку, найяскравішими прикладами дотримання публічного інтересу.

Відповідні публічні інтереси задовольняються органами державної влади. Визначення публічного адміністрування не закріплено в жодному нормативно-правовому акті України. Наприклад, Роман Мельник зазначає, що «термін «публічне адміністрування» сьогодні застосовується переважно на теоретичному рівні» [23, с. 39]. Автор апелює до того, що публічне адміністрування є формою реалізації виконавчої влади [23, с. 39]. Колпаков і Кузьменко наголошують на тому, що публічне управління складається з державного та громадського управління [26, с. 13]. Відповідно зрозумілим є те, що суб'єкти публічного адміністрування – це органи виконавчої влади та органи місцевого самоврядування. В окремих випадках до них належать Президент України, Верховна Рада України, судові органи, органи прокуратури, військові цивільні адміністрації.

Одним із головних завдань публічної адміністрації є введення в дію прийнятих законодавчим органом влади України нормативно-правових актів та їхнє активне впровадження. Для реалізації покладених Конституцією України та законами України завдань органи публічного адміністрування використовують також і великі дані.

Проаналізувавши чинні відповідні нормативно-правові акти щодо компетенції суб'єктів публічної адміністрації, для розкриття теми я виокремила такі їхні важливі повноваження. Згідно з п. 1 та п. 4 ч. 1 ст. 116 Конституції України Кабінет Міністрів України (далі – КМУ) як вищий орган виконавчої влади в Україні здійснює внутрішню політику держави, розробляє та здійснює загальнодержавні програми економічного, науково-технічного, соціального та культурного розвитку, утворює [27]. Відповідно до п. 6 ч. 1 ст. 20 Закону України «Про КМУ» утворення, реорганізація та ліквідація міністерств та інших центральних органів виконавчої влади віднесено до компетенції КМУ [28].

Закон України «Про центральні органи виконавчої влади» надає міністрам право утворювати територіальні органи міністерства (п. 9 ч. 2 ст. 8), підприємства, установи та організації, що належать до сфери управління міністерства (п. 12 ч. 2 ст. 8), а також визначати порядок обміну інформацією між міністерством та центральним органом виконавчої влади (п. 20 ч. 2 ст. 18) [29]. Відповідно керівник

центрального органу виконавчої влади згідно з п. 8 ч. 4 ст. 19 Закону України «Про центральні органи виконавчої влади» забезпечує дотримання порядку обміну цією інформацією.

Важливою функцією місцевих державних адміністрацій згідно з нормами Закону України «Про місцеві державні адміністрації» є інформування населення в різних галузях: охорони довкілля (п. 6 ст. 21), зайнятості та праці (п. 8 ст. 24), забезпеченні законності та правопорядку (п. 4, 12 ст. 25) [30]. Окрім цього, місцеві органи виконавчої влади відповідно до п. 3 ст. 28 Закону України «Про місцеві державні адміністрації» мають право одержувати інформацію та інші дані від державних органів та органів місцевого самоврядування.

Органи місцевого самоврядування згідно з ч. 2 ст. 18 Закону України «Про місцеве самоврядування в Україні» мають право на отримання відповідної інформації від підприємств, установ та організацій, а згідно з пп. 11 та пп. 15 п. «б» ч. 1 ст. 33 до їхніх повноважень належать створення та забезпечення функціонування місцевих екологічних автоматизованих інформаційно-аналітичних систем та надання податковим органам визначену законом і Податковим кодексом України інформацію [31].

Наведені вище норми чинного законодавства України закріплюють функції суб'єктів публічного адміністрування, належне виконання яких забезпечується регулярним використанням великих даних. До них належать взаємодія між різними органами виконавчої влади, між органами державної влади та громадянами, накопичення та передача інформації, систематизація даних, створення нових державних установ, онлайн-платформ і електронних державних послуг.

2.2. Держава – акумулятор великих даних

Аргумент щодо того, що держава не лише активно використовує великі дані для здійснення своїх повноважень, але й має доступ до будь-яких даних, навряд чи може кимось заперечуватися. Зрозумілим є також і те, що повноваження

представників органів державної влади та їхні можливості є необмеженими. Особливу увагу варто звернути на те, що це стосується і даних щодо громадян.

Задля використання благ та послуг, які пропонує держава, людям необхідно «ділитися» своїми особистими даними. Наприклад, відповідно до вимог, встановлених ч. 5 ст. 160 Кодексу адміністративного судочинства, у позовній заяві необхідно зазначати РНОКПП або номер і серію паспорта [32]. Іншим прикладом може бути велика кількість державних реєстрів: Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань, Спадковий реєстр, Єдиний державний реєстр виконавчих проваджень, Державний реєстр обтяжень рухомого майна, у яких зосереджені масиви інформації про фізичних та юридичних осіб, держателем яких є відповідні органи виконавчої влади: Міністерство юстиції України та Державна виконавча служба України.

Підтвердженням того, що держава є «збирачем» великих даних, можуть бути, наприклад, камери відеоспостереження в публічних місцях задля забезпечення порядку та охорони суспільства. Незважаючи на те, що наразі немає законодавчого базису для застосування систем публічного відеоспостереження в Україні, такий механізм також передбачає обробку даних про подію, особу, місце вчинення правопорушення тощо.

Яскравим прикладом застосування великих даних державою є створення Єдиного державного вебпорталу відкритих даних, який передбачає завантаження, оприлюднення та періодичне оновлення розпорядниками інформації (до яких в розумінні ст. 13 Закону України «Про доступ до публічної інформації» належать, зокрема, суб'єкти владних повноважень) відкритих даних [33]. Вебпортал надає можливість використовувати в майбутньому всю наявну на ньому інформацію органів державної влади, що відкриває нові можливості, заощаджує час і зусилля, створює прозорий механізм діяльності державного апарату. Відкриті дані як компонент великих даних допомагають структурувати існуючу в державі різноманітну інформацію.

Відповідно до ч. 1 ст. 36 Закону України «Про Державний земельний кадастр» на офіційному вебсайті центрального органу виконавчої влади, що реалізує державну

політику у сфері земельних відносин, оприлюднюються картографічна основа, індексні кадастрові карти та всі відомості Державного земельного кадастру без права їх зміни [34]. Відповідний вебсайт Державної служби України з питань геодезії, картографії та кадастру пропонує своїм користувачам такі електронні послуги як замовлення витягу про земельну ділянку чи нормативну грошову оцінку землі, витягу з Державного реєстру сертифікованих інженерів-землевпорядників, отримання відомостей про власників та користувачів земельних ділянок [35]. Задля використання цих електронних сервісів особа повинна ідентифікуватися. Зокрема, згідно з інформацією, оприлюдненою на офіційному сайті Держгеокадстру, інформація про перегляд будь-яким користувачем сайту відомостей про право власності та речові права на земельні ділянки, зберігається [36]. Відповідно кожен власник тієї чи іншої земельної ділянки зможе в подальшому дізнатися про те, хто саме «цікавився» його нерухомим майном. Спершу здається, що це дуже зручний і швидкий спосіб отримання необхідної інформації, однак водночас відповідний орган державної влади отримує наші дані, що обробляються задля досягнення бажаного результату та зберігаються в системі.

Ще одним прикладом є Єдина цифрова відомча телекомунікаційна мережа Міністерства внутрішніх справ України (далі – ЄЦВТМ), яка відповідно до п. 4 Положення про ЄЦВТМ є мультисервісною телекомунікаційною мережею, що забезпечує передавання інформації, яка належить до державних інформаційних ресурсів [37]. Завдяки взаємодії органів виконавчої влади, належній обробці та передачі великих даних ЄЦВТМ створює можливість для обміну інформацією між різними центральними органами виконавчої влади, їхніми територіальними підрозділами, посадовими особами і належної комунікації між ними через спеціальні канали електрозв'язку. Як наслідок, створюється багаторівневий та масштабний вузол інформації, який допомагає якісно надавати відповідні послуги громадянам.

Застосування та обробка big data використовуються і для діджиталізації судової гілки влади. Зокрема, наказом Державної судової адміністрації України №247 було впроваджено в дослідну експлуатацію підсистему «Електронний суд» та

«Електронний кабінет» у всіх місцевих і апеляційних судах України, а також в Касаційному адміністративному суді у складі Верховного Суду [38]. Ця підсистема дозволяє учасникам судового процесу направляти за допомогою електронного сервісу процесуальні документи, оплачувати судовий збір, а також контролювати рух і стан свого документа в суді [39]. У нинішніх умовах карантину та дії воєнного стану така можливість є надзвичайно вигідною. Для отримання запропонованих системою послуг користувач повинен авторизуватися за допомогою електронного цифрового підпису. Дані про особу отримує електронний портал, і держава в черговий раз шляхом полегшення життя громадян отримує доступ до їхніх даних. 2 вересня 2019 року Постановою КМУ №829 Державне агентство з питань електронного урядування було перетворено в Міністерство цифрової трансформації України (далі – Мінцифри) [40]. Відповідно 18 вересня 2019 року КМУ постановою №856 затвердив Положення про Мінцифри, яке закріплює його компетенцію та сфери діяльності [41]. Таке перетворення зіграло велику роль у діджиталізації держави, підвищило рівень цифрового розвитку та затвердило новітні методи ведення діяльності публічних органів влади.

Відповідно до абз. 2 п. 1 Положення про Мінцифри цей оновлений центральний орган виконавчої влади, окрім іншого, забезпечує формування та реалізацію державної політики у таких сферах як електронне урядування та електронна демократія, впровадження електронного документообігу, відкриті дані, надання електронних та адміністративних послуг.

Роль нового міністерства полягає саме в оновленні застарілих механізмів і векторів державної політики, створенні нових можливостей і полегшенні окремих аспектів життя та діяльності громадян шляхом оцифровування всіх запропонованих державою послуг.

Одним з найперших і найвагоміших нововведень Мінцифри було запровадження Порталу «Дія» (далі – Портал) та однойменного мобільного застосунку. Метою цього проекту є переведення державних послуг в онлайн-формат і завантаження всіх необхідних кожній особі документів у смартфон.

Станом на сьогодні Портал налічує 77 державних послуг, які можна отримати онлайн [42]. Мобільний застосунок «Дія», зокрема, пропонує своїм користувачам застосовувати електронну версію паспорта громадянина України у формі картки, закордонного паспорта, картки платника податків, посвідчення водія, свідоцтва про реєстрацію транспортного засобу, студентського квитка, свідоцтва про народження дитини, довідки про взяття на облік внутрішньо переміщеної особи, COVID-сертифікату як власного, так і дитини. Окрім цього, мобільний додаток дозволяє контролювати наявність штрафів за порушення Правил дорожнього руху та відкриття виконавчих проваджень проти користувача.

Згідно з Постановою КМУ №1453 пред'явлення електронного посвідчення водія та електронного свідоцтва про реєстрацію транспортного засобу здійснюється без додаткового пред'явлення їхніх паперових аналогів [43]. Закон України №1368-IX прирівняв електронні версії внутрішнього паспорта у формі картки та закордонного паспорта до їхніх фізичних аналогів [44], а постанова КМУ №677 забезпечила можливість використовувати COVID-сертифікати завдяки мобільному додатку Дія [45]. Така уніфікація значно заощаджує час і ресурси, а також запобігає випадковій втраті паперового документу.

Задля використання мобільного додатку особа повинна ідентифікувати себе шляхом надання згоди на обробку своїх персональних даних. Керуючись Повідомленням про обробку персональних даних, володільцем персональних даних, що обробляються за допомогою застосунку «Дія» є Мінцифри, їхнім розпорядником – державне підприємство «Дія», а третіми особами, яким вони передаються, уже відповідно органи державної влади [46]. Таким чином користувачі мобільного додатку добровільно передають свої дані органам державної влади та погоджуються на їх обробку та використання.

Робота Дії як Порталу та мобільного додатку є яскравим відображенням систематизації, аналізу, отримання та використання значної кількості big data. Доступ до цього ресурсу надає його користувачам можливість для ознайомлення з різноманітною консолідованою інформацією з різноманітних джерел задля отримання ефективного результату.

Вищезазначені державні електронні сервіси передбачають не лише обробку big data для їхнього функціонування, а й отримання ними даних про своїх громадян, зокрема завдяки взаємодії з відповідними державними реєстрами. Метою такого збирання є покращення умов життя людей, удосконалення запропонованих державними органами послуг і економія часу.

2.3. Сфери застосування big data в публічному адмініструванні

2.3.1. Надання державних послуг

На суб'єктів публічного адміністрування покладено функції надання публічних послуг. Згідно з пп. 3 п. 1 Листа Міністерства юстиції України №967-0-2-09-22 державні послуги як вид публічних послуг надаються органами державної влади (в основному виконавчої) та державними підприємствами, установами, організаціями, а муніципальні – органами місцевого самоврядування [47].

Застосування big data у сфері надання адміністративних послуг, на мою думку, є найяскравішим прикладом використання та накопичення великих даних державою. Задля якісного та точного надання адміністративної послуги необхідні якісні та точні дані, їхня належна обробка та впорядкування. Щодня органи виконавчої влади та органи місцевого самоврядування отримують величезний масив інформації шляхом надання адміністративних послуг.

Згідно з п. 1 ст. 1 Закону України «Про адміністративні послуги» адміністративною послугою є результат здійснення владних повноважень суб'єктом надання адміністративних послуг за заявою фізичної або юридичної особи, спрямований на набуття, зміну чи припинення прав та/або здійснення обов'язків такої особи відповідно до закону [48]. Процес надання та отримання адміністративних послуг передбачає ознайомлення, використання та обробку великої кількості даних. Сьогодні Україна прагне максимально спростити порядок надання адміністративних послуг шляхом переведення такої роботи в електронний вид.

Першим кроком для досягнення цієї мети було прийняття Верховною Радою України Закону України «Про електронні довірчі послуги», який передбачав створення належної автоматизації відносин між органами державної влади та громадянами, зокрема представниками бізнесу. Згідно з п. 7 ч. 1 ст. 1 цього закону електронна довірча послуга надається для забезпечення електронної взаємодії двох або більше суб'єктів, які довіряють надавачу електронних довірчих послуг щодо надання такої послуги [49]. Законом України «Про електронні довірчі послуги» запровадилися такі інструменти електронної ідентифікації як електронний підпис, електронна печатка та навіть електронна позначка часу. Відповідно вищезазначений нормативно-правовий акт дозволяє уникати паперових труднощів, автоматизує електронні дані про осіб, а також сприяє міжнародному співробітництву, адже при дотриманні вимог його статті 38 громадяни України можуть отримувати адміністративні послуги за кордоном. По суті прийняття цього закону стало підґрунтям для переведення державних послуг в електронний формат і запровадження можливих сьогодні механізмів Порталу та мобільного застосунку «Дія».

У грудні 2019 року КМУ постановою №1137 офіційно визнав Портал Єдиним державним вебпорталом електронних послуг [50]. Відповідно цифровізація України перейшла на новий рівень, де громадяни можуть отримувати адміністративні послуги шляхом подання онлайн-заяви чи онлайн-запиту.

Портал надає всю необхідну інформацію як для громадян, так і для представників бізнесу, що хочуть отримати адміністративну послугу [51], а також інструкції щодо правильного оформлення необхідних документів. Серед можливих електронних державних послуг Порталу є автоматична реєстрація та закриття ФОП, зміна місця проживання, подання заяви на отримання субсидії або видачу будівельного паспорта [42].

Відповідно Портал не лише впорядковує та забезпечує доступ до потрібної інформації щодо процесу надання адміністративних послуг, а й отримує, обробляє та надає всі дані щодо стадії та результату надання тієї чи іншої послуги в електронному вигляді. Зокрема, для застосування такого онлайн механізму та

отримання бажаного результату користувачі спочатку проходять ідентифікацію за допомогою електронного цифрового підпису. Іншим варіантом є авторизація шляхом підтвердження своєї особи за допомогою BankID, яке полягає в зазначенні імені, прізвища та по батькові, РНОКПП, дати народження, статі та банку, клієнтом якого ви є [46]. Інші необхідні дані для надання послуг Портал отримує від взаємодії з іншими реєстрами.

На прикладі автоматичної реєстрації ФОП пропонуємо розглянути механізм роботи Порталу. Згідно з інформацією, зазначеною на офіційному сайті Порталу, на подання заяви для отримання відповідної послуги користувач витратить приблизно 10 хвилин, а сама реєстрація його як фізичної особи-підприємця буде здійснена протягом однієї хвилини [52]. Важливим є те, що державна реєстрація здійснюється автоматично, без участі державного реєстратора. Дія пропонує інструкцію щодо порядку реєстрації ФОП як онлайн, так і офлайн, а також направляє на ознайомлення з інформацією щодо таких подібних послуг як внесення змін про ФОП та закриття ФОП [52]. Для підготовки такої спрощеної процедури надання досить непростой адміністративної послуги необхідно опрацювати досить багато великих даних, скомпільовати їх та правильно систематизувати.

Револьюційним стало затвердження постановою КМУ №691 Порядку надання комплексної послуги «єМалятко», який встановлює механізм надання універсальної послуги, що включає в себе всі необхідні для забезпечення прав новонародженої дитини послуги. Згідно з п. 1 цієї постанови до них належать державна реєстрація народження та визначення походження дитини, реєстрація місця проживання, призначення допомоги при народженні дитини тощо [53]. Таке поєднання різних послуг в одній є ще одним результатом обробки та аналізу величезної кількості big data та їхнього застосування органами державної влади, що налагоджує зв'язок між громадянами та носіями влади, економить час і матеріальні витрати.

Створення електронного сервісу «Електронний кабінет платника» відповідно до п. 1 розділу II наказу Міністерства фінансів України №637 передбачає надання необхідної документації платниками податків, а також отримання інформації та

послуг, передбачених Податковим кодексом України [54]. Подання податкової та фінансової звітності через Електронний кабінет здійснюється шляхом ідентифікації особи за допомогою електронного цифрового підпису. До того ж вебсайт Електронного кабінету надає доступ до різних важливих реєстрів, як наприклад, Реєстр платників єдиного податку, Реєстр платників ПДВ, Реєстр страхувальників. Це ще один технологічний прогрес держави за допомогою належного застосування масиву великих даних, який зібрав в одному місці велику кількість інформації з вільним і швидким доступом.

Окрему увагу варто приділити також прийняттю КМУ постанови №895, яка затверджує порядок проведення експериментального проєкту щодо запровадження Єдиної державної електронної системи дозвільних документів (далі – Порядок) [55]. Функціонування такої електронної системи забезпечить переведення адміністративних послуг у сфері ліцензування в електронну форму. Як наслідок, здобувачі ліцензій і ліцензіати не будуть зобов'язані щоразу надавати інформацію та необхідні документи про себе до органу ліцензування, адже ця автоматизована система забезпечить належну взаємодію між різними органами державної влади та інформаційними ресурсами відповідно до п. 69 Порядку задля вільного доступу до необхідних даних. Задля успішної реалізації цього експериментального проєкту необхідні належна взаємодія органів виконавчої влади та структурування наявної в них інформації, що забезпечується саме за допомогою великих даних.

2.3.2. Запобігання вчиненню правопорушень

Великі дані, що знаходяться в розпорядженні держави, можуть використовуватися задля зниження рівня злочинності в суспільстві. Сьогоднішній активний розвиток технологій, можливий доступ до окремих даних і їхня належна обробка допомагають запобігти вчиненню неправомірних дій.

