Міністерство освіти і науки України

Національний університет «Києво-Могилянська академія»

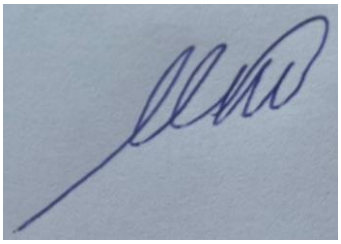
Факультет правничих наук

Кафедра міжнародного та європейського права

Магістерська робота
освітній ступінь – магістр

на тему: «**ДІЯЛЬНІСТЬ ПУБЛІЧНИХ ОРГАНІВ У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ЄВРОПЕЙСЬКОМУ СОЮЗІ, США ТА УКРАЇНІ: ОСНОВНІ ЗАСАДИ ЗАКОРДОННОЇ РЕГУЛЯТОРНОЇ ПОЛІТИКИ ТА ШЛЯХИ ВДОСКОНАЛЕННЯ ДЛЯ УКРАЇНИ**»

The activity of public authorities in the sphere of personal data protection in the European Union, the United States and Ukraine: basic principles of foreign regulatory policy and the ways for improvement in Ukraine.



Виконала: студентка 2-го року
магістерської програми,
Спеціальності 081 Право
Павлишин Марта Тарасівна
Керівник: Берлач Н.А.,
Доктор юридичних наук,
Рецензент _____
Магістерська робота захищена
З оцінкою «_____»
Секретар ЕК _____
«____» _____ 2021 року

Київ – 2021

Декларація

академічної доброчесності

студента/ студентки НаУКМА

Я Павлишин Марта Тарасівна,
студент(ка) 2 року навчання факультету древніших наук,
спеціальність 081 Право,
адреса електронної пошти martapavlysh@gmail.com

- підтверджую, що написана мною кваліфікаційна/магістерська робота на тему «Діяльність публічних органів у сфері захисту персональних даних у Європейському Союзі, США та Україні: основні засади зовнішньої регуляторної політики та шляхи вдосконалення для України» відповідає вимогам академічної доброчесності та не містить порушень, передбачених пунктами 3.1.1-3.1.6 Положення про академічну доброчесність здобувачів НаУКМА від 07.03.2018 року, зі змістом якого ознайомлений/ ознайомлена;
- підтверджую, що надана мною електронна версія роботи є остаточною і готовою до перевірки;
- згоден/ згодна на перевірку моєї роботи на відповідність критеріям академічної доброчесності, у будь-який спосіб, у тому числі порівняння змісту роботи та формування звіту подібності за допомогою електронної системи Unicheck.
- даю згоду на архівування моєї роботи в репозитаріях та базах даних університету для порівняння цієї та майбутніх робіт.

12.05.2021 _____ Павлишин М.Т.

Дата *Підпис* *Прізвище, ініціали*

Зміст

ВСТУП

У Європейському Союзі штрафи за порушення захисту персональних даних є чи не одними із найбільших і можуть становити кілька десятків мільйонів євро, а наглядові органи розглядають більше тисячі скарг у рік від осіб, які постраждали від порушення захисту їхніх персональних даних.

Право на захист персональних даних є одним із невід'ємних прав людини і одним з тих, що зараз найбільше обговорюється у цифровій сфері, адже таргетована реклама, рекомендації у стрічках новин, онлайн-покупки – все це нам доступно завдяки обробці великих масивів даних, які включають і наші персональні дані. Відтак, щоб забезпечити дотримання права на захист персональних даних у державах діють публічні органи (як державні, так і органи місцевого значення), які покликані виконувати це завдання. Від діяльності публічних органів, їхньої організації та повноважень безпосередньо залежить виконання та дотримання законодавства у сфері захисту персональних даних.