Першим аргументом до наведеної вище тези є те, що big data руйнують корупцію. Протягом останніх декілька років прозорість і відкритість діяльності органів державної влади стали головними принципами української політики. Поява

різноманітних відкритих реєстрів, завдяки яким можна контролювати діяльність посадовців і ознайомитися з наявними в них активами, значно знизилася можливість у державі рівень корупційних правопорушень. Зокрема, особи, уповноважені на виконання функцій держави або місцевого самоврядування, відповідно до ч. 1 ст. 45 Закону України «Про запобігання корупції» зобов'язані щорічно подавати декларацію майнового стану [56]. На основі цієї норми НАЗК було створено Реєстр декларацій, який дозволяє ознайомитися з декларацією будь-якого державного службовця. За допомогою даних, завантажених у цей реєстр, кожен може порівняти реальне фінансове становище суб'єкта декларування з його задокументованим майном.

Більше того, з 2018 року на підставі Рішення НАЗК №166 в Україні функціонує Єдиний реєстр осіб, які вчинили корупційні або пов'язані з корупцією правопорушення (далі – Реєстр корупціонерів). Згідно з пп. 3 п. 3 Розділу I Положення про Реєстр корупціонерів метою створення Реєстру корупціонерів посеред іншого є визначення сфер державної політики та державних посад з найбільш корупційними ризиками, а також запровадження та реалізація антикорупційних політики [57]. Реєстр корупціонерів формується даними про будь-якого суб'єкта вчинення корупційного злочину: як фізичної, так і юридичної особи. Вільний доступ до Реєстру корупціонерів дозволяє здійснити пошук також і за номером статті, по якій було винесено судові рішення щодо правопорушника. Створений на підставі постанови КМУ №694 Єдиний вебпортал використання публічних коштів також покликаний фільтрувати прозорість державних грошових транзакцій. Відповідно до п. 7 Порядку адміністрування єдиного вебпорталу використання публічних коштів на відповідному вебпорталі відображені, зокрема, дані щодо використання коштів державного і місцевих бюджетів, а також суб'єктами господарювання державної і комунальної власності, отриманих ними від провадження їх господарської діяльності [58]. Такий вільний доступ до інформації здатний зменшити можливість вчинення корупційних дій і підвищити якість бюджетних процесів.

Що стосується міжнародного досвіду використання big data для зниження кількості правопорушень, то, наприклад, у Китаї широко розповсюджено встановлення камер розпізнавання обличчя задля швидкого пошуку підозрюваних. Так званий урядовий проєкт «Гостре око» покликаний забезпечувати безпеку громадян, встановити суспільний порядок, а також використовуватися в управлінні, включаючи вирішення проблем дорожнього руху, корупції та насильства [59] шляхом використання додаткових камер і великих даних. Масштаби застосування такої технології щорічно зростають на території КНР, водночас значно знижуючи кількість кримінальних правопорушень [59].

Україна також не відстає від практики зарубіжних країн і в 2018 році Київською міською радою було затверджено Комплексну міську цільову програму «Електронна столиця», яка посеред іншого передбачає «технічну підтримку встановлених камер відеоспостереження» [60]. Метою такого нововведення на території столиці України є саме зниження рівня злочинності. Відповідно дані, що накопичуються цілодобово за допомогою таких технологій, допомагають в майбутньому не лише виявити суб'єктів скоєних правопорушень або зафіксувати номери автомобілів порушників правил дорожнього руху, а також встановити постійні місця вчинення злочинів у Києві.

Наступним кроком до використання великих даних у протидії правопорушенням стало схвалення розпорядженням Київської міської ради в 2021 році проєкту міської цільової програми профілактики та протидії злочинності в місті Києві «Безпечна столиця» [61]. Головною метою такої програми є забезпечення публічного порядку, зниження рівня злочинності та підвищення рівня розкриття правопорушень. Одним із заходів для досягнення цих цілей є технічне забезпечення відео- та аудіообладнанням не лише вулиць Києва, але й адміністративних будівель підрозділів Національної поліції у Києві [61]. Окрім цього, посадових осіб столичної поліції планується оснащувати боді-камерами. Таким чином завдяки обміну та поширенню інформації про правопорушення, злочинців або підозрюваних у скоєнні злочинів у електронних системах органи

місцевого самоврядування зможуть якісніше виконувати свої обов'язки та гарантувати належну безпеку громадянам.

Варто зазначити, що станом на сьогодні програма «Безпечне місто» діє й у інших містах України. Наприклад, у Дніпрі за час дії програми у 2016-2020 роках було створено Центр обробки даних, отриманих з камер відеоспостереження [62].

Big data може сприяти суспільному порядку не лише шляхом їх використання, а й заборони поширення. Так, наприклад, 28 квітня 2017 року рішенням Ради національної безпеки і оборони України (далі – РНБО) було встановлено заборону Інтернет-провайдером надавати послуги з доступу користувачам мережі Інтернет до таких ресурсів як «Mail.ru», «Вконтакте» та «Однокласники» [63]. Окрім цього, рішення стосувалося й санкцій проти російських телеканалів, які транслювали ворожі заклики до сепаратизму та сприяли внутрішній дестабілізації в Україні. Зважаючи на збройну агресію Росії проти України з 2014-го року, безпека української цілісності та суверенітету є пріоритетом для представників органів державної влади. Російські сервери мали велику популярність серед українських користувачів, які щоденно завантажували на них різноманітну інформацію. Зокрема, зібрані на російських сайтах великі дані щодо українців, могли бути використані для підризу економіки, національної безпеки, а також в інтересах здійснення терористичних актів. Запроваджена заборона однозначно запобігла вчиненню окремих видів злочинів шляхом вільного доступу російських спецслужб до баз даних України.

2.3.3. Охорона здоров'я

Сфера охорони здоров'я охоплює велику кількість даних щодо медичних препаратів, історій хвороби, курсів лікування, лікарів і пацієнтів. Систематизація та належна обробка існуючої в медичній галузі інформації можлива завдяки big data.

11 березня 2020 року КМУ своєю постановою №211 установив на всій території України карантин у зв'язку з поширенням пандемії коронавірусу [64]. Задля

захисту населення до постанови були внесені зміни 29 березня 2020 року постановою КМУ №241, серед яких обов'язкова обсервація протягом 14 днів для осіб, які повернулися з країн/регіонів із місцевою передачею вірусу в громаді, після перетину державного кордону [65].

Для належного дотримання норм постанови Мінцифри створило електронний сервіс «Дій вдома», за допомогою якого можна було б здійснювати контроль за особами, що перебувають на самоізоляції за місцем свого проживання. Згідно з Інструкцією з використання електронного сервісу «Дій вдома» такий «контроль відбувається за допомогою регулярних повідомлень у додатку в довільні проміжки часу протягом дня та перевірки відповідності фотографії обличчя особи еталонній фотографії, зробленій під час встановлення мобільного додатку, та геолокації мобільного телефона в момент фотографування» [66]. Якщо відповідні дії не було зроблено, верифікація вважається нездійсненою.

Досягнути бажаного результату Мінцифри допомогли мобільні оператори Київстар, Водафон-Україна та Лайфселл. На основі big data, отриманих від цих компаній, Мінцифри було створено карту, яка відображає кількість порушників самоізоляції в кожному населеному пункті України [67]. Згідно з інформацією, оприлюдненою в прес-офісі Мінцифри, персональні дані абонентів не передаються державі та є захищеними [67]. Таке нововведення мало на меті запобігти поширенню пандемії на території України, забезпечити суспільний порядок та охорону здоров'я громадян. У будь-якому випадку важко уявити, наскільки великим був масив інформації, проаналізованої протягом режиму обсервації осіб, які повернулися в Україну в березні.

Загалом пандемія значно вплинула на медичну реформу в Україні та змусила прискорити багато процесів. Зокрема, комунікація між органами державної влади та окремими медичними закладами потребувала швидкості, оперативності та результативності в боротьбі проти вірусу. Вагому роль у забезпеченні надійного захисту населення відіграють саме великі дані та правомірність їхнього застосування. Наприклад, щоденне сповіщення Міністерства охорони здоров'я

України щодо кількості осіб, які захворіли та/або одужали від коронавірусу, потребувало обробки великого масиву даних з усіх регіонів України.

28 грудня 2020 року КМУ схвалив Концепцію розвитку електронної охорони здоров'я (далі – Концепція), яка повинна підвищити ефективність і прозорість сфери охорони здоров'я за допомогою інформаційних технологій [68]. Саме обробка big data може сприяти чіткому та правильному прогнозуванню потенційних захворювань громадян, необхідних засобів для медицини, а також забезпечувати постійний доступ як лікарів, так і пацієнтів до правдивих і актуальних даних. Концепція передбачає створення «єдиного медичного інформаційного простору як сукупності баз та банків даних, технологій їх ведення та використання, інформаційно-телекомунікаційних систем та мереж» [68].

Зокрема, уже діє платформа «Є ЛІКИ», завдяки якій можна виявити, чи є ті чи інші медикаменти в конкретній лікарні [69]. Автори концепції наголошують на тому, що станом на сьогодні існує велика проблема застарілого механізму лікування українців, незважаючи на наявність різноманітної новітньої інформації, якою оперують більшість спеціалістів. Систематизація всіх необхідних відомостей про хворих, застосованих методів лікування, наявних медичних послуг призведе до підвищення якості обслуговування та вільного доступу до необхідних ресурсів у галузі охорони здоров'я.

Яскравим прикладом застосування норм Концепції на практиці є створення Електронної системи здоров'я в Україні (далі – ЕСОЗ), яка складається з Центральної бази даних і електронної медичної інформаційної системи [70]. Поява цієї платформи забезпечує пряму взаємодію органів виконавчої влади та суб'єктів господарювання у сфері охорони здоров'я. Станом на сьогодні до ЕСОЗ підключені надавачі медичної допомоги, первинної медичної допомоги, спеціалізованої медичної допомоги та аптечні заклади [71]. Можливості, які відкриває ЕСОЗ, дозволяють зберігати всі медичні дані щодо пацієнтів в одному місці, доступ до яких відкритий як для пацієнтів, так і для лікарів, які надають їм медичну допомогу. Така уніфікація сприяє прозорості діяльності працівників медичної сфери, переходу з паперового на електронний облік документації, а також впроваджує

інноваційні підходи в медицині. Зокрема, КМУ постановою №126 запровадив обов'язкову реєстрацію всіх суб'єктів господарської діяльності з медичної практики в ЕСОЗ [72]. Таким чином незалежно від форми власності всі лікарні, медичні центри, лабораторії, поліклініки та аптеки перейдуть на електронну форму ведення документації і надання своїх послуг. Отже, усі наявні в Україні медичні дані буде систематизовано та завантажено в одну систему. Цей прогресивний шлях до цифровізації сфери охорони здоров'я несе в собі лише позитивні зміни в суспільстві, однак його прокладання можливе лише завдяки правовому використанню великих даних.

Завдяки роботі ЕСОЗ сьогодні українці можуть отримати електронні рецепти на лікарські препарати при визначених хронічних захворюваннях у рамках програми «Доступні ліки» [73]. Сервіс дозволяє хворим не звертатися особисто до лікарів за рецептом, а отримати його у вигляді смс-повідомлення. Придбати ліки за е-рецептом можна в аптеках, що також є учасниками ЕСОЗ.

29 вересня 2021 року КМУ затвердив план заходів щодо реалізації Концепції, для здійснення яких необхідне широке використання великих даних. Першочергово варто звернути увагу на те, що у 2022 році перед органами державної влади у сфері охорони здоров'я відповідно до п. 6 Плану заходів стоять задачі щодо створення технічних можливостей для доступу до знеособлених агрегованих великих даних в електронній охороні здоров'я та прозорих правил їх використання, а також розроблення концепції стратегічних напрямів розвитку кібербезпеки [74]. У період з 2022 по 2025 рік планується розвиток цифрових компетентностей, інформаційної культури, цифрової грамотності, кібербезпеки серед медичних працівників і пацієнтів, а також розвиток персоналізованої медицини, телемедицини, систем для обробки великих даних, штучного інтелекту [74]. Як бачимо, цифровізація медичної сфери шляхом використання великих даних чітко закріплена вже й на нормативному рівні.

Цінність великих даних у сфері охорони здоров'я підтверджує й міжнародна спільнота. Зокрема, Дмитро Самофалов зазначає, що станом на сьогодні «лідером використання даних у публічному управлінні виступає Японія» [75, с. 277]. У своїй

статті автор наводить приклад реформування медицини японським урядом, який визнав головним завданням у покращенні медичної сфери саме «більш ефективне використання інформації» [75, с. 277]. За допомогою належної системи передачі та обробки даних Японія прагне подолати нові виклики, які кидає сфера охорони здоров'я.

Зважаючи на те, що сьогодні світ переживає важкі часи епідеміологічної небезпеки, органи державної влади повинні використовувати всі інструменти, надані великими даними, для належної комунікації, запобігання ризиків і створення безпечних і якісних умов лікування громадян.

2.3.4. Освіта та наука

Освіта є базисом розвитку кожної держави, а її розвиток у теперішньому прогресивному світі напряму залежить від ефективного використання big data. Належна обробка даних сприяє актуалізації та структуризації навчального матеріалу, створенню надійної та доступної бази ресурсів, забезпеченню умов комфортного отримання послуг з освіти, наданню актуальної та важливої інформації.

За допомогою такої обробки протягом останніх років стали можливими систематизація та оприлюднення результатів шкільних міських, обласних і всеукраїнських олімпіад, доступ абітурієнтів до їхніх результатів зі вступних іспитів, формування рейтингів вступників до кожного вищого навчального закладу України, а на цій підставі й формування рейтингу університетів з найвищим показником успішності студентів-вступників.

Станом на сьогодні Міністерство освіти і науки України (далі – МОН) на своєму офіційному вебсайті надає доступ до різноманітних онлайн-сервісів у сфері освіти, серед яких онлайн-звернення до освітнього омбудсмана, Електронна бібліотека для вчителів і директорів шкіл, інформаційна сторінка учасників зовнішнього незалежного оцінювання, статистика результатів ЗНО по регіонах і офіційні звіти проведення ЗНО [76]. Таке величезне накопичення даних щодо питань, пов'язаних

з освітою, значно полегшує професійну діяльність учителів, викладачів і професорів, діджиталізує навчання учнів і студентів, економить їхній час і створює нові можливості для навчального процесу.

Наказом МОН №620 було створено Єдину державну електронну базу з питань освіти України (далі – ЄДЕБО). Відповідно до п. 1 Положення про ЄДЕБО цей портал є автоматизованою системою збирання, оброблення, зберігання та захисту інформації щодо здобувачів освіти, суб'єктів освітньої діяльності, що формується та використовується для забезпечення потреб фізичних та юридичних осіб [77]. Наразі за допомогою ЄДЕБО можна знайти необхідну інформацію щодо вступу до вищого навчального закладу за такими пошуковими критеріями як освітній рівень, спеціальність, конкурсні предмети [78], перевірити достовірність документів про освіту [79] та студентських і учнівських квитків [80]. До того ж користувачам ЄДЕБО доступні дані про наявні заклади вищої освіти в Україні, зокрема, їхня структура, особливості вступної кампанії та освітніх програм [81]. Такий електронний механізм щоденно оновлює всю передбачену в ньому інформацію та допомагає майбутнім студентам у виборі ВНЗ. Окрім усього переліченого вище, кожного літа ЄДЕБО оприлюднює списки вступників за рейтинговим балом після подання їхніх заявок до бажаного університету. Відповідно створення ЄДЕБО максимально спростило порядок вступу абітурієнтів, адже протягом останніх років майбутнім студентам не потрібно було приїжджати до омріяних ВНЗ, стояти в чергах, подавати документи в паперовому вигляді та чекати результатів особисто. Усі етапи вступної кампанії можна пройти, знаходячись удома та зареєструвавшись у системі. Ще однією перевагою ЄДЕБО, на мою думку, є забезпечення прозорості вступу до ВНЗ і запобігання корупційних злочинів шляхом всезагального оприлюднення даних щодо незалежних іспитів і рейтингових списків.

Вагомим кроком і показником рішучості органів публічного адміністрування в трансформації і діджиталізації сфери освіти та науки став підготовлений МОН проєкт Концепції цифрової трансформації освіти і науки на період до 2026 року [82]. МОН наголошує на недоступності актуальної інформації, наявній бюрократичній складовій освітніх установ, необхідності оновлення застарілих і

неефективних підходів до навчання, опануванні працівниками закладів освіти та науки інформаційно-комунікаційних технологій, запровадженні належного комп'ютерного забезпечення та доступу до Інтернету [82]. Усі ці проблеми стали причинами для розроблення і майбутньої реалізації концепції. Зокрема, своєю метою автори проєкту визначають використання цифрових технологій для трансформації процесів у системі освіти і науки з метою їх спрощення, автоматизації та зручності для користувачів [82]. Запропоновані кроки передбачають систематизацію великого масиву наявних у державі даних, їхню належну обробку та використання.

Серйозним поштовхом до цифровізації сфери освіти та науки стало поширення пандемії коронавірусу на території України, запровадження урядом карантинних обмежень у березні 2020 року та перехід шкіл та університетів на навчання в дистанційному форматі. На підставі вимушених змін у навчальному процесі, задля уникнення стресу, незручностей і проблем, що виникли як в учнів, так і в учителів, на замовлення Мінцифри та МОН було створено Всеукраїнську школу онлайн. На цій платформі учні та їхні батьки можуть знайти онлайн-курси всіх необхідних шкільних предметів з 5 по 11 клас, ознайомитися з великою кількістю шкільного матеріалу, переглянути відеоуроки та засвоїти вивчену інформацію шляхом вирішення тестів [83].

Наказом МОН №1545 була запроваджена можливість ведення електронних щоденників і журналів у закладах загальної середньої освіти [84]. Документ передбачає дослідну експлуатацію такого підходу до навчання, і вже сьогодні ця інновація долає незручності паперового документообігу та забезпечує постійний доступ до необхідних даних. Однією з можливостей системи є «перехід на збір освітньої статистики з використанням індивідуальних даних учнів та педагогічних працівників із їх подальшою деперсоналізацією» [85]. Водночас важливо наголосити на тому, що Методичними рекомендаціями щодо заповнення Класного журналу учнів початкових класів Нової української школи встановлено, що обробка персональних даних при веденні журналу здійснюється із забезпеченням захисту персональних даних, а інформація, зазначена в журналі, має бути захищена

від несанкціонованого знищення або змінення [86]. Відповідно МОН при масштабному переведенні документів в електронний формат прагне запобігти потенційним правопорушенням з отриманими даними учнів і вчителів.

Що стосується науки, цифрова трансформація має на меті створити Національну електронну науково-інформаційну систему URIS (далі – Система). Уже 15 лютого 2022 року відбулася її попередня презентація [87]. Система – це майбутня автоматизована база даних щодо наукових установ, учених, їхніх публікацій і проєктів [87]. Така систематизація даних сприятиме не лише належному та швидкому інформуванню громадян, а й ефективності прийнятих рішень органів державної влади щодо фінансування та розвитку наукової сфери. Станом на сьогодні Система ще перебуває в стані доопрацювання, адже згідно з інформацією МОН на першому етапі її розробки були допущені порушення у зборі та відцифруванні даних [88]. Цей приклад є гарним підтвердженням відповідального ставлення органів публічного адміністрування до пропорційності досягнення поставлених цілей і забезпечення прав громадян (зокрема, прав на інформацію та на повагу до приватного життя).

У сфері освіти та науки Мінцифри зробило вагомий внесок не лише для учнів і студентів, а й для представників старшого покоління. Створення проєкту «Дія. Цифрова освіта» має на меті навчання цифровій грамотності українців [89]. На онлайн-платформі можна знайти безкоштовні онлайн-курси з різних тем, що включають у себе освітні серіали, подкасти та гайди, які допомагають користувачам отримати цифрову освіту [89]. Зважаючи на те, що поступово всі державні послуги переходять в онлайн-формат, Дія прагне допомогти і заохочує суспільство в інтерактивній формі опанувати базові знання та навички технологічного світу.

2.3.5. Соціальний захист

Соціальна політика України також стає на шлях діджиталізації. Станом на сьогодні сфера соціального захисту включає в себе велику кількість запропонованих

державою соціальних послуг, створених реєстрів і документів. Належні систематизація та автоматизація зможуть значно полегшити більшість процесів, зекономити зусилля та час як органів виконавчої влади у сфері соціальної політики, так і громадян.

Найяскравішим і вагомим внеском у розвиток цифровізації соціальної сфери було створення Порталу електронних послуг Пенсійного фонду України (далі – вебпортал). Ще 30 липня 2015 року постановою Правління Пенсійного фонду України №13-1 було затверджено Положення про організацію прийому та обслуговування осіб, які звертаються до органів Пенсійного фонду України, відповідно до якого послуги, що надаються Пенсійним фондом України, можуть надаватися в електронній формі завдяки вебпорталу [90]. Станом на сьогодні вебпортал пропонує користувачам такі послуги як формування та подання заяв на призначення та на перерахунок пенсії, анкети для внесення змін даних в Реєстрі застрахованих осіб і анкети надання інформації для автоматичного призначення пенсії за віком, попереднє замовлення паперових документів [91]. Окрім того, можна переглянути свою електронну пенсійну справу та внести до неї зміни, а також отримати відомості про себе з Реєстру застрахованих осіб, Реєстру страхувальників, Електронного реєстру листків непрацездатності [91]. Задля отримання вищезазначених послуг користувач вебпорталу повинен авторизуватися за допомогою електронного цифрового підпису онлайн або ж подати необхідну заяву особисто. Вебпортал є уніфікованим джерелом пошуку інформації, якою оперує Пенсійний фонд України. Відповідно на ньому щоденно активно приймаються, обробляються, зберігаються та передаються великі об'єми даних.

Важливим нововведенням у діджиталізації соціальної сфери було створення на підставі постанови КМУ №328 згаданого вище Електронного реєстру листків непрацездатності (далі – ЕРЛН), який функціонує на підставі даних про листки непрацездатності та має на меті допомогти застрахованим особам отримати допомогу по тимчасовій непрацездатності, вагітності та пологам, а також проводити перевірки обґрунтованості видачі та продовження листків непрацездатності [92]. Відповідно наказ Міністерства охорони здоров'я України

№1066 зобов'язав заклади охорони здоров'я формувати медичні висновки про тимчасову непрацездатність в електронній формі [93], а так звані е-лікарняні згідно з наказом Міністерства охорони здоров'я України №1234 формують в ЕРЛН на підставі цих медичних висновків [94]. Таким чином інформація про медичні висновки, внесені до Реєстру медичних висновків, передається в ЕРЛН, дані якого зможуть переглянути на вебпорталі Пенсійного фонду України як роботодавці, так і працівники. Водночас ЕРЛН на пряму взаємодіє зі згаданою вище ЕСОЗ, адже формування лікарем медичного висновку про тимчасову непрацездатність здійснюється в ЕСОЗ відповідно до п. 3 ч. 2 Порядку організації ведення ЕРЛН та надання інформації з нього. Отже, взаємодія органів виконавчої влади в різних сферах шляхом передачі та отримання інформації набула сьогодні електронної, так званої віртуальної форми, яка постійно удосконалюється та значно спрощує життя українців, особливо коли мова йде про тяжкі захворювання.

Статтею 15 Закону України «Про соціальні послуги» передбачено створення Реєстру надавачів та отримувачів соціальних послуг [95]. На виконання ч. 11 ст. 15 вищезазначеного закону постановою КМУ №99 було затверджено Порядок формування, ведення та доступу до Реєстру надавачів та отримувачів соціальних послуг (далі – Реєстр) [96]. Згідно з п. 2 цього порядку Реєстр призначений для збирання, реєстрації, накопичення, зберігання, використання, знеособлення і знищення даних про надавачів та отримувачів соціальних послуг, визначених законодавством. Станом на сьогодні Реєстр ще не запрацював, адже постановою КМУ №99 встановлено зобов'язання Міністерства соціальної політики України наповнити Реєстр необхідною інформацією до 1 червня 2022 року, зокрема використовуючи дані органів виконавчої влади під час надання соціальних послуг. Така автоматизація соціальних послуг передбачає обробку величезного масиву великих даних, що перебувають у державі, їхнього впорядкування та надання якісніших і більш швидких послуг громадянам.

Широкомасштабне впровадження в державні процеси Єдиної інформаційної системи соціальної сфери (далі – ЄІСС) має на меті радикально змінити сферу надання соціальних послуг. Ця комплексна система покликана створити зручну

єдину базу даних для соціальної сфери за рахунок належного технічного забезпечення, оброблення, накопичення та впорядкування даних з різних інформаційних систем. ЄІСС передбачає, зокрема, створення Єдиного соціального реєстру як реєстру отримувачів соціальної підтримки (абз. 3 п. 2 Положення про ЄІСС), уніфікацію різноманітних процесів щодо соціального захисту, автоматизувати звернення заявників до інституцій соціального захисту (п. 3 Положення про ЄІСС) [97]. Завдяки роботі ЄІСС українцям більше не доведеться особисто звертатися до різних державних установ, подавати паперові заяви та стояти в чергах. Проєкт є дуже корисним і актуальним, адже заощаджує час, сили та матеріальні ресурси, береже здоров'я та запобігає вчиненню корупційних злочинів. Зважаючи на те, що зазвичай отримувачами соціальних послуг є вразливі групи населення, пенсіонери, інваліди, малозабезпечені особи чи безробітні, створення такого зручного порталу повинно сприяти належному забезпеченню їхніх невід'ємних прав.

2.3.6. Використання великих даних під час війни

Кібербезпека є однією з фундаментальних засад для побудови громадянського і правового суспільства станом на сьогодні. В Україні питання захисту в кіберпросторі регулює Закон України «Про основні засади забезпечення кібербезпеки України». Відповідно до п. 5 ст. 1 вищезазначеного закону кібербезпекою є захищеність інтересів людей і держави під час використання кіберпростору, а згідно з п. 7 ст. 1 кіберзахистом є конкретні заходи, спрямовані на запобігання та захист від кіберзлочинів [98]. Стрімкий розвиток технологій спричиняє нові види злочинів, які можуть посягати на національну безпеку та оборону держави у віртуальному світі за допомогою великих даних.

У січні та лютому 2022-го року в Україні було здійснено 3 масштабні кібератаки на державні електронні ресурси, від яких постраждало 22 сайти [99], Портал, банківський і енергетичний сектори [100; 101]. На щастя, усі спроби дестабілізувати ситуацію в країні та поширити паніку були вдало розгромлені

українськими фахівцями Мінцифри та Державної служби спеціального зв'язку та захисту інформації. Очевидним стало те, що завдяки великим даним можна посягнути на державну безпеку. Водночас вправне та чітке використання big data органами державної влади може і забезпечити належний захист країни.

24-го лютого 2022 року росія розпочала повномасштабну війну проти України. 21 століття пропонує нам нові виклики та можливості, а також і нові способи ведення війни. Одним із них став цифровий фронт, який в Україні успішно очолює Мінцифри на чолі з міністром цифрової трансформації України, віце-прем'єр-міністром Михайлом Федоровим.

Першим і важливим запровадженням Мінцифри під час війни було створення в застосунку Дія єДокумент, призначеного для українців, які втратили свої документи внаслідок бойових дій. Відповідно до п. 5 Порядку застосування єДокумента в період дії воєнного стану особи можуть використовувати єДокумент без додаткового пред'явлення паперових аналогів документів [102]. Цей тимчасовий електронний документ містить усі необхідні дані про українця, що відповідно були систематизовані на підставі належної та швидкої обробки big data державних органів і реєстрів. Він автоматично з'являється абсолютно у всіх користувачів мобільного додатку Дія та дозволяє не звертатися до державних установ для відновлення своїх документів.

Великі дані надали змогу реалізувати запроваджену урядом матеріальну підтримку осіб, робота яких тимчасово зупинена. У рамках програми єПідтримка громадяни, на яких розповсюджувалася вимоги постанови КМУ №199 [103], могли оформити заяву на отримання допомоги в розмірі 6500 гривень через мобільний додаток Дія [104]. У випадку успішного результату розгляду заяви особа отримує відповідну грошову суму на банківську картку.

До того ж постановою КМУ №331 уряд призначив матеріальну компенсацію роботодавцям, які працевлаштували внутрішньо переміщених осіб під час воєнного стану [105]. Цю послугу можна отримати як на Порталі, так і офлайн. У випадку вибору онлайн-варіанту Портал автоматично знайде роботодавця завдяки взаємодії з реєстрами Пенсійного фонду України [106]. Підписана електронним

підписом заява роботодавця направляється до Державного центру зайнятості, що яскраво ілюструє співпрацю різних органів виконавчої влади задля досягнення спільної мети.

Ще одним важливим і революційним нововведенням стала можливість інформування держави про пошкоджене та знищене внаслідок дій, спричинених російською агресією, нерухоме майно, порядок здійснення якої визначено постановою КМУ №380 [107]. Завдяки застосунку Дія громадяни України можуть внести всю необхідну інформацію щодо пошкодженої чи знищеної нерухомості, яку потім Мінцифри згідно з п. 5 постанови КМУ №380 зобов'язане передати відповідним держателям інформаційно-комунікаційної системи для збору, обробки та обліку даних. Таке прийняте КМУ рішення покликане належним чином забезпечити права громадян, які постраждали внаслідок війни, шляхом майбутньої компенсації понесених ними втрат або збитків. Технічне забезпечення цієї опції потребувало активного та оперативного використання великих даних і належної взаємодії між органами виконавчої влади. Загалом послуга є дуже зручною для українців, адже процес заповнення та подання заяви є автоматизованим і ретельно прописаним.

Постановою КМУ №455 було затверджено можливість подання особою заяви щодо отримання допомоги від міжнародних організацій за допомогою застосунку Дія [108]. Зокрема, передбачено, що необхідні для заяви дані можуть отримуватися шляхом електронної інформаційної взаємодії з інформаційно-комунікаційними системами та публічними електронними реєстрами органів державної влади [108]. Нормативно затверджений механізм застосування цієї послуги ілюструє майбутню циркуляцію даних українців з різних реєстрів.

Застосунок Дія створив можливість для осіб, що вимушено покинули своє рідне місто, подати онлайн заявку про отримання статусу внутрішньо переміщеної особи [109], а також отримати фінансову допомогу від держави, яка встановлена постановою КМУ №332 [110]. Поява такої функції знову ж таки значно полегшила процес отримання послуги громадянами та убезпечила від небезпечних пересувань до будівель центральних органів виконавчої влади.

Ще одним важливим проєктом, розробка якого була б неможливою без великих даних, є платформа «Допомога». Створена Міністерством соціальної політики України програма дозволяє швидко збирати заявки українців, які потребують гуманітарної допомоги, забезпечити адресний розподіл необхідної продукції [111]. До того ж бажаючі надавати допомогу також мають змогу допомогти нужденним у цьому особам. За технічного сприяння Мінцифри отримання та надання допомоги як у грошовому, так і у матеріальному вигляді здійснюється онлайн, дуже оперативно та ефективно [112].

Окрім неймовірних зручності, швидкості та якості, які пропонують нам описані вище функції, вони ще й захищають персональні дані українців від неправомірного використання ворогом. Наприклад, особисті подання паперових заяв на отримання необхідних послуг несуть у собі потенційну загрозу викрадення, неправомірного використання чи неправомірного доступу ворога до персональних даних українців. Мінцифри гарантує належну безпеку при передачі та обробці інформації про особу. Кіберзахист України полягав також і в обмеженні доступу до інформації. Зокрема, з початку вторгнення окупанта державними органами, які відповідають за національну безпеку, було обмежено доступ до більшості сайтів, реєстрів і порталів. Метою здійснення таких дій був захист не тільки державних установ, але й персональних даних громадян.

Окрім забезпечення кібербезпеки українського суспільства, створення зручних і дистанційних сервісів надання послуг, Мінцифри активно проводить цифрову блокаду країни-окупанта. Більшість державних сайтів і баз даних росії не працюють, великі технологічні компанії та міжнародні корпорації покинули ринок країни-агресора. Таке відсторонення підприємницького світу від окупанта відбувається завдяки важкій та плідній роботі робітників Мінцифри в поширенні інформації щодо воєнної агресії росії, аргументації щодо неприпустимості фінансової підтримки ворога.

Війна в Україні стала черговим доказом того, наскільки високим є рівень цифровізації в Україні, наскільки підготовленими є наші державні службовці та

наскільки сучасними є методи та принципи надання державних послуг. Взаємодія органів влади та великих даних здатна подолати всі провокації та загрози ворога.

Сьогодні big data є невід'ємною частиною публічного адміністрування та має надзвичайно позитивний вплив на його процеси. Органи державної влади на підставі обробки масиву даних здійснюють свою діяльність і забезпечують громадян належними умовами життя. Доступ до відкритих ресурсів, пришвидшення правових, політичних і економічних процесів у країні, модернізація суспільства, економія часу, гарантована прозорість діяльності влади та належна безпека громадян – усе це є перевагами використання big data органами виконавчої влади.

Протягом останніх років Україна активно впроваджує цифровізацію в усі сфери громадського життя. Регулярно з'являється все більше онлайн-сервісів у публічному секторі, державні послуги переводяться в електронний формат, діджиталізуються застарілі механізми діяльності органів державної влади, органів місцевого самоврядування та правоохоронних органів. Будучи розпорядником інформації, держава є не лише акумулятором усіх наявних даних, вона також поширює їх з невинною швидкістю, забезпечуючи найбільший комфорт своїх громадян.

Використання великих даних у сфері надання послуг спрощує порядок ведення господарської діяльності українських підприємців, зменшує корупцію, підвищує якість наданих органами державної влади послуг і полегшує процес їх надання та отримання. Окрім цього, великі дані здатні впливати на перебіг подій війни в 21-му столітті, допомогти знищувати ворога та боронити Батьківщину.

Big data можуть забезпечити безпеку людства, покращити умови життя пересічних громадян, запобігти правопорушенням, відкривати нові можливості, а також видозмінити механізми взаємодії суб'єктів публічного адміністрування та

суспільства. Досягти цього можна завдяки чіткому та правильному застосуванню великих даних державою.

РОЗДІЛ 3

ВПЛИВ ВЕЛИКИХ ДАНИХ НА ПРАВА ЛЮДИНИ

3.1. Порушення прав людини шляхом використання big data

Незважаючи на всі переваги, які мають великі дані в публічному адмініструванні, відкритим залишається питання безпеки, конфіденційності та дотримання прав людини. Певне безвідповідальне відношення людей до передачі своїх даних або недобросовісне виконання посадових обов'язків суб'єктами публічної адміністрації може призвести до непоправних наслідків.

Накопичення великого масиву даних дозволяє органам державної влади та приватним компаніям за допомогою логічних методів дослідження сформувати певний портрет тієї чи іншої особи на підставі даних, які вона самостійно передає в тій чи іншій формі [5, с. 59]. Яскравим прикладом такого аналізу є кейс Cambridge Analytica, який стосується накопичення компанією особистих даних користувачів соціальної мережі Facebook без їхнього дозволу для втручання в такі серйозні події як вибори президента США у 2016 році та вихід Великої Британії з Європейського Союзу. На основі вподобань, історії пошуку та підписок Cambridge Analytica змогла шляхом розповсюдження маніпулятивної інформації вплинути на думку потенційних виборців, вторгнутися в державно-політичні процеси та стати джерелом конформізму. З цього виникає запитання: «Чи завжди великі дані використовуються з правовою метою?».

Беручи до уваги міжнародний досвід неправомірного використання великих даних, варто зазначити, що в 2016 році у США Федеральна комісія зі зв'язку внесла зміни до законодавства, якими зобов'язала Інтернет-провайдерів «збирати поведінкові дані споживачів, які не стосуються підвищення безпеки та ефективності їхніх послуг, лише при отриманні їхньої явної згоди» [113, с. 227]. Щоправда нововведення стосувалися лише провайдерів, якими керує Федеральна комісія зі зв'язку. Таким чином орган законодавчої влади США прийняв революційне рішення у сфері захисту персональних даних користувачів Інтернету та убезпечив

від несанкціонованого використання їхніх даних. На жаль, через декілька місяців прийнята Конгресом США резолюція відмінила оновлені правила конфіденційності в Інтернеті [113, с. 228]. Цей крок назад викликав чимало занепокоєння та супротиву. На мою думку, у такий спосіб держава залишила за собою законне право слідкувати за діями своїх громадян, маніпулювати їхніми вчинками та всебічно контролювати політично-суспільні позиції людей.

Зокрема, американська письменниця, професорка Гарвардської школи бізнесу Шосана Зубофф наголошує на тому, що законодавство США захищало таємницю телефонних дзвінків і водночас так недобросовісно проігнорувало захист приватного життя в мережі Інтернет [113, с. 228]. Використаний нею в однойменній праці термін «наглядний капіталізм» використовується як економічний інструмент універсального нагляду за учасниками різноманітних політико-економічних процесів шляхом постійного збору їхніх даних. Зубофф дійшла висновку, що люди готові обміняти свої персональні дані на безкоштовні послуги, які можна отримати в мережі Інтернет [113, с. 229]. Авторка вважає, що органи державної влади «співпрацюють» з такими великими корпораціями як Google та Facebook задля встановлення масштабного контролю над суспільством. Підтвердженнями цієї позиції є безліч компаній, діяльність яких полягає в накопиченні та обробці персональних даних певної групи людей для надання професійних послуг своїм клієнтам [113, с. 231, 232]. Я вважаю, що саме існування подібних фірм уже відображає недосконалість державного регулювання питань захисту прав людини, приватного життя та конфіденційності. На жаль, навіть така прогресивна країна як США також недостатньо вмотивована на встановлення системи прозорості та збереження даних осіб.

Використання великих даних у неправомірних цілях може призвести до незворотних наслідків щодо життя та здоров'я осіб. У 2017 році Управління з санітарного контролю за якістю харчових продуктів і медикаментів Міністерства охорони здоров'я та соціальних служб США оголосило про відкликання деяких вразливих моделей кардіостимуляторів через загрозу кібератак [114]. Кардіостимулятори є важливими пристроями, що забезпечують життєдіяльність

людини та роботу серця саме за допомогою технологічного втручання. Відповідно орган охорони здоров'я США мав на меті запобігти потенційній шкоді, яку можуть спричинити злам кардіостимуляторів і можливість їхнього віддаленого управління через мережу Wi-Fi.