Актуальність дослідження. Питання діяльності публічних органів у сфері захисту персональних даних є особливо актуальним зараз в Україні та світі. Прийняття у Європейському Союзі GDPR запустило своєрідну ланцюгову реакцію, і значна кількість держав почали здійснювати перегляд власного законодавства у сфері захисту персональних даних, в тому числі в частині діяльності публічних органів. Зокрема, через два роки після прийняття GDPR відбулось прийняття схожого регулятора у Каліфорнії, що в свою чергу запустило ланцюгову реакцію у інших штатах, а на федеральному рівні в США нарешті почали розглядати проєкти законів у сфері захисту персональних даних та створення окремого спеціального публічного органу для забезпечення виконання та дотримання законодавства у цій сфері.

Хвиля перегляду та реформування законодавства не оминула в тому числі Україну. Одна із ключових проблем українського законодавства у сфері персональних даних полягає в тому, що у нас немає належного публічного органу, який би здійснював забезпечення виконання та дотримання

законодавства у цій сфері. До 2014 року в Україні діяла Державна служба України з питань захисту персональних даних в системі органів центральної влади, що не відповідало вимогам незалежності. Тепер функції такого публічного органу здійснює Уповноважений Верховної Ради України з прав людини, однак, він не є спеціальним органом, а здійснює загальні функції, і теж не до кінця відповідає вимозі незалежності.

Україна прямує у Європейський Союз і, підписавши Угоду про асоціацію, взяла на себе зобов'язання модернізувати власне законодавство для відповідності європейським стандартам, в тому числі у сфері захисту персональних даних. Зараз в Україні відбуваються активні обговорення проєкту нового закону, який в тому числі має врегульовувати питання діяльності публічного органу. Відтак, для України актуальний аналіз діяльності публічних органів у сфері захисту персональних даних у світі для побудови власної системи шляхом інкорпорації найкращих світових практик та для уникнення типових поширених помилок.

Мета і завдання цієї роботи. Метою цієї роботи є проведення аналізу існуючих систем публічних органів у сфері захисту персональних даних, а саме у Європейському Союзі, США та Україні для вивчення їхньої діяльності, ефективності, переваг і недоліків у роботі, щоб використати наявний аналіз для реформування системи в Україні.

Для досягнення цієї мети необхідно вирішити наступні завдання:

1. Проаналізувати, що саме розуміють під персональними даними, витоки концепції захисту персональних даних та різницю між персональними даними та приватністю для визначення меж компетенції та щодо якого обсягу відомостей здійснюють свої повноваження публічні органи у цій сфері;
2. Проаналізувати як організована діяльність публічних органів у сфері захисту персональних даних у Європейському Союзі, які відбулись зміни за останній період і визначити основні переваги та проблеми;

3. Проаналізувати як організована діяльність публічних органів у сфері захисту персональних даних у США, яка різниця між діяльністю цих органів на федеральному рівні та на рівні штатів, визначити основні переваги та недоліки;
4. Проаналізувати діяльність публічних органів у сфері захисту персональних даних в Україні, які зміни відбувались у зазначеному напрямку з часів прийняття профільного закону у сфері захисту персональних даних, визначити на основі аналізу основні недоліки у діяльності публічних органів в Україні.
5. На основі проведеного аналізу закордонного досвіду та правового регулювання в Україні запропонувати власні шляхи вдосконалення діяльності публічних органів в Україні.

Об'єктом дослідження є діяльність публічних органів у сфері захисту персональних даних у різних правових системах.

Предметом дослідження є правове регулювання діяльності публічних органів у сфері захисту персональних даних у Європейському Союзі, США, Україні та ефективність виконання ними покладених на них функцій.

Практичне значення цієї роботи полягає в тому, що результати цього дослідження можуть бути використані у науковій сфері для подальшого аналізу діяльності публічних органів; в практичній сфері для розробки проєктів законів у сфері захисту персональних даних та регулювання діяльності публічних органів.

Основні джерела у дослідженні – це нормативно-правова база Європейського Союзу, США та України, інформація, що надається відповідними публічними органами, зокрема аналітика, роз'яснення та інструкції, а також звіти їхньої діяльності, судові справи, в тому числі Європейського суду з прав людини, а також праці таких науковців як Бем М., Городиський І., Гнатюк С., Гастінґс П., Бальтазар А., Стівенс Ґ.

Методи дослідження. У цій роботі були застосовані такі методи дослідження як історико-правовий, метод аналізу і синтезу, метод порівняльного

аналізу, статистичний.