У 2020 році під час проведення виборів в Ізраїлі стався масштабний витік даних виборців. Партією «Лікуд» було створено додаток, завдяки якому можна було виявити потенційних виборців і залучати їх до голосування [115]. Для реєстрації користувачі повинні були внести в застосунок свої персональні дані: ПІБ, номер телефону, адресу проживання, а також інформацію про знайомих, які також підтримують «Лікуд» [115]. Таким чином завдяки збиранню персональних даних про виборців партія мала змогу заохочувати громадян приходити на виборчі дільниці, впливати на їхнє виборче право та як наслідок отримувати більше голосів. Однак через певні технічні недоліки додатку персональні дані майже шести з половиною мільйонів ізраїльтян були доступні для кожного [116]. Помилка системи дозволила завантажити цей реєстр виборців будь-кому. Прагнення політиків підвищити явку осіб на виборах завдяки великим даним закінчилися провалом і серйозним порушенням порядку доступу до персональних даних, прав людини на повагу до приватного життя та на конфіденційність.

Станом на сьогодні люди не можуть бути впевнені в тому, що вони мають повний захист від так званого зливу їхньою персональною інформацією. Зі стрімким розвитком технологій кібербезпека стає передовою в державному управлінні. Шахрайство з використанням даних здійснюється за допомогою соціальної інженерії. Зокрема, останнім часом значного поширення набув такий вид шахрайства як вішинг, мета якого полягає в отриманні реквізитів банківських карток осіб через телефонні дзвінки [117]. Представляючись представником банку, злочинці прагнуть заволодіти фінансовими активами індивіда. Можливі ситуації, коли працівники банку, у якому не обслуговується людина, телефонують, пропонуючи свої послуги. Тому можна дійти висновку, що передані клієнтами банківських установ відомості потрапляють до третіх осіб, чим порушується конфіденційність громадян.

Згадані вище камери відеоспостереження, встановлені на вулицях міст, також несуть потенційну загрозу правам людини. Завдяки цим пристроям можна ідентифікувати особу, так як потрапивши хоча б один раз в об'єктив відеокамери ці дані зберігаються в системі протягом невизначеного часу. Станом на сьогодні в Україні такі комплекси використовуються переважно органами місцевого самоврядування задля забезпечення належного порядку в місті. Незважаючи на правову та благородну мету, у законодавстві відсутні правові підстави для встановлення камер відеоспостереження представниками місцевої влади [118, с. 16]. Можливим є посилання на статтю 38 Закону України «Про місцеве самоврядування в Україні», яка встановлює повноваження органів сільських, селищних і міських рад щодо забезпечення законності, правопорядку, охорони прав, свобод і законних інтересів громадян. Чинним законодавством України зображення особи чітко не належить до персональних даних, тому такі прогалини закону не накладають на адміністраторів систем відеоспостереження прямого обов'язку із захисту отриманої інформації [119]. Таким чином порядок дотримання правових вимог щодо збирання, обробки та зберігання даних про громадян у випадках використання систем відеонагляду по суті не вимагається на законодавчому рівні. Як наслідок, можливі зловживання з отриманою через відеозаписи інформацією, неправомірний доступ до неї та використання.

Наприклад, в 2019 році в Україні громадянин Киргистану намагався встановити вибухонебезпечний пристрій на машину співробітника Головного управління розвідки Міністерства оборони України, однак через невідомі несправності йому цього не вдалося [120]. Інформацію щодо місцезнаходження автомобіля потерпілого злочинця отримав саме завдяки камерам відеоспостереження «Smart city», доступ до яких мав його родич, співробітник правоохоронного органу [121]. Відповідно нерегульований порядок використання широко розповсюджених камер відеозапису може мати зворотній ефект – не запобігання правопорушенням, а їхнє вчинення.

Що стосується побутового життя, зазвичай, особа, замовляючи будь-який товар або послугу в мережі Інтернет, підписує згоду на обробку персональних даних при

отриманні адміністративних послуг і, не замислюючись, погоджується на запропоновані умови. Задля отримання бажаного блага вказує свої дані (наприклад, прізвище, ім'я, номер телефону, професію тощо). Найбільшою загрозою такої дії є те, що передана інформація залишиться в базі відповідного органу державної влади чи компанії назавжди, а надійність технологічної системи від злому та інших хакерських атак не гарантована. Більше того, мета використання цієї інформації не завжди є правовою.

Загалом інформаційний тероризм, зокрема його вид – кібертероризм, як один із найнебезпечніших злочинів 21 століття характеризується тим, що «він не має національних меж» [122, с. 137] і тому знайти суб'єкта цього правопорушення досить важко. До того ж методи та способи діяльності кібертерористів удосконалюються паралельно зі способами захисту від хакерських атак, що робить їх майже непереможними [122, с. 137]. Вагому роль у запобіганні такого виду злочинів повинні відігравати держави шляхом запровадження надійних механізмів контролю за несанкціонованим використанням даних і убезпечення вже отриманих даних від втрати.

У контексті цієї проблеми не можна не згадати про відносно нещодавній скандал з розповсюдженням персональних даних громадян, а саме: водійських прав, на анонімному телеграм-каналі UA Baza [123]. Правопорушником у цій ситуації безліч осіб визнали саме мобільний застосунок «Дія», який має доступ до водійських посвідчень його користувачів. У будь-якому випадку, враховуючи специфіку таких правопорушень, досить важко знайти особу, відповідальну за такі порушення прав суб'єктів персональних даних. Подібні інциденти провокують недовіру до суб'єктів публічної адміністрації та їхнього неналежного виконання своїх обов'язків щодо захисту даних та прав на невтручання в приватне життя своїх громадян.

У січні 2022 року знову було здійснено провокацію, відповідно до якої у мережі Інтернет з'явилося повідомлення щодо продажу персональних даних українців, нібито отриманих з Порталу. Мінцифри заперечило цей факт і наголосило на тому, що така дія є частиною гібридної війни, яку веде росія, а дані громадян під

надійним захистом [124]. Знову великі дані стали приводом до заподіяння шкоди національним і приватним інтересам.

Наведені вище приклади яскраво ілюструють порушення представниками державної влади права на приватне життя особи, передбачене зокрема ст. 32 Конституції України та ст. 8 Конвенції про захист прав людини і основоположних свобод (далі – ЄКПЛ) [125]. Недотримання меж можливого втручання в особисте життя громадян та безвідповідальне використання їхніх даних призведе до тотального контролю з боку держави. У контексті цього питання важливо пам'ятати про дотримання принципу пропорційності між можливим втручанням в приватне життя осіб, необхідного для досягнення легітимної мети.

3.2. Механізми захисту прав людини від неправового застосування big data

3.2.1. Міжнародне та національне законодавство у сфері кібербезпеки та захисту персональних даних

Питання захисту персональних даних є досить важливим для міжнародної спільноти. Першим і основним міжнародним нормативно-правовим актом, який забезпечив право осіб на безпечне використання їхніх даних, стала Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних (далі – Конвенція). Незважаючи на відносно давній рік прийняття, 1981-й, Конвенція досі є актуальною та загальнозживаною.

Положення Конвенції встановлюють основні принципи захисту персональних даних при їхній автоматизованій обробці, до яких належать сумлінне та законне отримання даних, сумісне з визначеними та легальними цілями зберігання даних, їхня точність та адекватність [126]. Сторони Конвенції зобов'язуються дотримуватися основоположних прав людини, зокрема права на приватне життя, та згідно з ч. 1 ст. 3 Конвенції застосовувати її норми не лише в державному, але й приватному секторі.

У 2018 році Рада Європи прийняла Протокол CETS № 223, яким було внесено ряд змін до Конвенції, що модернізували її норми. Наприклад, до принципів обробки даних додано пропорційність, прозорість, мінімізацію, а до обов'язків Сторін Конвенції – вживання ефективних заходів для виконання умов Конвенції [127].

Сьогодні у сфері захисту даних на теренах Європи ключовим і найбільш дієвим є Загальний регламент про захист даних, прийнятий Європейським парламентом у 2016 році (далі – Регламент). Норми Регламенту встановили нові стандарти у сфері захисту приватності осіб і запобігання несанкціонованого вторгнення в особисті дані. Згідно з п. (11) ст. 1 Регламенту згода суб'єкта даних для опрацювання даних може бути виражена не лише у формі заяви, а й у будь-якій ствердній дії, яка конкретно підтверджує бажання особи на опрацювання своїх даних [128]. Більше того, Регламентом встановлено право на відкликання цієї згоди. Ця нібито формальність є гарантією забезпечення правомірного використання отриманої від індивіда інформації.

Важливим аспектом цього документу є надання статтею 17 Регламенту суб'єктам даних права на стирання свої персональних даних (так зване право на забуття), яке, зокрема, органи державної влади зобов'язані здійснити. Зміст цього права полягає в можливості суб'єкта даних вимагати видалення персональних даних з мережі Інтернет, які відображаються після введення в пошукову систему його імені. Підставою для такого вилучення повинні бути визначені Регламентом обставини, як наприклад, зникнення мети для обробки та зберігання таких даних, відкликання згоди на обробку, відсутність легітимних засад для обробки. Ця норма стала революційною у сфері захисту персональних даних, адже надає право вибору, свободу та безпеку суб'єкту даних.

Право на забуття є важливим гарантом забезпечення захисту персональних даних і права на приватне життя осіб, адже з часом та чи інша інформація про індивіда може стати нерелевантною та наносити шкоду суб'єкту даних. Тривале зберігання певних відомостей у відкритому доступі є серйозною проблемою сьогодення, вирішити яку мають на меті положення Регламенту.

Зокрема, такі технологічні гіганти як Google та Meta, що володіє соціальною мережею Facebook, стали заручниками проблеми дотримання права на забуття. Згідно з опублікованим Звітом про доступність сервісів і даних з 2015 по 2022 рік до Google було направлено більше 1 000 000 запитів та майже 5 000 000 URL-адрес на видалення, з яких найбільша кількість відсилала до домену Facebook [129]. Незважаючи на запевнення головного директора Meta Марка Цукерберга в Європарламенті в тому, що його соціальна мережа дотримується вимог Регламенту, статистика наявних порушень права на забуття досі невтішна.

За порушення положень Регламенту встановлені досить високі адміністративні штрафи, які досягають розміру до 20 мільйонів євро (п. 5 ст. 83 Регламенту). Така серйозна відповідальність, на мою думку, є належною, зважаючи на масштабність проблеми захисту персональних даних. Згідно з результатами дослідження міжнародної юридичної фірми DLA Piper за два роки дії Регламенту загальна сума накладених штрафів досягнула 272 мільйонів євро [130]. Відповідна статистика ілюструє, що проблеми в дотриманні норм Регламенту в Європі все ще існують, однак ефективність його застосування є безумовною.

Яскравим прикладом захисту персональних даних у США є Каліфорнійський закон про захист конфіденційності споживачів (California Consumer Privacy Act). У багатьох аспектах цей нормативно-правовий акт відображає положення Регламенту. Головними особливостями американського закону є те, що він досить широко трактує поняття персональних даних, до яких належать псевдоніми, геолокація, інформація про освіту, пости в соціальних мережах, а також за умовчанням дозволяє «продаж даних» третім особам з правом вимагати видалення даних і припинення їхнього продажу [131]. Сфера дії цього акту поширюється лише на штат Каліфорнія, однак зважаючи на те, що саме там розташована та зареєстрована найбільша кількість світових технологічних і бізнес-компаній, його актуальність і дієвість є беззаперечними.

Уперше питання кібербезпеки врегулювала Конвенція Ради Європи про кіберзлочинність. Цей документ не надає конкретного визначення кіберзлочину, однак групує ці правопорушення на такі категорії: проти конфіденційності,

цілісності та доступності комп'ютерних даних і систем, пов'язані з комп'ютерами, зі змістом та з порушенням авторських та суміжних прав [132]. Конвенція про кіберзлочинність у статті 22 містить важливі для кіберпростору положення, які визначають юрисдикцію вчинення кіберзлочинів. Згідно з ч. 1 ст. 22 цього акту на правопорушення, визначені Конвенцією, поширюється територіальна юрисдикція, а у випадках вчинення злочину поза межами територіальної юрисдикції держави застосовується кримінальне законодавство держави, громадянином якої є злочинець. Зважаючи на особливість і безмежність кіберпростору, Конвенція про кіберзлочинність у ч. 5 ст. 22 закріплює можливість для Сторін Конвенції у випадках колізії проводити консультації щодо визначення найбільш придатної юрисдикції для переслідування. Завдяки аналізу норм цієї конвенції можна дійти висновку, що незважаючи на її революційність і фундаментальність, вона не вирішує всі виклики технологічного сьогодення. Відповідно тому належна реалізація її положень і подальше прийняття суміжних нормативно-правових актів здатні боротися з поширеною кіберзлочинністю.

Станом на сьогодні питання кібербезпеки не є пріоритетним в Україні. На жаль, у нашій державі законодавство щодо забезпечення інформаційної безпеки не достатньо розвинене, не розроблений чіткий механізм захисту громадян від неправового доступу та використання їхніх даних, притягнення до відповідальності за такі дії.

Стаття 32 Конституції України забороняє збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди.

Головним нормативно-правовим актом в Україні, який регулює питання, пов'язані з великими даними, є згаданий вище Закон. Сфера цього Закону визначає порядок і правові підстави обробки персональних даних: їхнє збирання, накопичення, зберігання, поширення, видалення або знищення. Варто звернути увагу на те, що обробка персональних даних згідно з Законом означає будь-які дії володільця інформації щодо них і не виключно із сукупністю таких даних (наприклад, реєстром або базою) [133, с. 23]. Обробка можлива лише за визначених Законом обставин.

Прийняття Регламенту сприяло внесенню змін до Закону, у результаті чого багато його норм повторюються й в українському законодавстві. Зокрема, також передбачена обов'язкова згода суб'єкта персональних даних на обробку інформації, а цілі такої обробки повинні бути конкретними та законними відповідно до ст. 6 Закону. П. 11 ч. 2 ст. 8 Закону надає суб'єкту даних й право відкликати надану згоду.

Якщо розглядати дієвість Закону, то можна виявити більше його недоліків, ніж переваг. Наприклад, передбачений Законом порядок доступу третіх осіб до персональних даних не є досконалим, адже він не зобов'язує проводити ідентифікацію такого запитувача інформації шляхом, наприклад, особистого подання запиту чи використання електронного цифрового підпису [133, с. 152].

Стаття 24 Закону встановлює обов'язок володільців і розпорядників даних, серед яких зокрема і органи державної влади, забезпечувати захист цих даних, однак конкретний порядок досягнення цієї мети досі не розроблений. Після ратифікації Україною Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних і Додаткового протоколу до неї до Закону були внесені зміни, що поклали на Уповноваженого Верховної Ради України з прав людини (далі – Уповноважений) функції з контролю за дотриманням законодавства про захист персональних даних. Контроль передбачає проведення Уповноваженим перевірок, складання акту, який інформує про наявність або відсутність порушень згідно з ч. 1 ст. 23 Закону. Уповноважений має право здійснити захід реагування у вигляді видання припису або складання протоколу про адміністративне порушення, передбаченого ст. 188-39 Кодексу про адміністративні правопорушення [134].

Зазначена адміністративна відповідальність не є достатньо ефективною та надійною, адже ч. 4 ст. 188-39 КУпАП встановлює накладення штрафу за порушення прав суб'єкта персональних даних лише у випадку недодержання правопорушником порядку захисту цих даних [135]. Відповідна прив'язка саме до порядку захисту даних значно обмежує сферу дії цієї статті. Загалом будь-яке порушення встановлених прав суб'єкта персональних даних повинно призводити

до негативних наслідків для особи, яка його вчинила, а таке звужене формулювання законодавчої норми робить її застосування майже неможливим.

Відсутність адміністративної відповідальності юридичних осіб також сприяє порушенню права осіб, чиї дані було незаконно використано, адже виявити конкретну особу, яка працює в тому чи іншому державному органі та порушила вимоги законодавства щодо захисту персональних даних, досить важко.

Незважаючи на закріплення в п. 8 ч. 2 ст. 8 Закону права на звернення зі скаргами на обробку своїх персональних даних не лише до Уповноваженого, а й до суду, ще одним недоліком Закону є відсутність права на компенсацію у випадку задоволення такого виду скарг [133, с. 146].

Відповідно станом на сьогодні українське законодавство у сфері захисту персональних даних потребує внесення ряду змін і доповнень. Задля належної взаємодії суб'єктів публічної адміністрації і громадян, дієвого механізму захисту прав людини варто створити окремий незалежний орган, головними функціями якого буде нагляд і дотримання прав людини щодо їхніх персональних даних з правом виявляти, розслідувати та визнавати правопорушеннями такі дії, що суперечать законодавству у сфері захисту персональних даних.

У 2021 році до Верховної Ради України було подано два законопроекти, що покликані реформувати сферу захисту персональних даних і привести українське законодавство у відповідність до міжнародних правових норм. Проект Закону України «Про захист персональних даних» передбачає оновлений механізм обробки персональних даних, містить змістовний перелік важливих термінів для захисту прав суб'єкта даних, деталізує вимоги до надання згоди для обробки персональних даних, розширює права суб'єктів даних, а також регламентує порядок обробки персональних даних у правоохоронних цілях [136]. Законопроект 5628 посилює захист персональних даних шляхом обов'язкового призначення представниками органів державної влади посадової особи, відповідальної з питань захисту персональних даних [136]. Впровадження норм європейського законодавства, що відображені в цьому законопроекті, оновить застарілий і недієвий механізм регулювання захисту персональних даних у нашій країні.

Загалом прийняття такого закону позитивно вплине на захист прав людини, розвиток приватних компаній і подальшу діджиталізацію державного сектору в Україні.

Другий законопроект 6177 передбачає створення нового центрального органу виконавчої влади Національної комісії з питань захисту персональних даних та доступу до публічної інформації (далі – Національна комісія). Цей контролюючий орган покликаний забезпечити державну політику у сфері захисту персональних даних та доступу до публічної інформації, а також здійснювати державний контроль за дотриманням законодавства про захист персональних даних та/або доступу до публічної інформації [137]. На відміну від Уповноваженого, який у зв'язку з відсутністю необхідних повноважень, Національна комісія матиме компетенцію щодо прийняття активних рішень для запобігання правопорушенням з персональними даними. Окрім запровадження вузькопрофільної і чітко визначеної спеціалізації нового органу, законопроект відповідає важливим міжнародним стандартам, дотримання яких є необхідним для України як правової сучасної держави.

Незважаючи на наявність нормативно-правових актів, які регулюють сферу захисту персональних даних, усе ж найбільш дієвим способом забезпечення прав людини сьогодні є ретельна перевірка суб'єктів, яким передається особиста інформація, мети здійснення такої передачі, а також правил обробки персональних даних. Українське законодавство лише зароджується в цій галузі, тому поки не може належно та ефективно захистити від неправового використання даних і, як наслідок, втручання в приватне життя. Прийняття оновлених і сучасних законопроектів у сфері захисту персональних даних є необхідним для належного забезпечення прав людини в Україні.

3.2.2. Суб'єкти публічної адміністрації з кібербезпеки та захисту персональних даних в Україні

Зважаючи на потенційні ризики, які може нести неправомірне використання великих даних, необхідно знати та розуміти, які органи державної влади відповідальні за інформаційну та кібербезпеку України, а також захист персональних даних громадян.

Згаданий вище Закон України «Про основні засади забезпечення кібербезпеки України» у статті 5 відносить до безпосередніх суб'єктів забезпечення кібербезпеки Президента України через РНБО, Національний координаційний центр кібербезпеки, КМУ, а також центральні органи виконавчої влади, правоохоронні, розвідувальні та контррозвідувальні органи.

Мінцифри, будучи основним органом впровадження великих даних у державну діяльність, розробляє пропозиції щодо прийняття або внесення змін до нормативно-правових актів з питань захисту персональних даних згідно з пп. 13 п. 4 Положення про Мінцифри, бере участь у формуванні державної політики щодо технічного захисту інформації та кіберзахисту згідно з пп. 14 п. 4 Положення про Мінцифри. Першочергове завдання міністерства у сфері кібербезпеки полягає у створенні таких технологічних продуктів, застосування яких не нанесе шкоди персональним даним його користувачів.

Постановою КМУ №885 було затверджено Положення про Міністерство культури та інформаційної політики (далі – МКІП). До повноважень міністерства належать, зокрема, розробка програмних документів у сфері захисту інформаційного простору України від зовнішнього інформаційного впливу згідно з пп. 147 п. 4 Положення про МКІП і технічний захист інформації відповідно до пп. 5 п. 5 Положення про МКІП [138]. Забезпечення інформаційної безпеки міністерство здійснює як безпосередньо, так і через свої структурні підрозділи. Наприклад, створений при МКІП у 2021 році Центр стратегічних комунікацій покликаний протидіяти дезінформації, розбудовувати стратегічні комунікації та співпрацювати з міжнародними партнерами задля інформування щодо гібридної війни росії [139]. Окрім того, до повноважень цього органу належать постійний моніторинг і попередження про наявні чи потенційні інформаційні атаки країни-агресора на власному сайті, офіційних сторінках у соціальних мережах і месенджерах, а також

підвищення рівня компетентності державних службовців у гібридних кіберзагрозах шляхом проведення тренінгів [140]. Відповідно Центр виконує важливу роль у протидії інформаційній небезпеці, попереджуючи як представників органів державної влади, так і громадян, а також контролює рівень обізнаності міжнародної спільноти про неправомірні дії росії під час війни.

На офіційному сайті МКІП можна також ознайомитися із систематизованими даними щодо ведення інформаційної війни проти російської федерації [141]. До механізмів протидії агресії належать зібрані МКІП фото та відеоматеріали, які доводять присутність російських військ на території українського Донбасу [142], що стануть доказами для Міжнародного кримінального суду, добірка українських видань, які висвітлюють суспільне, політичне та економічне життя в анексованому Криму [143], та інтернет-ресурси, які публікують матеріали щодо війни в Україні, роботи російських пропагандистських ЗМІ та блогерів, достовірні факти щодо історії української державності [139]. Станом на сьогодні МКІП відіграє надзвичайно важливу роль у протидії інформаційних атак, забезпеченню не лише українського, але й світового суспільства правдивими фактами та задокументованими матеріалами, а також гарантує дотримання прав і свобод громадян від неправомірного доступу до їхніх персональних даних.

Важливим гарантом забезпечення прав і свобод людини в Україні є РНБО. У контексті інформаційної безпеки та захисту персональних даних варто звернути увагу на такий робочий орган РНБО як Центр протидії дезінформації (далі – Центр), створений відповідно до рішення РНБО від 11 березня 2021 року [144], уведеного в дію указом Президента України №106/2021 [145]. Серед основних завдань Центру згідно з п. 6 Положення про Центр є виявлення та вивчення поточних і прогнозованих загроз інформаційній безпеці України, чинників, які сприяють цьому, пошук та протидія дезінформації, а також протидія пропаганді [146]. Головною метою створення цього органу було забезпечення інформаційної безпеки у зв'язку з активним веденням гібридної війни та стрімким поширенням неправдивих даних.

Загалом Центр створює надійну та ефективну інформаційну основу для боротьби проти фейків як в медіа, так і в Інтернет-мережі, викриває недостовірні дані та маніпуляції з боку ворога та активно інформує населення щодо потенційних загроз задля забезпечення національної безпеки України. Одним із проєктів Центру була підготовка та опублікування разом з Апаратом РНБО глосарію щодо правильного та правового вживання термінів, які використовуються для освітлення збройної агресії росії проти України [147].

Під час повномасштабної війни на території України Центр неодноразово наголошував на тому, щоб українці дбали про свою кібербезпеку та не користувалися російськими сайтами, а також завжди перевіряли правильність посилання, за яким вони переходять. Така необачність може призвести не лише до загрози персональним даним, але й інформаційній безпеці України загалом.

На відміну від Центру стратегічних комунікацій, головними завданнями якого є створення належного рівня обізнаності українців у питаннях дезінформації, проведення інфокомпаній і комунікаційних стратегій, навчання громадян щодо виявлення фейків, Центр здійснює конкретні заходи із забезпечення інформаційної безпеки та протидії інформаційним загрозам шляхом надання РНБО необхідних матеріалів та аналітики, підготовкою конкретних пропозицій і планів дій задля захисту національних інтересів держави.

Національний координаційний центр кібербезпеки як робочий орган РНБО відповідно до п. 3 Положення про Національний координаційний центр кібербезпеки контролює діяльність суб'єктів, які забезпечують кібербезпеку, аналізує та контролює стан кібербезпеки в державі, прогнозує та виявляє потенційні загрози, розробляє та впроваджує нові механізми протидії кіберзагрозам [148]. Цей орган був створений як частина реалізації Стратегії кібербезпеки України та має на меті підвищити рівень кіберзахисту.

Постановою КМУ №831 було створено Департамент кіберполіції як міжрегіональний територіальний орган Національної поліції (далі – кіберполіція) [149]. Саме цей орган реалізовує державну політику у сфері протидії кіберзлочинності [150] та є провідним у кіберзахисті України.

Діяльність кіберполіції полягає в розкритті злочинів, вчинених шляхом створення фішингових ресурсів, фішингових атак, онлайн-шахрайств, вчинених з використанням соціальних мереж, месенджерів і телеграм-каналів, запобіганні розповсюдженню порнографічних матеріалів. Відповідно цей правоохоронний орган працює з правопорушеннями, способами вчинення яких були великі дані та які посягають на інформаційну безпеку та персональні дані осіб.

Зокрема, під час війни кіберполіція викрила безліч злочинців, які ошукували людей під виглядом збору гуманітарної допомоги чи надання державних виплат, перевезення з місць бойових дій, а також заблокувала багато Інтернет-ресурсів ворога, які розміщували неправдиву інформацію, російську пропаганду та вводили людей в оману. Таким чином прогресивні органи державної влади, які захищають кіберпростір України, за допомогою великих даних і технологічних знань запобігають вчиненню правопорушень щодо персональних даних осіб і національної безпеки держави.

До суб'єктів захисту персональних даних та інформаційного простору загалом належить і Служба безпеки України (далі – СБУ). Згідно з ч. 1 ст. 10 Закону України «Про СБУ» до складу Центрального управління СБУ належить підрозділ контррозвідального захисту інтересів держави у сфері інформаційної безпеки [151]. Створений Ситуаційний центр забезпечення кібербезпеки СБУ здійснює діяльність щодо протидії кіберрозвідкам іноземних держав, боротьбі з кібертероризмом і кібершпигунством [152].

Кіберспеціалісти СБУ викривають колишніх співробітників правоохоронних органів, які продають персональні дані українців, перехоплюють телефонні розмови російських окупантів на території України, ліквідовують Інтернет-мережі ворожих інформаційних агентів, притягують до відповідальності хакерів.

Станом на сьогодні в Україні суб'єкти публічної адміністрації активно виконують свої функції із захисту персональних даних громадян і кіберпростору та забезпечення інформаційної безпеки. Створення, масштабний розвиток і широка сфера впливу на правовідносини в Україні цих органів виконавчої влади гарантують дотримання і захист основоположних прав людини.

Розповсюдження великих даних у різних сферах життєдіяльності та їхнє щоденне нагромадження кидають виклики суб'єктам публічної адміністрації належним чином контролювати ці процеси. Стрімкий розвиток технологій збільшує кількість неправомірних дій за допомогою big data, саме тому велика відповідальність покладається саме на володільців і розпорядників персональних даних в особі органів державної влади, які є гарантами дотримання прав людини.

Фундамент міжнародного законодавства у сфері захисту персональних даних і кібербезпеки вже покладено, а в Україні лише зароджується. Незважаючи на це, велика кількість органів державної влади, до компетенції яких належить забезпечення порядку в інформаційному та кіберпросторі, відіграють велику роль у забезпеченні інформаційної безпеки осіб.

Недосконалий механізм захисту персональних даних громадян змушує їх детально та відповідально ознайомлюватися з умовами надання згоди на обробку своїх даних під час будь-якого правочину або взагалі обмежити обсяг такої інформації. Вирішенням цих проблем стане приведення норм українського законодавства до міжнародних стандартів у сфері захисту персональних даних та інформаційної безпеки загалом, створення окремих незалежних адміністративних органів, які здійснюватимуть контроль за дотриманням прав людини саме під час діяльності суб'єктів публічного адміністрування та приватних компаній з їхніми даними, а також розширення ареалу інформаційних прав громадян.

РОЗДІЛ 4

СУДОВА ПРАКТИКА У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Важливу роль у сфері захисту персональних даних, звичайно, відіграють суди. Станом на сьогодні в Україні практика розгляду справ щодо захисту персональних даних (зокрема, у контексті порушення статті 188-39 КУпАП) не є занадто розповсюдженою. Незважаючи на це, наявні рішення українських судів різних інстанцій внесли фундаментальні зміни та значно розширили розуміння проблеми порушення прав людини шляхом неправомірного використання не лише великих даних, але й персональних даних.

Перше та головне, на мою думку, рішення, яке необхідно розглянути в контексті дослідженої проблеми є рішення Конституційного Суду України (далі – КСУ) від 20 січня 2012 року, у якому було надано офіційне тлумачення частин 1 та 3 статті 32 Конституції України. Відповідно КСУ до персональних даних відніс «національність, освіта, сімейний стан, релігійні переконання, стан здоров'я, матеріальний стан, адреса, дата і місце народження, місце проживання та перебування тощо, дані про особисті майнові та немайнові відносини цієї особи з іншими особами, зокрема членами сім'ї, а також відомості про події та явища, що відбувалися або відбуваються у побутовому, інтимному, товариському, професійному, діловому та інших сферах життя особи, за винятком даних стосовно виконання повноважень особою, яка займає посаду, пов'язану зі здійсненням функцій держави або органів місцевого самоврядування» [153]. КСУ вперше надав перелік відомостей про особу, що становлять її персональні дані, а також відніс цю інформацію до конфіденційної. До того ж у своєму визначному рішенні КСУ зазначив, що «збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди державою, органами місцевого самоврядування, юридичними або фізичними особами є втручанням в її особисте та сімейне життя. Таке втручання допускається винятково у випадках, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини» [153].

Надзвичайно важливим, на мою думку, є рішення КСУ від 11 жовтня 2018 року, у якому було визнано неконституційними норми Бюджетного кодексу України, відповідно до яких: «під час здійснення повноважень з контролю за дотриманням бюджетного законодавства...Міністерство фінансів України має право на безоплатне отримання інформації, що містить банківську таємницю, персональні дані, та на доступ до автоматизованих інформаційних і довідкових систем, реєстрів та банків даних, держателем (адміністратором) яких є державні органи або органи місцевого самоврядування» [154].

КСУ наголошує на тому, що «відсутність будь-яких меж дискреції, встановленої законом, щодо подальших дій з інформацією, яка містить персональні дані, унеможлиблює навіть мінімальний захист суб'єкта персональних даних» [154], і таким чином оспоровані норми порушують «такі елементи принципу верховенства права як юридична визначеність і заборона свавілля» [154], що в результаті може порушити право на приватне життя громадян.

У рішенні від 22 січня 2020 року КСУ знову зробив свій вагомий внесок у сфері захисту персональних даних, а саме зазначив, що конституційна скарга, на відміну від конституційного звернення та подання, є «індивідуальною формою звернення до КСУ та містить персональні дані особи» [155], тому не може бути оприлюднена назагал. Встановлена ч. 4 ст. 42 ЗУ «Про Конституційний Суд» заборона на надання інформації за запитами щодо матеріалів справи, яку розглядає суд, має «легітимну мету та спрямована на захист конфіденційної інформації про особу» [155]. Така позиція КСУ ілюструє розуміння держави щодо того, наскільки важливим і необхідним є належно встановлений правовий захист персональних даних.

Не досить поширеною, однак важливою є практика Верховного Суду у сфері захисту персональних даних. Наприклад, Верховний Суд України у своїй постанові від 27 вересня 2017 року звернувся до питання відшкодування моральної шкоди за неправомірне розповсюдження персональних даних. Зокрема, суд звернув увагу, що суди попередніх інстанцій «не звернули уваги на те, що позивач пов'язував моральну шкоду зі спричиненими йому неправомірними діями відповідача душевними стражданнями» [156], а тому при винесенні своїх рішень керувалися

лише тим, що «факт розповсюдження персональних даних не може бути підтвердженням завдання моральної шкоди» [156]. Верховний Суд України наголосив на тому, що «суди мали б виходити з презумпції спричинення позивачу моральної шкоди відповідачем та обов'язку саме відповідача спростувати таку презумпцію» [156]. Такою правовою позицією суд забезпечує захист прав суб'єктів даних.

Ще однією важливою позицією у захисті від неправомірного втручання органів державної влади в приватне життя людини (зокрема, шляхом використання їхніх персональних даних) є позиція Верховного Суду в постанові від 16 квітня 2020 року. Відповідно Верховний Суд зазначив, що «виконання службових обов'язків не дозволяє посадовій особі діяти в межах «якщо не заборонено, то дозволено», оскільки недотримання чітко визначених повноважень, або відповідних процедурних правил, є свавіллям з боку уповноважених осіб» [156]. Така аргументація суду щодо неправомірного розголошення керівником апарату суду персональних даних іншої особи є позитивною прикладом у сфері захисту прав людини від перевищення повноважень органів державної влади.

Судова практика також підкреслює певні неточності українського законодавства у сфері захисту персональних даних. Так, наприклад, Велика Палата Верховного Суду при розгляді справи №806/3265/17 звернула увагу на те, що українським законодавством «не врегульовано питання щодо наслідків відмови особи від обробки її персональних даних, тобто фактично відсутня будь-яка альтернатива такого вибору, що у свою чергу обумовлює неякість закону та порушення конституційних прав такої особи» [158]. Відповідно суд наголошує на тому, щоб відмовитися від примушування громадян до надання згоди на обробку їхніх даних необхідно керуватися законодавчо закріпленими принципами відкритості, прозорості та адекватності обробки даних, а також використовувати «традиційні методи ідентифікації особи у випадках відмови від обробки» [158].

Аналізуючи судову практику судів першої та апеляційної інстанцій за порушення законодавства у сфері захисту персональних даних, я дійшла висновку, що найчастіше притягають до відповідальності за ч. 4 ст. 188-39 КУпАП. Гіпотеза цієї

статті викладена досить загально, зокрема, не конкретизовано, які саме діяння можуть порушити «порядок захисту персональних даних». Для кращого розуміння дії ч. 4 ст. 188-39 КУпАП у повсякденному житті я пропоную ознайомитися з підготовленим аналізом судової практики.

Найпоширенішими діями, які суди відносять до недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, є:

- розміщення зверення третьої особи, яке містить її персональні дані, в месенджері Viber/мережі Facebook [159; 160; 161; 162; 163];
- опублікування на офіційному вебсайті/сторінці Facebook міської ради рішення органу виконавчої влади та/або інша публікація з персональними даними третіх осіб [164; 165; 166; 167; 168; 169; 170; 171];
- опублікування на офіційному вебсайті університету наказу, який містить персональні дані третіх осіб [172; 173; 174; 175; 176];
- розміщення на біл-бордах/дошках об'яв персональних даних боржників [177; 178];
- надання державним службовцем інформації про дату призначення другій особі пенсії [179];
- надання державним службовцем довідки про перелік власників майнових паїв [180];
- розміщення відеозапису з оголошенням листа, у якому зазначені персональні дані ймовірних учасників вчиненого раніше правопорушення [181];
- розміщення в мобільному додатку персональних даних [182];
- надсилання на персональну електронну адресу список військовозобов'язаних працівників з їхніми персональними даними [183];
- поширення персональних даних боржників представником органу виконавчої влади у соціальній мережі Facebook [184];
- опублікування на сайті ПрАТ персональних даних [185].

З чого можна зробити висновок, що зазвичай, порушення захисту персональних даних здійснюється шляхом використання мережі Інтернет, а також інших

технологічних сервісів. Потрапивши один раз у загальний доступ Інтернету, дані тієї чи іншої особи буде досить складно видалити назавжди.

Важливою особливістю є також те, що в більшості випадків суб'єктом такого виду правопорушення є представники органів державної влади. На жаль, проведений мною аналіз доводить те, що станом на сьогодні в Україні суб'єкти владних повноважень не забезпечують належний захист персональних даних громадян.

Захист персональних даних розглядається та захищається Європейським судом з прав людини (далі – ЄСПЛ) крізь призму встановленого статтею 8 ЄКПЛ права на приватне життя. Відповідно порушення встановленого порядку обробки чи доступу персональних даних є вторгненням у приватне життя особи. Правові позиції ЄСПЛ щодо дослідженої теми є надзвичайно важливими, адже вони розширюють ореол можливих порушень і механізмів захисту приватного життя. У різних справах ЄСПЛ вносив свій вагомий внесок у захист персональних даних і запроваджував нові підходи до розуміння та сфери дії статті 8 ЄКПЛ.

У справі «Гаскін проти Сполученого Королівства» ЄСПЛ наголошує на тому, що право на доступ до власних персональних даних повинно забезпечуватися органами державної влади через право на повагу до приватного та сімейного життя [186, ст. 57]. У цьому рішенні суд звернув увагу на тому, що у справах щодо захисту персональних даних важливо також не забувати про досягнення принципу пропорційності. ЄСПЛ зазначив, що суб'єкт даних має право «отримати доступ до матеріалів про його особисте і сімейне життя при досягненні конфіденційності державних архівів, яка може бути необхідна для захисту третіх осіб» [186, ст. 60]. Неодноразово ЄСПЛ звертав увагу на захист інформації про стан здоров'я осіб. Зокрема, у справі «М. С. проти Швеції» ЄСПЛ зазначив, що «дотримання конфіденційності відомостей про здоров'я є основоположним принципом правових систем держав-учасниць ЄКПЛ» [187, п. 41]. А у справі «Z проти Фінляндії» ЄСПЛ визнав, що розголошення апеляційним судом у своєму рішенні відомостей про те, що заявниця є ВІЛ-інфікованою, порушило її право на приватне життя [188, п. 80, 85].

Ще одним важливим аспектом захисту відомостей про стан здоров'я є період можливого зберігання таких даних. Наприклад, у справі «С. і Марпер проти Сполученого Королівства» ЄСПЛ визнав непропорційним втручанням у приватне життя «зберігання відбитків пальців, клітинних зразків та профілів ДНК підозрюваних, але незасуджених осіб» [189, п. 125].

Цікавою є позиція суду у справі «Кьопке проти Німеччини», яка стосувалася неправомірного здійснення відеоспостереження за особою. З мотивів побоювання вчинення заявницею крадіжки було встановлено відеоспостереження на її робочому місці. ЄСПЛ прийняв рішення не на користь заявниці, адже було досягнуто «справедливого балансу між правом на повагу до приватного життя робітника, захисту майнових прав роботодавця та суспільного інтересу» [190]. У своєму рішенні ЄСПЛ наголосив на тому, що такий обмежувальний захід був необхідним задля запобігання можливим майбутнім більш серйозним злочинам.

Водночас у справі «Аллан проти Сполученого Королівства» ЄСПЛ визнав «використання аудіо- і відеопристроїв у тюремній камері, а також кімнаті для побачень втручанням у право на приватне життя» [191, п. 46, 57].