Історико-правовий метод використовується із зв'язку із тим, що для аналізу поняття «персональні дані» необхідно проаналізувати історичний розвиток цього поняття, звідки він бере початок та як змінювався. Для огляду діяльності публічних органів необхідно встановити, як змінювались їхні повноваження та ефективність їхньої діяльності у різний період часу. Метод *аналізу і синтезу* у цьому дослідженні передбачає аналіз окремих повноважень публічних органів і подальший їх синтез для встановлення ключових компетенцій. Метод *порівняльного аналізу* застосовується для порівняння поняття «персональні дані» та діяльності публічних органів у різних правових системах для встановлення основних відмінностей та спільних рис у понятті та переваг і недоліків у діяльності публічних органів. *Статистичний* метод застосовується для опрацювання даних щодо кількості розгляду скарг, відкритих проваджень, які були здійснені публічними органами.

Структура роботи. Ця робота складається з, вступу, чотирьох розділів, дев'яти підрозділів, висновків, списку використаних джерел, а також переліку умовних позначень та скорочень. Загальний обсяг магістерської роботи становить 100 сторінок.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

201 CMR 17.00	201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth
CAN-SPAM Act	Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM) Act of 2003
CCPA	California Consumer Privacy Act
COPPA	Childern's Online Privacy Protection Act
CPPA	California Privacy Protection Agency
CPRA	California Privacy Rights Act
DPA	Data Protection Authority
GBL	General Business Law § 899-aa
HIPPA	Health Insurance Portability and Accountability Act
Департамент	Департамент у сфері захисту персональних даних
Директива	Директива 95/46/ЄС Європейського парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року
ДСЗПД	Державна служба України з питань захисту персональних даних
Закон	Закон України «Про захист персональних даних»
Закон про внесення змін	Закон України «Про внесення мін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних»
Інспектор	Європейський інспектор із захисту персональних даних
Конвенція	Конвенція про захист основоположних прав та свобод
Конвенція 108	Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних
Меморандум	Меморандум про взаєморозуміння між Європейською

	радою із захисту персональних даних та Європейським інспектором із захисту персональних даних
Пакт	Міжнародний пакт про громадянські та політичні права
Порядок про здійснення контролю	Порядок здійснення Уповноваженим контролю за додержанням законодавства про захист персональних даних
Положення	Положення про Державну службу України з питань захисту персональних даних
Рада	Європейська рада із захисту даних
Регламент	Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв’язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)
Робоча група	Робоча група захисту фізичних осіб у зв’язку із обробкою персональних даних
Уповноважений	Уповноважений Верховної Ради України з прав людини

РОЗДІЛ 1. ЗАГАЛЬНИЙ ОГЛЯД КОНЦЕПЦІЇ ПЕРСОНАЛЬНИХ ДАНИХ ТА ПОНЯТТЯ ПЕРСОНАЛЬНИХ ДАНИХ

В цілях дослідження діяльності публічних органів у сфері захисту персональних даних в правових системах Європейського Союзу, США та України варто спершу проаналізувати, що саме розуміють під персональними даними. Від обсягу захисту, який надається інформації, залежить щодо якої інформації здійснює публічний орган нагляд за дотриманням законодавства. Для цього необхідно проаналізувати витоки концепції персональних даних та її розвиток, а також, які саме відомості охоплюються поняттям «персональні дані» у правових системах Європейського Союзу, США та України. Відтак, у Розділі 1 ми проаналізуємо (**1.1**) витоки та розвиток концепції персональних даних та (**1.2**) які саме відомості чи їх сукупність становлять собою поняття «персональні дані».

1.1 Витоки та розвиток концепції персональних даних

При здійсненні пошуку інформації про концепцію захисту персональних даних, її витоки та розвиток, більшість джерел вказують на витоки цієї концепції із права на приватність. Під правом на приватність часто розуміють саме право на повагу до приватного та сімейного життя, недоторканність житла та кореспонденції, яке в тій чи іншій формі уособлене у статтях міжнародних актів в сфері прав людини [1].[1] В межах цієї роботи ми використовуватимемо формулювання «право на приватність».