Згідно з матеріалами справи «Класс та інші проти Німеччини» за поштою та телефонним зв'язком заявників було здійснено таємне стеження, що на їхню думку, порушувало право на приватне життя. ЄСПЛ детально проаналізував німецьке законодавство на відповідність правомірності заходів стеження та дійшов висновку, що органи державної влади повинні були вжити такі заходи, адже вони були «необхідні в демократичному суспільстві в інтересах національної безпеки та запобігання заворушенням і злочинам» [192, п. 60].

Схожою є позиція ЄСПЛ у справі «Уцун проти Німеччини», якою стеження через GPS було визнано пропорційним законній меті [193, п. 78]. Цю пропорційність ЄСПЛ аргументує тим, що «спостереження здійснювалося протягом відносно короткого періоду часу і лише на вихідних або коли підозрюваний їхав у автомобілі» [193, п. 80], а також тому, що такий вид спостереження було обрано лише після того, як менш серйозні методи виявилися недієвими.

Важливою у сфері захисту персональних даних є позиція ЄСПЛ у справі «К.У. проти Фінляндії». Відповідно до обставин справи «невідома особа розмістила на інтернет-сайті знайомств від імені 12-річного заявника оголошення» [194, п. 7]. ЄСПЛ визнав, що це оголошення «мало злочинний характер, зачіпало неповнолітнього громадянина і робило його об'єктом уваги педофілів» [194, п. 45]. Звернути увагу хочу на тому, що ЄСПЛ наголосив, що гарантія свободи думки та конфіденційності повідомлень в Інтернеті «не може бути абсолютною, та за деяких обставин повинна підкорюватися таким задачам як запобігання заворушень або захист прав і свобод інших людей» [194, п. 49].

Міжнародна практика розгляду справ щодо захисту персональних даних стосувалася також і права бути забутим. Уперше ЄСПЛ зіткнувся з проблемою «забуття» у справі «Зегерштед-Віберг та інші проти Швеції». Відповідно до обставин справи заявники в минулому були членами комуністичних революційних партій, одним із принципів яких було насильницький супротив поліції. Ця інформація зберігалася поліцією в базі секретних даних протягом довгого періоду часу, щодо деяких із заявників – аж з 1969 року. ЄСПЛ визнав, що таке тривале зберігання «навіть чи може вважатися достатнім відносно розглянутої справи через тридцять років» [195, п. 90], а тому спричинило непропорційне вторгнення в приватне життя.

Проблему реалізації права на забуття розглядав також і Суд Європейського Союзу. У справі *Google Spain, Google Inc. v AEPD, Mario Costeja González* суд визнав, що у випадку, коли обробка інформації більше нерелевантна, а особа, якої стосується ця інформація, не відіграє суспільно важливої ролі, то такі дані повинні бути видалені з пошукової системи мережі Інтернет [196, п. 94]. Суд ЄС у цьому рішенні наголосив на тому, що суб'єкт даних може адресувати вимогу щодо видалення даних напряму до контролера даних, який зобов'язаний дослідити це питання [196, п. 77]. У випадку відмови контролера в задоволенні такого запиту суб'єкт даних може звернутися до вищого органу державної влади чи до суду [196, п. 77].

У контексті розгляду захисту персональних даних не можна не згадати всесвітньовідому справу герцогині Сассекської Меган Маркл проти видавця

бульварної газети The Mail on Sunday та власника вебсайту MailOnline. Справа стосувалася опублікування цими двома медіа-ресурсами приватного листа герцогині до її батька без її згоди. Вищий Суд Англії та Уельсу визнав, що «зміст листа є приватним і конфіденційним та підпадає під сферу дії статті 8 ЄКПЛ», а тому ЗМІ порушили право на приватне життя заявниці [197, п. 22].

Аналізуючи вітчизняну та міжнародну судову практику, я дійшла висновку, що станом на сьогодні система захисту персональних даних формується не лише в законодавчому полі, але й у судовому. Відносно мала кількість розглянутих українськими судами справ ще не створює усталеної практики захисту права на приватне життя через належне дотримання законодавства у сфері захисту персональних даних. Натомість завдяки прогресу міжнародної судової практики вітчизняні суди мають належний орієнтир для вирішення спорів з дослідженої теми.

Водночас наявні правові позиції судів різних інстанцій удосконалюють та деталізують не зовсім чітке законодавче регулювання сфери захисту персональних даних і започатковують тенденцію звернень громадян до суду задля захисту їхніх прав.

ВИСНОВКИ

Незважаючи на відносно нещодавню появу феномену big data, він уже встиг стати вагомою частиною багатьох не лише підприємницьких, але й державних процесів. Застосування великих даних у публічному адмініструванні характеризується такими особливостями.

1. Станом на сьогодні відсутній як загальний доктринальний, так і нормативний підхід у визначенні явища big data. Норми міжнародного права, зокрема європейського, певною мірою регулюють порядок збирання, використання та обробки даних, однак цей механізм поки не є досконалим. Що стосується українського законодавства, його положення скоріше опосередковано вирішують питання, що стосуються великих даних.
2. Протягом останніх 5 років діджиталізація стала одним із основних векторів державної політики в Україні. За допомогою big data значних удосконалень і змін зазнали наразі сфери надання державних послуг, запобігання правопорушенням, охорони здоров'я, освіти та науки, соціального захисту та кібербезпеки.
3. Суб'єкти публічного адміністрування регулярно впроваджують big data в нові сфери життєдіяльності громадян шляхом модернізації застарілих систем, переведенні більшості державних сервісів на онлайн-платформи та уніфікації наявної в державі інформації. Такі зміни створили максимально комфортні умови користування державними благами, заклали засади для вільного розвитку та встановили цифровий механізм безпеки населення.
4. Застосування великих даних у публічному адмініструванні гарантує прийняття ефективних і дієвих рішень на державному рівні, заощаджує час і відкриває нові можливості для громадян, знижує рівень правопорушень і навіть протидіє ворогу під час війни.
5. Поширення великих даних сприяє розвитку кіберзлочинів, запобіганням яких першочергово повинні займатися органи державної влади. Прийняті українські та міжнародні нормативно-правові акти, сфера дії яких стосується кіберзахисту, а також створені та діючі суб'єкти публічної адміністрації, компетенція яких полягає

в кіберзахисті, стали важливим кроком для зменшення правопорушень у кіберпросторі та забезпеченні інформаційної безпеки.

6. Важливою складовою великих даних є персональні дані, захист яких повинен бути передовим у сфері використання big data. Закон України «Про захист персональних даних» потребує значних змін і оновлень, які заповнять термінологічні прогалини, ґрунтуватимуться на принципах обробки персональних даних, утворюють надійну систему протидії неправомірним доступу та використанню персональних даних і втручання в особисте життя.

7. Недосконалість положень українського законодавства призводить до маніпуляцій з особистою інформацією осіб, а також порушення права на приватне життя. Вирішення цієї проблеми можливе шляхом запровадження дієвого механізму контролю за використанням даних, погодження норм національного законодавства з приписами міжнародного права та встановлення конкретної відповідальності.

8. У зв'язку з відсутністю надійного захисту з боку держави єдиним способом захиститися від несанкціонованого втручання в особисте життя є самостійна фільтрація суб'єкта та мети отримання даних.

9. Судова практика у сфері захисту персональних даних в Україні лише на етапі формування, однак уже розширює область застосування відповідальності за порушення законодавства у сфері захисту персональних даних. З іншого боку правові позиції міжнародних судів є орієнтиром для вирішення вітчизняних судових спорів.

10. Big data у публічному адмініструванні мають свої вагомі переваги для суспільства та розвитку держави, однак водночас станом на сьогодні головною проблемою, яку викликає це використання, є загроза приватному життю громадян.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A short history of Big Data. Big Data Framework. 2019. URL: <https://www.bigdataframework.org/short-history-of-big-data/> (дата звернення: 12.02.2021).
2. Fredriksson C., Mubarak F., Tuohimaa M., Zhan M. Big Data in the Public Sector: A Systematic Literature Review. 2017. URL: https://www.researchgate.net/publication/320911071_Big_Data_in_the_Public_Sector_A_Systematic_Literature_Review (дата звернення: 16.02.2022).
3. Харарі Ювал Ной. Номо деус: за лаштунками майбутнього. Київ: BookChef. 2018. 512 с.
4. Stryker C. Big Data will impact every part of your life. Youtube. TEDx. Talks. 2014. URL: <https://www.youtube.com/watch?v=0Q3sRSUYmys> (дата звернення: 20.02.2021).
5. Шваб К. Четвертая промышленная революция. «Эксмо». 2016. Top Business Awards. 138 с.
6. Апетик А. Чи допомагає Big Data захищати права людини? Експертний центр з Прав Людини. 2020. URL: <https://ecpl.com.ua/news/chy-dopomahaie-big-data-zakhyshchaty-prava-liudyny/> (дата звернення: 12.02.2021).
7. Clifford A. Lynch. Big data: How do your data grow? Nature, vol. 455, no. 7209. 2008. 28-29 p.
8. Ramesh Dontha. The Origins of Big Data. KDnuggets. 2017. URL: <https://www.kdnuggets.com/2017/02/origins-big-data.html> (дата звернення: 12.02.2021).
9. Старжинський А. Як українці працюють з Big Data. НВ Бізнес. 2016. URL: https://nv.ua/ukr/biz/experts/yak-ukrajinci-pracyuyut-z-big-data-220125.html?utm_content=set_lang (дата звернення: 12.02.2021).
10. Segal T. Big Data. Investopedia. Business Essentials. 2021. URL: <https://www.investopedia.com/terms/b/big-data.asp> (дата звернення: 12.02.2021).

11. Botelho B., Bigelow S. J. Definition of “big data”. TechTarget. SearchDataManagement. 2019. URL: https://searchdatamanagement.techtarget.com/definition/big-data?_gl=1*hhk0q5*_ga*MTg1Nzg5ODM3MS4xNTUyNDg4OTQy*_ga_RRBYR9CGB9*MTYxMzAzMjgyNS4xLjEuMTYxMzAzMjgzMi4w&_ga=2.37778592.2010792807.1613032827-1857898371.1552488942 (дата звернення: 12.02.2021).
12. Grassegger H., Krogeus M. (Das Magazin). Ich habe nur gezeigt, dass es die Bombe gibt. Tages Anzeiger International. 2018. URL: <https://www.tagesanzeiger.ch/ausland/europa/diese-firma-weiss-was-sie-denken/story/17474918> (дата звернення: 12.02.2021).
13. Davenport T. H. Big Data at Work: Dispelling the Myths, Uncovering the Opportunities. Boston. Harvard Business Review Press. 2014. 240 p.
14. York P., Bamberger M. Measuring results and impact in the age of dig data: The nexus of evaluation, analytics and digital technology. The Rockefeller Foundation. 2020. 70 p. URL: <https://www.rockefellerfoundation.org/wp-content/uploads/Measuring-results-and-impact-in-the-age-of-big-data-by-York-and-Bamberger-March-2020.pdf> (дата звернення: 20.02.2021).
15. Mayer-Schönberger V., Cukier K. Big Data: A Revolution That Will Transform How We Live, Work, and Think. Eamon Dolan/Houghton Mifflin Harcourt, 2013. 256 p.
16. Bryant A. How is Big Data being used more in the leadership and management field? The New York Times. 2013. URL: <https://www.nytimes.com/2013/06/20/business/in-head-hunting-big-data-may-not-be-such-a-big-deal.html> (дата звернення: 16.02.2022).
17. Dijcks J.-P. Oracle: Big Data for the Enterprise. An Oracle White Paper. 2011. URL: <https://www.oracle.com/technetwork/database/bi-datawarehousing/wp-big-data-with-oracle-521209.pdf> (дата звернення: 16.02.2022).
18. Про доступ до публічної інформації: Закон України від 13.01.2011 р. №2939-VI: станом на 19 лютого 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text> (дата звернення: 23.02.2022).

19. Про захист персональних даних: Закон України від 01.06.2010 р. №2297-VI: станом на 13 лютого 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 23.02.2022).
20. Studinka J., Guenduez A. A. The Use of Big Data in the Public Policy Process: Paving the Way for Evidence-Based Governance. Smart Government Lab, Institute for Public Management and Governance, University of St. Gallen, St. Gallen, Switzerland. 2018. 29 p. URL: <https://www.alexandria.unisg.ch/255680/1/Studinka%20and%20Guenduez%20-%20The%20Use%20of%20Big%20Data%20in%20the%20Public%20Policy%20Processes-%20Paving%20the%20Way%20for%20Evidence-Based%20Governance%20.pdf> (дата звернення: 20.02.2021).
21. Big Data: What is it and why it matters. Big Data Insights. SAS Insights. SAS Institute Inc. URL: https://www.sas.com/en_us/insights/big-data/what-is-big-data.html (дата звернення: 20.02.2021).
22. Hadi H. J., Shnain A. H., Hadishaheed S., Ahmad A. H. Big data and five V's characteristics. International Journal of Advancees in Electronics and Computer Science. 2015. 16-23 p. URL: http://www.ijer.in/journal/journal_file/journal_pdf/12-105-142063747116-23.pdf (дата звернення: 16.02.2022).
23. Мельник Р.С., Бевзенко В.М. Загальне адміністративне право: Навчальний посібник. Київ: Ваіте. 2014. 376 с. URL: <https://www.osce.org/files/f/documents/d/c/358156.pdf> (дата звернення: 04.03.2022).
24. Галуцько В. В. Публічний інтерес в адміністративному праві. Форум права. 2010. №4. С. 178-182. URL: [http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/3372/Publichnyi%20inte res%20v%20administratyvnomu%20_Halunko%20_2010.pdf?sequence=1](http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/3372/Publichnyi%20interes%20v%20administratyvnomu%20_Halunko%20_2010.pdf?sequence=1) (дата звернення: 04.03.2022).

25. Стеценко С. Публічний інтерес доцільно сприймати як сукупність взаємообумовлених інтересів суспільства і держави. Судова влада України. 04.12.2020 р. URL: <https://supreme.court.gov.ua/supreme/pres-centr/news/1034963> (дата звернення: 13.03.2022).
26. Колпаков В. К., Кузьменко О. В. Адміністративне право України: Підручник. Київ: Юрінком Інтер. 2003. 544 с. URL: <https://law.sspu.edu.ua/files/documents/books/library/5/kolpakov.pdf> (дата звернення: 14.03.2022).
27. Конституція України: Закон України від 28.06.1996 р. №254к/96-ВР: станом на 1 січня 2020 р. URL: <https://zakon.rada.gov.ua/laws/show/254k/96-вр#Text> (дата звернення: 15.03.2022).
28. Про Кабінет Міністрів України: Закон України від 27.02.2014 р. №794-VII: станом на 13 лютого 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/794-18#Text> (дата звернення: 14.03.2022).
29. Про центральні органи виконавчої влади: Закон України від 17.03.2011 р. №3166-VI: станом на 13 лютого 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/3166-17#Text> (дата звернення: 14.03.2022).
30. Про місцеві державні адміністрації: Закон України від 09.04.1999 р. №586-XIV: станом на 1 серпня 2021 р. URL: <https://zakon.rada.gov.ua/laws/show/586-14#Text> (дата звернення: 14.03.2022).
31. Про місцеве самоврядування в Україні: Закон України від 21.05.1997 р. №280/97-ВР: станом на 13 лютого 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/280/97-вр#Text> (дата звернення: 14.03.2022).
32. Кодекс адміністративного судочинства: Кодекс України від 06.07.2005 р. №2747-IV: станом на 15 серпня 2020 р. URL: <https://zakon.rada.gov.ua/laws/show/2747-15#Text> (дата звернення: 26.02.2021).
33. Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних: Постанова Кабінету Міністрів України від 21.10.2015 р. №835: станом на 13 жовтня 2020 р. URL: <https://zakon.rada.gov.ua/laws/show/835-2015-п#Text> (дата звернення: 01.03.2021).

34. Про Державний земельний кадастр: Закон України від 07.07.2011 р. №3613-VI: станом на 26 лютого 2021 р. URL: <https://zakon.rada.gov.ua/laws/show/3613-17#Text> (дата звернення: 25.03.2021).
35. Сайт Державної служби України з питань геодезії, картографії та кадастру. Електронні сервіси земельного кадастру. URL: <https://e.land.gov.ua/services> (дата звернення: 25.03.2021).
36. Сайт Державної служби України з питань геодезії, картографії та кадастру. Електронні послуги Держгеокадастру. URL: https://e.land.gov.ua/auth_select (дата звернення: 25.03.2021).
37. Про затвердження Положення про єдину цифрову відомчу телекомунікаційну мережу МВС: Наказ Міністерства внутрішніх справ України від 04.07.2016 р. №596: станом на 24 грудня 2019 р. URL: <https://zakon.rada.gov.ua/laws/show/z1055-16#Text> (дата звернення: 03.05.2022).
38. Про запровадження в дослідну експлуатацію підсистем «Електронний суд» та «Електронний кабінет»: Наказ Державної судової адміністрації України від 01.06.2020 р. №247. URL: https://dsa.court.gov.ua/userfiles/media/media/2020/4/N_247_20.pdf (дата звернення: 05.05.2022).
39. Електронний суд. Що таке електронний суд? ЄСІТС Технічна підтримка користувачів. URL: <https://id.court.gov.ua>, https://wiki-ccs.court.gov.ua/w/Категорія:Електронний_суд (дата звернення: 30.04.2022).
40. Деякі питання оптимізації системи центральних органів виконавчої влади: Постанова Кабінету Міністрів України від 02.09.2019 р. №829: станом на 20 лютого 2021 р. URL: <https://zakon.rada.gov.ua/laws/show/829-2019-п#Text> (дата звернення: 25.02.2021).
41. Питання Міністерства цифрової трансформації: Постанова Кабінету Міністрів України від 18.09.2019 р. №856: станом на 7 лютого 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/856-2019-п#Text> (дата звернення: 25.02.2021).
42. Сайт Дія: Державні послуги онлайн. Електронні послуги. URL: <https://diia.gov.ua/services> (дата звернення: 30.04.2022).

43. Про затвердження Порядку формування та перевірки електронного посвідчення водія, електронного свідоцтва про реєстрацію транспортного засобу, їх електронних копій: Постанова Кабінету Міністрів України від 29.12.2021 р. №1453. URL: <https://zakon.rada.gov.ua/laws/show/1453-2021-п#Text> (дата звернення: 30.04.2022).
44. Про внесення змін до Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус: Закон України від 30.03.2021 р. №1368-IX. URL: <https://zakon.rada.gov.ua/laws/show/1368-20#Text> (дата звернення: 30.04.2022).
45. Деякі питання формування та використання сертифіката, що підтверджує вакцинацію від гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2, негативний результат тестування або одужання особи від зазначеної хвороби: Постанова Кабінету Міністрів України від 29.06.2021 р. №677: станом на 9 березня 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/677-2021-п#Text> (дата звернення: 30.04.2022).
46. Сайт Дія: Державні послуги онлайн. Обробка персональних даних. Повідомлення про обробку персональних даних. URL: https://diia.gov.ua/app_policy (дата звернення: 30.04.2022).
47. Щодо надання роз'яснення термінів, які застосовуються у Законі України «Про внесення змін до деяких законодавчих актів України щодо відповідальності за корупційні правопорушення»: Лист Міністерства юстиції України від 18.12.2009 р. №967-0-2-09-22. URL: <https://zakon.rada.gov.ua/laws/show/v967-323-09#Text> (дата звернення: 02.05.2022).
48. Про адміністративні послуги: Закон України від 06.09.2012 р. №5203-VI: станом на 19 лютого 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/5203-17#Text> (дата звернення: 30.04.2022).
49. Про електронні довірчі послуги: Закон України від 05.10.2017 р. №2155-VIII: станом на 1 січня 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text> (дата звернення: 02.05.2022).

50. Питання Єдиного державного вебпорталу електронних послуг та Реєстру адміністративних послуг: Постанова Кабінету Міністрів України від 04.12.2019 р. №1137: станом на 29 березня 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/1137-2019-п#Text> (дата звернення: 30.04.2022).
51. Сайт Дія: Державні послуги онлайн. URL: <https://diia.gov.ua> (дата звернення: 30.04.2022).
52. Сайт Дія: Державні послуги онлайн. Автоматична реєстрація ФОП. URL: <https://diia.gov.ua/services/reystraciya-fop> (дата звернення: 01.05.2022).
53. Про реалізацію експериментального проекту щодо створення сприятливих умов для реалізації прав дитини: Постанова Кабінету Міністрів України від 10.07.2019 р. №691: станом на 14 березня 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/691-2019-п#Text> (дата звернення: 01.05.2022).
54. Про затвердження Порядку функціонування Електронного кабінету: Наказ Міністерства фінансів України від 14.07.2017 р. №637: станом на 21 травня 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/z0942-17#Text> (дата звернення: 02.05.2022).
55. Про реалізацію експериментального проекту щодо запровадження першої черги Єдиної державної електронної системи дозвільних документів: Постанова Кабінету Міністрів України від 11.08.2021 р. №895. URL: <https://zakon.rada.gov.ua/laws/show/895-2021-п#Text> (дата звернення: 02.05.2022).
56. Про запобігання корупції: Закон України від 14.10.2014 р. №1700-VII: станом на 13 лютого 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/1700-18#Text> (дата звернення: 03.05.2022).
57. Про затвердження Положення про Єдиний державний реєстр осіб, які вчинили корупційні або пов'язані з корупцією правопорушення: Рішення Національного агентства з питань запобігання корупції від 09.02.2018 р. №166: станом на 15 квітня 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/z0345-18#Text> (дата звернення: 03.05.2022).
58. Про затвердження Порядку адміністрування єдиного вебпорталу використання публічних коштів: Постанова Кабінету Міністрів України від 14.09.2015 р. №694.

URL: <https://zakon.rada.gov.ua/laws/show/694-2015-п#Text> (дата звернення: 03.05.2022).

59. Dixon Robyn. China's new surveillance program aims to cut crime. Some fear it'll do much more. Los Angeles Times. World&Nation. 2018. URL: <https://www.latimes.com/world/asia/la-fg-china-sharp-eyes-20181027-story.html> (дата звернення: 06.05.2022).

60. Про затвердження Комплексної міської цільової програми «Електронна столиця» на 2019-2022 роки: Рішення Київської міської ради від 18.12.2018 р. №461/6512. URL: <https://kmr.gov.ua/sites/default/files/461-6512.pdf> (дата звернення: 07.03.2021).

61. Про схвалення проекту міської цільової програми профілактики та протидії злочинності в місті Києві «Безпечна столиця» на 2022-2024 роки: Розпорядження Київської міської ради від 11.08.2021 р. №1760. URL: https://kyivcity.gov.ua/npa/pro_skhvalennya_proyektu_misko_tsilovo_programi_profilaktiki_ta_protidi_zlochinnosti_v_misti_kiyevi_bezpechna_stolitsya_na_2022-2024_roki/ (дата звернення: 03.05.2022).

62. Офіційний вебсайт Дніпровської міської ради. Безпечне місто. URL: <https://dniprorada.gov.ua/uk/page/-62> (дата звернення: 03.05.2022).

63. Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій): Рішення Ради національної безпеки і оборони України від 28.04.2017 р.: станом на 19 березня 2019 р. URL: <https://zakon.rada.gov.ua/laws/show/n0004525-17#Text> (дата звернення: 06.03.2021).

64. Про запобігання поширенню на території України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2: Постанова Кабінету Міністрів України від 11.03.2020 р. №211: станом на 24 лютого 2021 р. URL: <https://zakon.rada.gov.ua/laws/show/211-2020-п#Text> (дата звернення: 01.03.2021).

65. Про внесення змін до постанови Кабінету Міністрів України від 11 березня 2020 р. № 211: Постанова Кабінету Міністрів України від 29.03.2020 р. №241. URL: <https://zakon.rada.gov.ua/laws/show/241-2020-п#Text> (дата звернення: 01.03.2021).

66. Інструкція з використання електронного сервісу «Дій вдома» Єдиного державного веб-порталу електронних послуг для вирішення питання щодо обсервації (ізоляції) осіб, які перетинають державний кордон або в'їжджають з тимчасово окупованих територій у Донецькій та Луганській областях, Автономної республіки Крим і м. Севастополя. 2020. URL: <https://www.kmu.gov.ua/storage/app/sites/1/18%20-%20Department/18%20-%20PDF/04.2020/instrukciya-diy-vdoma.pdf> (дата звернення: 02.03.2021).
67. Сайт Міністерства та Комітет цифрової трансформації України. Мінцифра використовує Big Data для боротьби з пандемією. Новини. 2020. URL: <https://thedigital.gov.ua/news/mintsifra-vikoristovue-big-data-dlya-borotbi-z-pandemiei> (дата звернення: 02.03.2021).
68. Про схвалення Концепції розвитку електронної охорони здоров'я: Розпорядження Кабінету Міністрів України від 28.12.2020 р. №1671-р: станом на 28 грудня 2020 р. URL: <https://zakon.rada.gov.ua/laws/show/1671-2020-p#Text> (дата звернення: 02.03.2021).
69. Сайт проєкту «Є ЛІКИ». URL: <https://eliky.in.ua> (дата звернення: 18.02.2022).
70. Сайт Електронної системи охорони здоров'я в Україні. URL: <https://ehealth.gov.ua> (дата звернення: 18.02.2022).
71. Сайт Електронної системи охорони здоров'я в Україні. Підключені до ЦБД Медичні Інформаційні Системи. URL: <https://ehealth.gov.ua/pidklyucheni-do-ehealth-mis/> (дата звернення: 18.02.2022).
72. Деякі питання провадження господарської діяльності з медичної практики: Постанова Кабінету Міністрів України від 16.02.2022 р. №126. URL: <https://zakon.rada.gov.ua/laws/show/126-2022-p#Text> (дата звернення: 18.02.2022).
73. Сайт Електронної системи охорони здоров'я в Україні. Що потрібно знати про «Доступні ліки»? URL: <https://ehealth.gov.ua/2022/01/24/shho-potribno-znaty-pro-dostupni-lyky/> (дата звернення: 18.02.2022).
74. Про затвердження плану заходів щодо реалізації Концепції розвитку електронної охорони здоров'я: Розпорядження Кабінету Міністрів України від

- 29.09.2021 р. №1175-р: станом на 12 лютого 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/1175-2021-p#Text> (дата звернення: 18.02.2022).
75. Самофалов Д. Зарубіжний досвід використання відкритих даних як комунікаційного інструменту для покращення публічного управління та публічного адміністрування охороною здоров'я. Наукові перспективи №1(7). 2021. 271-286 с. URL: https://www.researchgate.net/publication/349589902_ZARUBIZNIJ_DOSVID_VIKORISTANNA_VIDKRITIH_DANIH_AK_KOMUNIKACIJNOGO_INSTRUMENTU_DLA_POKRASENNA_PUBLICNOGO_UPRAVLINNA_TA_PUBLICNOGO_ADMINISTRUVANNA_OHORONOU_ZDOROV%27A (дата звернення: 18.02.2022).
76. Сайт Міністерства освіти і науки України. Дистанційні та онлайн-сервіси в освіті. URL: <https://mon.gov.ua/ua/distancijni-ta-onlajn-servisi-v-osviti> (дата звернення: 09.03.2021).
77. Про затвердження Положення про Єдину державну електронну базу з питань освіти: Наказ Міністерства освіти і науки України від 08.06.2016 р. №620: станом на 8 червня 2018 р. URL: <https://zakon.rada.gov.ua/laws/show/z1132-18#Text> (дата звернення: 09.03.2021).
78. Сайт Єдиної державної електронної бази з питань освіти. Вступна кампанія 2022. URL: <https://vstup.edbo.gov.ua> (дата звернення: 04.05.2022).
79. Сайт Єдиної державної електронної бази з питань освіти. Реєстр документів про освіту. URL: <https://info.edbo.gov.ua/edu-documents/> (дата звернення: 05.05.2022).
80. Сайт Єдиної державної електронної бази з питань освіти. Реєстр студентських (учнівських) квитків. URL: <https://info.edbo.gov.ua/student-tickets/> (дата звернення: 04.05.2022).
81. Сайт Єдиної державної електронної бази з питань освіти. Реєстр суб'єктів освітньої діяльності. URL: https://registry.edbo.gov.ua/?fbclid=IwAR2GR_L4o9TEbK_KlSxYaMCFIDCsWNO0iIXSPQsKNU9YEmAbGBASMBUaMt8 (дата звернення: 09.03.2021).

82. Проект Концепції цифрової трансформації освіти і науки на період до 2026 року. URL: <https://mon.gov.ua/ua/news/koncepciya-cifrovoyi-transformaciyi-osviti-i-nauki-mon-zaproshuye-do-gromadskogo-obgovorenniya> (дата звернення: 21.02.2022).
83. Сайт Всеукраїнської школи онлайн. Міністерство освіти і науки України. URL: <https://lms.e-school.net.ua> (дата звернення: 09.03.2021).
84. Про введення в дослідну експлуатацію програмного модуля електронних щоденників та журналів закладів загальної середньої освіти ПАК «АІКОМ»: наказ Міністерства освіти і науки України від 22.12.2020 р. №1545. URL: <https://mon.gov.ua/ua/npa/pro-vvedennya-v-doslidnu-ekspluataciyu-programnogo-modulya-elektronnih-shodennikiv-ta-zhurnaliv-zakladiv-zagalnoyi-serednoyi-osviti-pak-aikom> (дата звернення: 21.02.2022).
85. Сайт E-journal. URL: <https://e-journal.iea.gov.ua> (дата звернення: 21.02.2022).
86. Про внесення змін до методичних рекомендацій щодо заповнення Класного журналу учнів початкових класів Нової української школи: наказ Міністерства освіти і науки України від 02.09.2020 р. №1096. URL: <https://mon.gov.ua/storage/app/uploads/public/5f5/083/b49/5f5083b492f90273019122.pdf> (дата звернення: 21.02.2022).
87. Сайт Міністерства освіти і науки України. Новини. Відбулася попередня презентація Національної електронної науково-інформаційної системи URIS. 18.02.2022 р. URL: <https://mon.gov.ua/ua/news/vidbulasya-poperednya-prezentaciya-nacionalnoyi-elektronnoyi-naukovo-informacijnoyi-sistemi-uris> (дата звернення: 21.02.2022).
88. Сайт Міністерства освіти і науки України. Цифрова трансформація освіти і науки. Національна електронна науково-інформаційна система (URIS). URL: <https://mon.gov.ua/ua/osvita/cifrova-osvita/elektronna-naukovo-informacijna-sistema> (дата звернення: 21.02.2022).
89. Проект Дія. Цифрова освіта URL: <https://thedigital.gov.ua/projects/osvita> (дата звернення: 15.03.2022).
90. Про організацію прийому та обслуговування осіб, які звертаються до органів Пенсійного фонду України: Постанова Правління Пенсійного фонду України від

- 30.07.2015 р. №13-1: станом на 10 грудня 2021 р. URL: <https://zakon.rada.gov.ua/laws/show/z0991-15#Text> (дата звернення: 31.01.2022).
91. Сайт Пенсійного Фонду України. Портал електронних послуг. URL: <https://portal.pfu.gov.ua/sidebar/Templates/Default> (дата звернення: 31.01.2022).
92. Деякі питання організації ведення Електронного реєстру листків непрацездатності та надання інформації з нього: Постанова Кабінету Міністрів України від 17.04.2019 р. №328: станом на 5 січня 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/328-2019-п#Text> (дата звернення: 31.01.2022).
93. Деякі питання формування медичних висновків про тимчасову непрацездатність та проведення їхньої перевірки: Наказ Міністерства охорони здоров'я України від 01.06.2021 року №1066: станом на 28 січня 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/z0728-21#Text> (дата звернення: 31.01.2022).
94. Про затвердження Порядку видачі (формування) листків непрацездатності в Електронному реєстрі листків непрацездатності: Наказ Міністерства охорони здоров'я від 17.06.2021 р. №1234: станом на 28 січня 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/z0890-21#Text> (дата звернення: 13.03.2022).
95. Про соціальні послуги: Закон України від 17.01.2019 р. №2671-VIII: станом на 15 грудня 2021 р. URL: <https://zakon.rada.gov.ua/laws/show/2671-19#Text> (дата звернення: 31.01.2022).
96. Про Реєстр надавачів та отримувачів соціальних: Постанова Кабінету Міністрів України від 27.01.2021 р. №99. URL: <https://zakon.rada.gov.ua/laws/show/99-2021-п#Text> (дата звернення: 31.01.2022).
97. Про затвердження Положення про Єдину інформаційну систему соціальної сфери: Постанова Кабінету Міністрів України від 14.04.2021 р. №404. URL: <https://zakon.rada.gov.ua/laws/show/404-2021-п#Text> (дата звернення: 31.01.2022).
98. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. №2163-VIII: станом на 15 грудня 2021 р. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 04.05.2022).
99. Від кібератаки 14 січня постраждали 22 державних органи. Сайт Державної служби спеціального зв'язку та захисту інформації. Новини. 24.01.2022 р. URL:

<https://cip.gov.ua/ua/news/vid-kiberataki-14-sichnya-postrazhdali-22-derzhavnikh-organi> (дата звернення: 04.05.2022).

100. Михайло Федоров: Україна змогла відбити найбільшу за всю історію країни кібератаку. Єдиний веб-портал органів виконавчої влади України. Урядовий портал. Новини. 16.02.2022 р. URL: <https://www.kmu.gov.ua/news/mihajlo-fedorov-ukrayina-zmogla-vidbiti-najbilshu-za-vsyu-istoriyu-krayini-kiberataku> (дата звернення: 04.05.2022).

101. Чергова кібератака на сайти державних органів та банки. Сайт Державної служби спеціального зв'язку та захисту інформації. Новини. 23.02.2022 р. URL: <https://cip.gov.ua/ua/news/chernova-kiberataka-na-saiti-derzhavnikh-organiv-ta-banki> (дата звернення: 04.05.2022).

102. Деякі питання застосування «Документа в період дії воєнного стану: Постанова Кабінету Міністрів України від 10.03.2022 р. №248. URL: <https://zakon.rada.gov.ua/laws/show/248-2022-п#Text> (дата звернення: 04.05.2022).

103. Питання надання у 2022 році застрахованим особам одноразової матеріальної допомоги у зв'язку із втратою частини заробітної плати (доходу), робота (економічна діяльність) яких тимчасово зупинена внаслідок проведення бойових дій під час воєнного стану в Україні: Постанова Кабінету Міністрів України від 04.03.2022 р. №199. URL: <https://zakon.rada.gov.ua/laws/show/199-2022-п#Text> (дата звернення: 04.05.2022).

104. Сайт Дія: Гід з державних послуг. «Підтримка/Допомога у 6500 гривень/Виплата внаслідок війни. URL: <https://guide.diia.gov.ua/view/nadannia-dopomohy-v-ramkakh-prohramy-iepidtrymka-u-zviazku-iz-vtratoiu-chastyny-zarobitnoi-platy-dokhodu-robota-ekonomichna-diia> (дата звернення: 04.05.2022).

105. Про затвердження Порядку надання роботодавцю компенсації витрат на оплату праці за працевлаштування внутрішньо переміщених осіб внаслідок проведення бойових дій під час воєнного стану в Україні: Постанова Кабінету Міністрів України від 20.03.2022 р. №331: станом на 8 квітня 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/331-2022-п#Text> (дата звернення: 06.05.2022).

106. Сайт Дія: Державні послуги онлайн. Компенсація за працевлаштування ВПО. URL: <https://diia.gov.ua/services/kompensaciya-za-pracevlashtuvannya-vpo> (дата звернення: 06.05.2022).
107. Про збір, обробку та облік інформації про пошкоджене та знищене нерухоме майно внаслідок бойових дій, терористичних актів, диверсій, спричинених військовою агресією Російської Федерації: Постанова Кабінету Міністрів України від 26.03.2022 р. №380: станом на 26 березня 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/380-2022-п#Text> (дата звернення: 04.05.2022).
108. Деякі питання подання заяви в електронній формі щодо отримання допомоги від міжнародних організацій: Постанова Кабінету Міністрів України від 16.04.2022 р. №455. URL: <https://zakon.rada.gov.ua/laws/show/455-2022-п#Text> (дата звернення: 04.05.2022).
109. Отримати статус та допомогу для внутрішньо переміщених осіб тепер можна в Дії. Єдиний веб-портал органів виконавчої влади України. Урядовий портал. Новини. 19.04.2022 р. URL: <https://www.kmu.gov.ua/news/otrimati-status-ta-dopomogu-dlya-vnutrishno-peremishchenih-osib-teper-mozhna-v-diyi> (дата звернення: 04.05.2022).
110. Деякі питання виплати допомоги на проживання внутрішньо переміщеним особам: Постанова Кабінету Міністрів України від 20.03.2022 р. №332: станом на 19 квітня 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/332-2022-п#Text> (дата звернення: 04.05.2022).
111. Внутрішньо переміщені особи. Новини. Мінсоцполітики запустило платформу «Допомога для адресного та ефективного розподілу гуманітарної допомоги». Сайт Міністерства соціальної політики України. 21.03.2022 р. URL: <https://www.msp.gov.ua/news/21589.html> (дата звернення: 05.05.2022).
112. Сайт «Допомога». URL: <https://social.edopomoga.gov.ua> (дата звернення: 05.05.2022).
113. Зубофф Ш. Эпоха надзорного капитализма. Битва за человеческое будущее на новых рубежах власти. Издательство Института Гайдара. 2022. 784 с.

114. Franceschi-Bicchierai Lorenzo. 465,000 Patients Need Software Updates for Their Hackable Pacemakers, FDA Says. Vice. Tech by Vice. August 30, 2017. URL: https://www.vice.com/en/article/nee5bw/465000-patients-need-software-updates-for-their-hackable-pacemakers-fda-says?mc_cid=ae72c46711&mc_eid=975e3da6fe (дата звернення: 07.05.2022).
115. Staff Toi. Likud campaign chief credits get out the vote data app for huge gains. The Times of Israel. March 3, 2020. URL: <https://www.timesofisrael.com/likud-campaign-chief-credits-get-out-the-vote-data-app-for-huge-gains/> (дата звернення: 07.05.2022).
116. Bar-Zaik Ran. App used by Netanyahu's Likud leaks Israel's entire voter registry. Haaretz. Israel News. February 9, 2020. URL: <https://www.haaretz.com/israel-news/elections/.premium-app-used-by-netanyahu-s-likud-leaks-israel-s-entire-voter-registry-1.8509696> (дата звернення: 07.05.2022).
117. Савчук Т. Соціальна інженерія: як шахраї використовують людську психологію в інтернеті. Радіо Свобода. Суспільство. 2018. URL: <https://www.radiosvoboda.org/a/socialna-inzhenerija-shaxrajstvo/29460139.html> (дата звернення: 26.03.2021 року).
118. Батчаєв В. К., Шадська У. С. Відеоспостереження у публічних місцях: основи захисту персональних даних (посібник для органів місцевого самоврядування). Київ: Компринт. 2021. 98 с. URL: https://decentralization.gov.ua/uploads/library/file/753/POSIBNYK_videosposterezheniya_u_publichnyx_miscyax.pdf (дата звернення: 08.05.2022).
119. Чи легально встановлювати на міських вулицях камери із системою розпізнавання. Центр демократії та верховенства права. 30.06.2021 р. URL: <https://cedem.org.ua/analytics/kamery-rozpiznavannya-oblych/> (дата звернення: 08.05.2022).
120. Камери відеоспостереження використовують у боротьбі з коронавірусом. Ми вивчили, як ця система працює в Києві й чому це небезпечно. Заборона. Безпека. 25.04.2020 р.. URL: <https://zaborona.com/kamery-sposterezhennya-vykorystovuyut/> (дата звернення: 08.05.2022).