Захист персональних даних безпосередньо пов’язаний із правом на приватність, оскільки концепція персональних даних розвинулась саме із цього права, про що буде йти мова нижче.

«*Право бути залишеним у спокої*», – саме так сформулював право на

[1] Тут і надалі переклад іноземної літератури та нормативних джерел здійснений мною, Павлишин М. Т.

приватність суддя Верховного Суду США Луі Брендайс у своїй окремій думці у справі Олмстед проти США (англ. *Olmstead v. United States*) у 1928 році [2, с. 478]. Пізніше «право бути залишеним у спокої», сформоване Брендайсом у роботі 1890 року у співавторстві із Самюелем Ворреном [3], цитуватимуть у відомій справі Кац проти США (англ. *Katz v. United States*) 1967 року [4, с. 350], а з суддею Брендайсом пов'язуватимуть виникнення концепції права на приватність як такої [5, с. 1]. Згодом право на приватність було закріплене у Конвенції про захист основоположних прав та свобод (далі «Конвенція») у статті 8 як право на повагу до особистого та сімейного життя. Згідно зі статтею 8 Конвенції: «*кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції*» [6].

Негативний обов'язок держави щодо заборони свавільного або незаконного втручання у особисте та сімейне життя, а також свавільних чи незаконних посягань на недоторканність житла або таємницю кореспонденції особи був закріплений у статті 17 Міжнародного пакту про громадянські та політичні права від 1966 року (далі «Пакт») [7].

Варто зазначити, що у XX столітті науково-технічний прогрес був доволі стрімким, особливо в сфері інформатизації, який пришвидшив і автоматизував обробку великих масивів даних, в тому числі тих, що містять інформацію про фізичних осіб. Відтак, виникла потреба на міжнародному рівні врегулювати питання, які тісно пов'язані із розвитком інформаційних технологій та автоматизацією процесів.

Через 31 рік після прийняття Конвенції та 15 років після прийняття Пакту, у 1981 році держави-члени Ради Європи прийняли Конвенцію про захист осіб у зв'язку з автоматизованою обробкою персональних даних (далі «Конвенція 108»). Саме у преамбулі до Конвенції 108 персональні дані та право на приватність були вжиті поруч в одному контексті: «*беручи до уваги те, що бажано поширювати гарантії прав й основоположних свобод кожної людини, зокрема права на повагу до недоторканості приватного життя, з огляду на зростання транскордонного потоку персональних даних, які піддаються*

автоматизованій обробці» [8]. Із зазначеного у преамбулі уривку чітко випливає, що персональні дані, а саме їх захист, є частиною забезпечення права на приватність.

Зазначена Конвенція 108 вважається першим документом, який чітко встановлює міжнародні стандарти в сфері захисту персональних даних. Однак, на сьогоднішній день, деякі положення Конвенції 108 не відповідають актуальним проблемам та є застарілими. До тексту Конвенції 108 Комітетом міністрів Ради Європи були прийняті рекомендації, які тлумачать та деталізують належне застосування Конвенції 108 державами-членами Ради Європи щодо певної категорії даних чи певних дій із ними, які оновлюються регулярно та підтримують Конвенцію в актуальному стані [9, с. 16-17]. Однак, це не вирішує проблеми неактуальності Конвенції 108, тому в перспективі документ потребує оновлення.

Найкраще простежити розвиток концепції персональних даних із права на приватність можна саме у практиці Європейського суду з прав людини, ЄСПЛ. У інформаційній довідці ЄСПЛ щодо справ в сфері захисту персональних даних серед перших справ, які стосувались захисту персональних даних в контексті статті 8 Конвенції, наводяться в прикладі ті, які стосувались захисту кореспонденції осіб і їхніх телефонних комунікацій – Клас та інші проти Німеччини (англ. *Klass and Others v. Germany*) (1978 рік) та Мелоун проти Сполученого Королівства (англ. *Malone v. United Kingdom*) (1984 рік) [10, с. 2-3; 11, с. 31, 34]. Справи стосувались законності втручання держави (її органів, в тому числі поліції) у кореспонденцію та комунікацію осіб.

У справі Мелоун проти Сполученого Королівства, суддя Петтіті в окремій думці вперше вжив поняття «персональних даних» у фразі «файли (картотеки), що містять персональні дані» (англ. *personal data-files*) саме в контексті позначення даних приватного характеру, тобто тих, які стосуються приватного життя особи. В цій же ж окремій думці суддя Петтіті також послався на Рекомендацію R (83) 10 Комітету міністрів Ради Європи, в частині, що повага до приватного життя особи має бути гарантованою в будь-якому проєкті, що

передбачає використання персональних даних [12].

Відтак, окрема думка судді Петтіті – це перший документ в практиці ЄСПЛ, у якому поняття «персональні дані», хоч і не цілком автономно і не в притаманному йому на сьогоднішній день, але дотичному значенні вживається в контексті справи, яка стосувалась порушення статті 8 Конвенції, тобто порушення права на приватність.

Важливою в становленні практики захисту персональних даних є справа Леандер проти Швеції (англ. *Leander v. Sweden*) 1987 року. У ній заявник скаржився на зберігання поліцією безпеки (англ. *security police*) у таємному реєстрі інформації про заявника, після перевірки якої йому відмовили у працевлаштуванні у Воєнно-морський музей, при цьому не дозволивши ознайомитись із цією інформацією та надати свої коментарі щодо неї (параграф 9-17) [13]. Важливість цієї справи для становлення практики розгляду порушень, що стосуються персональних даних, полягає у наступному:

1. це перша справа, де заявлене порушення статті 8 Конвенції стосується саме зберігання даних про особу державою (її органами), а не втручання держави у кореспонденцію цих осіб (на відміну від справ Клас та інші проти Німеччини та Малоун проти Сполученого Королівства).
2. хоч втручання держави в право на повагу до приватного життя відповідно до статті 8 Конвенції було виправданим, суд визнав, що зберігання (англ. *storing*) та розкриття іншим особам (англ. *release*) даних про приватне життя особи разом із відмовою у можливості особи заперечити таку інформацію чи надати щодо неї коментарі становить собою порушення статті 8 Конвенції (параграф 48) [13].

Ще однією важливою справою є справа Ґаскін проти Сполученого Королівства (англ. *Gaskin v. United Kingdom*) 1989 року. У ній ЄСПЛ зазначив, що записи у файлі, які містили дані про дитинство заявника, без сумніву мають відношення до особистого життя заявника, а відтак попадають під регулювання статті 8 Конвенції (параграф 36-37) [14]. ЄСПЛ не надав своєї думки щодо того чи загальні права на доступ до персональних даних та інформації можуть

походити з пункту 1 статті 8 Конвенції (параграф 37) [14], але визнав, що в цій конкретній справі заявник мав свій інтерес у доступі до записів і така можливість доступу мала бути забезпечена (параграф 49) [14].

Вперше поняття «персональні дані» автономно та в звичному для нас значенні як частина права на приватність вживаються у справі Z проти Фінляндії (англ. *Z. v. France*) 1997 року. У цій справі ЄСПЛ зазначив наступне: «*У зв'язку з цим, Суд візьме до уваги, що захист персональних, і не в останню чергу медичних даних, є фундаментально важливим для користування особи своїм правом на повагу до приватного та сімейного життя, як це гарантовано відповідно до статті 8 Конвенції»* (параграф 95) [15]. Як бачимо, суд безпосередньо визнав і чітко зазначив, що захист персональних даних стосується саме права на приватність особи, а відтак персональні дані особи повинні захищатись в рамках статті 8 Конвенції, яка гарантує кожному право на повагу до приватного та сімейного життя.

Відтак, беручи до уваги вищенаведене, можемо з впевненістю сказати, що концепція захисту персональних даних розвинулась і продовжує бути частиною саме права на приватність особи. Основний розвиток ця концепція набула у 1980х роках минулого століття із прийняттям Конвенції 108 та розвитком судової практики, не в останню чергу практики ЄСПЛ.