121. Янукович почув кожного, а Зеленський побачить. Naspravdi Today. 29.08.2021 р. URL: <https://naspravdi.today/uk/2021/08/29/yanukovych-pochuv-kozhnoho-a-zelensky-shche-y-pobachyt/> (дата звернення: 08.05.2022).
122. Митко А. М., Кольцова І. І. Інформаційний тероризм як інструмент впливу на інформаційний конформізм в глобальному середовищі. Політичні проблеми міжнародних систем та глобального розвитку. 2018. 135-139 с. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILE=&2_S21STR=pollife_2018_2_24 (дата звернення: 26.03.2021).
123. Додаток «Дія» звинуватили у «зливів» персональних даних українців. Влада заперечує. BBC News Україна. 12.05.2020 р. URL: <https://www.bbc.com/ukrainian/news-52636988> (дата звернення: 26.03.2021).
124. Оголошення про продаж «злитих» даних українців внаслідок кібератаки є провокацією та продовженням гібридної війни. Сайт Міністерства цифрової трансформації. Прес-офіс Міністерства. Новини. 22.01.2022 р. URL: <https://thedigital.gov.ua/news/ogoloshennya-pro-prodazh-zlitikh-danikh-ukraintsiv-vnaslidok-kiberataki-e-provokatsieyu-ta-prodovzhennyam-gibridnoi-viyni> (дата звернення: 09.05.2022).
125. Конвенція про захист прав людини і основоположних свобод: Конвенція Ради Європи від 04.11.1950 р.: станом на 1 серпня 2021 р. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 26.03.2021).
126. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Конвенція Ради Європи від 28.01.1981 р.: станом на 6 липня 2010 р. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 27.03.2021).
127. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Council of Europe Treaty Series. No.223. Strasbourg. 10.X.2018. URL: <https://rm.coe.int/16808ac918> (дата звернення: 22.05.2022).

128. 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 вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних): Регламент Європейського Союзу від 27.04.2016 р. №2016/679. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 27.03.2021).

129. Запити на видалення контенту відповідно до законодавства ЄС у сфері захисту персональних даних. Звіт про доступність сервісів і даних. Google. URL: <https://transparencyreport.google.com/eu-privacy/overview?hl=uk-UA> (дата звернення: 07.02.2022).

130. McKean R., Kurowska-Tober E., Waem H. DLA Piper GDPR fines and data breach survey: January 2021. DLA PIPER Publications. 2021. URL: <https://www.dlapiper.com/en/uk/insights/publications/2021/01/dla-piper-gdpr-fines-and-data-breach-survey-2021/> (дата звернення: 27.03.2021).

131. California Consumer Privacy Act of 2018 [1798.100 - 1798.199.100]. California Civil Code CIV. URL: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 (дата звернення: 22.05.2022).

132. Конвенція про кіберзлочинність: Конвенція Ради Європи від 23.11.2001 р. : станом на 7 вересня 2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 23.05.2022).

133. Бем М. В., Городинський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. Київ: К.І.С. 2015. 220 с. URL: <https://rm.coe.int/168059920c> (дата звернення: 28.03.2021).

134. Про затвердження документів у сфері захисту персональних даних: Наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 р. №1/02-14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#n92 (дата звернення: 29.03.2021).

135. Кодекс про адміністративні правопорушення (статті 1-212-24): Кодекс України від 07.12.1984 р. №8073¹-Х: станом на 17 березня 2021 р. URL: <https://zakon.rada.gov.ua/laws/show/80731-10#Text> (дата звернення: 29.03.2021).
136. Проект Закону про захист персональних даних від 07.06.2021 р. №5628: станом на 2 червня 2021 р. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72160 (дата звернення: 23.05.2022).
137. Проект Закону про Національну комісію з питань захисту персональних даних та доступу до публічної інформації від 18.10.2021 р. №6177: станом на 11 листопада 2021 р. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72992 (дата звернення: 23.05.2022).
138. Деякі питання діяльності Міністерства культури та інформаційної політики: Постанова Кабінету Міністрів України від 16.10.2019 р. №885: станом на 13 березня 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/885-2019-п#Text> (дата звернення: 09.05.2022).
139. Сайт Центру стратегічних комунікацій. Про Центр. URL: <https://spravdi.gov.ua/pro-nas/> (дата звернення: 09.05.2022).
140. Сайт Міністерства культури та інформаційної політики України. Інформаційна політика та безпека. Центр стратегічних комунікацій. URL: <https://mkip.gov.ua/content/centr-strategichnih-komunikaciy-ta-informaciynoi-bezpeki-pri-ministerstvi-kulturi-ta-informaciynoi-politiki.html> (дата звернення: 09.05.2022).
141. Сайт Міністерства культури та інформаційної політики України. Інформаційна політика та безпека. ООС. Інформаційна війна. URL: <https://mkip.gov.ua/content/informaciyna-viyna.html> (дата звернення: 10.05.2022).
142. Сайт Міністерства культури та інформаційної політики України. Інформаційна політика та безпека. ООС. Інформаційна війна. Докази для Гааги. URL: <https://mkip.gov.ua/content/dokazi-dlya-gaagi.html> (дата звернення: 10.05.2022).
143. Сайт Міністерства культури та інформаційної політики України. Інформаційна політика та безпека. ООС. Інформаційна війна. Інформаційні видання. URL: <https://mkip.gov.ua/content/informaciyni-vidannya.html> (дата звернення: 10.05.2022).

144. Про створення Центру протидії дезінформації: Рішення Ради національної безпеки і оборони України від 11.03.2021 р.: станом на 23 березня 2021 р. URL: <https://zakon.rada.gov.ua/laws/show/n0015525-21#n2> (дата звернення: 10.05.2022).
145. Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації»: Указ Президента України від 19.03.2021 р. №106/2021. URL: <https://zakon.rada.gov.ua/laws/show/106/2021#Text> (дата звернення: 10.05.2022).
146. Питання Центру протидії дезінформації: Указ Президента України від 07.05.2021 р. №187/2021. URL: <https://zakon.rada.gov.ua/laws/show/187/2021#Text> (дата звернення: 10.05.2022).
147. Сайт Центру протидії дезінформації при РНБО України. Проекти. Глосарій. URL: <https://cpd.gov.ua/category/glossary/> (дата звернення: 10.05.2022).
148. Про Національний координаційний центр кібербезпеки: Указ Президента України від 07.06.2016 р. №242/2016: станом на 17 липня 2021 р. URL: <https://zakon.rada.gov.ua/laws/show/242/2016#n9> (дата звернення: 12.05.2022).
149. Про утворення територіального органу Національної поліції: Постанова Кабінету Міністрів України від 13.10.2015 р. №831. URL: <https://zakon.rada.gov.ua/laws/show/831-2015-п#Text> (дата звернення: 10.05.2022).
150. Сайт Департаменту кіберполіції Національної поліції України. URL: <https://cyberpolice.gov.ua> (дата звернення: 10.05.2022).
151. Про Службу безпеки України: Закон України від 25.03.1992 р. №2229-XII: станом на 7 травня 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/2229-12#Text> (дата звернення: 11.05.2022).
152. Сайт Служби безпеки України. Про СБУ. Структура. Ситуаційний центр забезпечення кібербезпеки. URL: <https://ssu.gov.ua/sytuatsiinyi-tsentr-zabezpechennia-kiberbezpeky> (дата звернення: 11.05.2022).
153. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України: Рішення Конституційного Суду України від 20.01.2012 р.

№2-пп/2012. URL: <https://zakon.rada.gov.ua/laws/show/v002p710-12#Text> (дата звернення: 03.02.2022).

154. Рішення Конституційного Суду України у справі за конституційним поданням Уповноваженого Верховної Ради України з прав людини щодо відповідності Конституції України (конституційності) окремих положень абзацу першого пункту 40 розділу VI „Прикінцеві та перехідні положення“ Бюджетного кодексу України: Рішення Конституційного Суду України від 11.10.2018 р. №7-п/2018. URL: <https://zakon.rada.gov.ua/laws/show/v007p710-18#Text> (дата звернення: 03.02.2022).

155. Рішення Конституційного Суду України у справі за конституційною скаргою Плєскача В'ячеслава Юрійовича щодо відповідності Конституції України (конституційності) положень другого речення частини четвертої статті 42 Закону України „Про Конституційний Суд України“: Рішення Конституційного Суду України від 22.01.2020 р. №1-п(І)/2020. URL: <https://zakon.rada.gov.ua/laws/show/va01p710-20#top> (дата звернення: 03.02.2022).

156. Постанова Верховного Суду України від 27 вересня 2017 р. Справа №6-1435цс17. URL: <https://oda.court.gov.ua/sud1590/pravovipoziciivsu/6-1435cs17> (дата звернення: 03.02.2022).

157. Постанова Верховного Суду від 16 квітня 2020 р. Справа №804/4069/17. URL: <https://revestr.court.gov.ua/Review/88815240> (дата звернення: 03.02.2022).

158. Постанова Верховного Суду від 19 вересня 2018 р. Справа №806/3265/17. URL: <https://revestr.court.gov.ua/Review/76822787> (дата звернення: 03.02.2022).

159. Постанова Броварського міськрайонного суду м. Києва від 9 квітня 2020 р. Справа №361/1579/20. URL: <https://revestr.court.gov.ua/Review/88698313> (дата звернення: 04.02.2022).

160. Постанова Коломийського міськрайонного суду Івано-Франківської області від 14 лютого 2017 р. Справа №346/200/17. URL: <https://revestr.court.gov.ua/Review/64723526> (дата звернення: 04.02.2022).

161. Постанова Малиновського районного суду м. Одеси від 8 жовтня 2021 р. Справа №521/14646/21. URL: <https://revestr.court.gov.ua/Review/101093100> (дата звернення: 04.02.2022).

162. Постанова Карлівського районного суду Полтавської області від 19 липня 2021 р. Справа №531/1185/21. URL: <https://reyestr.court.gov.ua/Review/98443033> (дата звернення: 04.02.2022).
163. Постанова Нетішинського міського суду Хмельницької області від 9 грудня 2019 р. Справа №679/1676/19. URL: <https://reyestr.court.gov.ua/Review/86237026> (дата звернення: 04.02.2022).
164. Постанова Соснівського районного суду м. Черкаси від 4 липня 2019 р. Справа №712/7293/19. URL: <https://reyestr.court.gov.ua/Review/82822611> (дата звернення: 04.02.2022).
165. Постанова Черкаського апеляційного суду від 29 листопада 2019 р. Справа №712/7293/19. URL: <https://reyestr.court.gov.ua/Review/86032571> (дата звернення: 04.02.2022).
166. Постанова Чортківського районного суду Тернопільської області від 16 вересня 2021 р. Справа №608/1904/21. URL: <https://reyestr.court.gov.ua/Review/99671794> (дата звернення: 04.02.2022).
167. Постанова Монастириського районного суду Тернопільської області від 6 вересня 2021 р. Справа 603/455/21. URL: <https://reyestr.court.gov.ua/Review/99430574> (дата звернення: 04.02.2022).
168. Постанова Вишгородського районного суду Київської області від 21 січня 2021 р. Справа №363/4644/20. URL: <https://reyestr.court.gov.ua/Review/94316421> (дата звернення: 04.02.2022).
169. Постанова Коломийського міськрайонного суду від 13 березня 2020 р. Справа №346/5963/19. URL: <https://reyestr.court.gov.ua/Review/88214446> (дата звернення: 04.02.2022).
170. Постанова Івано-Франківського апеляційного суду від 14 травня 2020 р. Справа №346/5963/19. URL: <https://reyestr.court.gov.ua/Review/89237104> (дата звернення: 04.02.2022).
171. Постанова Святошинського районного суду м. Києва від 6 лютого 2019 р. Справа №759/1399/19. URL: <https://reyestr.court.gov.ua/Review/79679768> (дата звернення: 04.02.2022).

172. Рішення Шевченківського районного суду м. Києва від 15 вересня 2020 р. Справа №761/23532/20. URL: <https://reyestr.court.gov.ua/Review/91799128> (дата звернення: 04.02.2022).
173. Постанова Київського апеляційного суду від 18 грудня 2020 р. Справа №761/23532/20. URL: <https://reyestr.court.gov.ua/Review/94663887> (дата звернення: 04.02.2022).
174. Постанова Соснівського районного суду м. Черкаси від 17 грудня 2021 р. Справа №712/12787/21. URL: <https://reyestr.court.gov.ua/Review/102213028> (дата звернення: 04.02.2022).
175. Постанова Шевченківського районного суду м. Києва від 11 вересня 2020 р. Справа №761/23539/20. URL: <https://reyestr.court.gov.ua/Review/91538114> (дата звернення: 04.02.2022).
176. Постанова Київського апеляційного суду від 18 грудня 2020 р. Справа №761/23539/20. URL: <https://reyestr.court.gov.ua/Review/94663886> (дата звернення: 04.02.2022).
177. Постанова Стрийського міськрайонного суду Львівської області від 31 серпня 2021 р. Справа №456/3511/21. URL: <https://reyestr.court.gov.ua/Review/99306854> (дата звернення: 04.02.2022).
178. Постанова Ленінського районного суду м. Запоріжжя від 23 вересня 2020 р. Справа №334/4896/20. URL: <https://reyestr.court.gov.ua/Review/91766936> (дата звернення: 04.02.2022).
179. Ухвала Вищого адміністративного суду України від 7 грудня 2016 р. Справа №К/800/33406/16. URL: <https://reyestr.court.gov.ua/Review/63406480> (дата звернення: 04.02.2022).
180. Ухвала Вищого адміністративного суду України від 13 липня 2017 р. Справа №К/800/50605/13. URL: <https://reyestr.court.gov.ua/Review/67828734> (дата звернення: 04.02.2022).
181. Постанова Луцького міськрайонного суду Волинської області від 2 грудня 2021 р. Справа №161/20346/21. URL: <https://reyestr.court.gov.ua/Review/101776717> (дата звернення: 04.02.2022).

182. Постанова Шевченківського районного суду м. Чернівці від 27 жовтня 2021 р. Справа №727/9879/21. URL: <https://reyestr.court.gov.ua/Review/100709158> (дата звернення: 04.02.2022).
183. Постанова Коломийського міськрайонного суду Івано-Франківської області від 23 грудня 2020 р. Справа №346/5287/20. URL: <https://reyestr.court.gov.ua/Review/93856648> (дата звернення: 04.02.2022).
184. Постанова Стрийського міськрайонного суду Львівської області від 18 серпня 2021 р. Справа №456/3297/21. URL: <https://reyestr.court.gov.ua/Review/99098891> (дата звернення: 04.02.2022).
185. Постанова Оболонського районного суду м. Києва від 8 листопада 2019 р. Справа №756/12839/19. URL: <https://reyestr.court.gov.ua/Review/85567874> (дата звернення: 04.02.2022).
186. Шевченко Т.С., Розкладай І.Є. Рішення Європейського суду з прав людини щодо доступу до інформації. Київ. 2014. 200 с. URL: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168044e84d> (дата звернення: 07.02.2022).
187. Case of M.S. v. Sweden. (1997), no 20837/92. URL: [https://hudoc.echr.coe.int/eng#{%22fulltext%22:\[%22%22CASE%20OF%20M.S.%20v.%20SWEDEN%22%22\],%22documentcollectionid%22:\[%22GRANDCHAMBER%22,%22CHAMBER%22\],%22itemid%22:\[%22001-58177%22\]}](https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22%22CASE%20OF%20M.S.%20v.%20SWEDEN%22%22],%22documentcollectionid%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-58177%22]}) (дата звернення: 07.02.2022).
188. Справа Z проти Фінляндії: Справа Європейського суду з прав людини від 25.01.1997 р. Заява №22009/93. URL: http://medicallaw.org.ua/fileadmin/user_upload/pdf/Z_against_Finland.pdf (дата звернення: 07.02.2022).
189. Справа С. і Марпер проти Сполученого Королівства: Справа Європейського суду з прав людини від 04.12.2008 р. Заяви № 30562/04 та 30566/04. URL: <http://privacy.khpg.org/1604922641> (дата звернення: 07.02.2022).
190. Case of Köpke v. Germany. (2010), no 420/07. URL: <https://www.bailii.org/eu/cases/ECHR/2010/1725.html> (дата звернення: 07.02.2022).

191. Case of Allan v. The United Kingdom. (2002), no 48539/99. URL: [https://hudoc.echr.coe.int/eng#{%22fulltext%22:\[%22%22CASE%20OF%20ALLAN%20v.%20THE%20UNITED%20KINGDOM%22%22\],%22documentcollectionid%22:\[%22GRANDCHAMBER%22,%22CHAMBER%22\],%22itemid%22:\[%22001-60713%22\]}](https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22%22CASE%20OF%20ALLAN%20v.%20THE%20UNITED%20KINGDOM%22%22],%22documentcollectionid%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-60713%22]}) (дата звернення: 07.02.2022).
192. Справа Класс та інші проти Німеччини: Справа Європейського суду з прав людини від 06.09.1978 р. Заява №5029/71. URL: https://zakon.rada.gov.ua/laws/show/980_093#Text (дата звернення: 07.02.2022).
193. Case of Uzun v. Germany. (2010), no 35623/05. URL: https://www.legislationline.org/download/id/7570/file/ECHR_case_Uzun_v_Germany_2010_en.pdf (дата звернення: 07.02.2022).
194. Case of K.U. v. Finland. (2008), no 2872/02. URL: <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-89964%22%5D%7D> (дата звернення: 07.02.2022).
195. Case of Segerstedt-Wiberg and Others v. Sweden. (2006), no 62332/00. URL: [https://hudoc.echr.coe.int/eng#{%22fulltext%22:\[%22Segerstedt-Wiberg%20and%20Others%20v.%20Sweden%22\],%22itemid%22:\[%22001-75591%22\]}](https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22Segerstedt-Wiberg%20and%20Others%20v.%20Sweden%22],%22itemid%22:[%22001-75591%22]}) (дата звернення: 07.02.2022).
196. Judgment of the Court in Case C-131/12 (Google Spain SL, Google Inc. v AEPD, Mario Costeja González). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN> (дата звернення: 07.02.2022).
197. Sussex v Associated Newspapers Ltd [2020] EWHC 1058 (Ch). URL: <https://www.judiciary.uk/wp-content/uploads/2020/05/sussex-v-associated-judgment-010520-1.pdf> (дата звернення: 07.02.2022).