Однак, варто розмежувати право на приватність та право на захист персональних даних. Незважаючи на те, що концепція захисту персональних даних розвинулась із права на приватність і право на захист персональних даних захищається в межах статей, які закріплюють прав на приватність, між цими правами існує суттєва різниця. Зокрема, ця різниця полягає у формулюванні та межах прав, адже право на приватність сформульоване як загальна заборона втручання в приватне життя, за винятком наявності виправданих підстав для такого втручання. Натомість право на захист персональних даних є сучасним та динамічним і стосується будь-яких випадків обробки персональних даних [16, с. 19-20].

Схожу думку висловив Пітер Гастінґс, Європейський інспектор із захисту

персональних даних (англ. *European Data Protection Supervisor, EDPS*) (далі – «Інспектор») з 2004 по 2014 роки. Він зазначає, що: «*захист персональних даних є ширшим поняттям, ніж захист приватності, оскільки стосується інших прав та свобод та всіх типів даних, незалежно від їхнього відношення до приватності, але водночас і більш обмежений, оскільки стосується тільки обробки персональних даних, коли ж інші аспекти приватності до уваги не беруться*» [17, с. 5].

1.2 Визначення поняття «персональні дані» та відомості, які ним охоплюються

Подальший розвиток захисту персональних даних можна прослідкувати у регіональному та національному законодавстві, зокрема у Директиві 95/46/ЄС Європейського парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року (англ. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Directive 95/46*) (далі «Директива»), яка врегульовувала питання захисту персональних даних у Європейському Союзі. На тексті цієї директиви базувалась розробка та прийняття Закону України «Про захист персональних даних» № 2297-VI від 1 червня 2010 року (далі «Закон») [9, с. 17].

На основі законодавства (міжнародного, регіонального та національного), яке врегульовує питання, які відносяться до сфери персональних даних, та інших дотичних інструментів ми спробуємо визначити, що саме означає поняття «персональні дані» та які відомості відносяться до персональних даних. Відтак, ми проаналізуємо, як визначають поняття «персональні дані» та які відомості до нього відносять у (***1.2.1***) Європейському Союзі, (***1.2.2***) США та (***1.2.3***) Україні.

1.2.1 Визначення поняття «персональні дані» та відомості, які до нього відносяться, у законодавстві Європейського Союзу

Один із перших правових інструментів, який врегульовував сферу захисту персональних даних – це вже згадана вище Конвенція 108. У статті 2 «Визначення» Конвенції 108 персональні дані пояснюються як «*інформація, що стосується конкретно визначеної особи або особи, що може бути конкретно визначеною*» [8]. Варто зазначити, що таку особу прийнято називати «суб'єктом даних» (стаття 2 та 4(1) відповідно) [18; 19].

У праві Європейського Союзу превалює використання саме терміну «персональні дані» (англ. *personal data*). Зокрема, термін «персональні дані» використовується у Директиві [20], а також у Регламенті Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних), (англ. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (*General Data Protection Regulation*)) (далі – «Регламент»), який прийшов на заміну Директиві і набув чинності 25 травня 2018 року [19].

Варто зауважити одразу, що Регламент поширюється не тільки на держав-членів Європейського Союзу, але й на держав-членів Європейської економічної зони, тобто в тому числі на Ісландію, Норвегію, Ліхтенштейн. В цілях цієї роботи на позначення держав, на які поширюється регламент, використовуватиметься формулювання «держави-члени».

Директива надавала визначення терміну «персональні дані» наступним чином: «*персональні дані» означають будь-яку інформацію, що стосується ідентифікованої фізичної особи чи фізичної особи, яку можна ідентифікувати («суб'єкт даних»); особою, яку можна ідентифікувати, є така, яка може бути встановленою прямо чи опосередковано, зокрема, за допомогою*

ідентифікаційного коду або одного чи більше факторів, притаманних фізичним, фізіологічним, розумовим, економічним, культурним чи соціальним аспектам її особистості.»

Для кращого розуміння терміну подаємо визначення також в оригіналі англійською мовою: «*personal data» shall mean any information relating to an identified or identifiable natural person («data subject»); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*» (стаття 2 (a)) [20].

Як бачимо із наведеного визначення та його оригінального звучання, рсональні дані в першу чергу повинні стосуватись саме фізичної особи, яка ідентифікована, або яку можна ідентифікувати. Крім того, такі відомості повинні вказувати на певні фактори, які специфічні (від вживання слова *specific* в оригінальній версії терміну з Директиви) для певної особи, тобто характерні виключно для цієї особи. Отже, персональні дані – це не будь-яка відомість чи сукупність відомостей про фізичну особу, а тільки така відомість чи її сукупність, яка вказує на конкретну фізичну особу з-поміж інших. Тобто, просто ім’я особи не викликатиме застосування законодавства у сфері захисту персональних даних, якщо воно самостійно не є унікальним і не дозволяє ідентифікувати конкретну особу без будь-якої іншої додаткової інформації [16, с. 90].

Варто зазначити, що обробка інформації щодо «ідентифікованої особи» та «особи, яку можна ідентифікувати» захищаються однаковим чином [16, с. 88]. Як видно із визначення, ідентифікація особи не обмежується її громадянським чи юридичним статусом. Ідентифікація особи пов’язана саме з її індивідуалізацією, тобто можливістю виділити конкретну особу серед інших в тому числі за допомогою ознак, які не обов’язково пов’язані з номером паспорта чи місцем реєстрації, як от псевдонім, локація, IP-адреса персонального комп’ютера. Варто також враховувати, що надмірна складність процесу ідентифікації особи, тобто залучення великої кількості ресурсів та часу для

встановлення особи, теж може вказувати на те, що особа не є такою, яку можна ідентифікувати (англ. *identifiable*) (параграф 17) [21, с. 3-4].

Свого часу Директива мала на меті гармонізувати законодавство держав-членів, зробити його послідовним та врегулювати вільну передачу персональних даних між державами [16, с. 29; 17, с. 9]. Однак, Директива мала бути імплементована в національне законодавство держав-членів Європейського Союзу, що залишало певну дискрецію державам при розробці власних законів [16, с. 30], а відтак регулювання сфери захисту персональних даних все одно здійснювалось у державах-членах Європейського Союзу по-різному.

У зв'язку з тим, що національне законодавство держав-членів Європейського Союзу у сфері захисту персональних даних таки відрізнялось через різну імплементацію Директиви у національну систему кожної держави, а також у зв'язку із швидким технологічним прогресом, появою соціальних мереж та стрімкою глобалізацією, виникла потреба у розробці нового правого інструменту, який би врегульовував питання захисту персональних даних з урахуванням нових реалій. Такий інструмент мав відповідати сучасним умовам, а саме тим, які були спричинені технологічним прогресом, але при цьому не потребувати регулярного перегляду чи внесення змін в основний текст, тобто залишатись актуальним тривалий період часу. Таким інструментом став Регламент, який був прийнятий у квітні 2016 року та набув чинності у травні 2018 року [16, с. 30].

Відповідно до статті 4 Регламенту персональні дані визначаються як «*будь-яка інформація, що стосується фізичної особи, яка ідентифікована чи яку можна ідентифікувати («суб'єкт даних»); фізична особа, яку можна ідентифікувати, є такою особою, яку можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами як ім'я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи.*» В оригіналі англійською мовою визначення

звучить наступним чином: *«personal data» means any information relating to an identified or identifiable natural person («data subject»); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*» (стаття 4) [19].

Якщо порівнювати визначення персональних даних у Регламенті та в Директиві, можна зробити висновок, що вони майже ідентичні. Обидва визначення включають будь-яку інформацію (англ. *any information*) щодо ідентифікованої особи, або такої особи, яку можна ідентифікувати. Обидва визначення наводять схожий перелік ідентифікаторів за якими прямо чи опосередковано (англ. *directly or indirectly*) можна особу встановити. Основна відмінність полягає в тому, що за Регламентом коло цих ідентифікаторів є більш уточненим. Окрім таких ідентифікаторів як ідентифікаційний номер або один чи більше факторів, що є визначальними для її фізичної, фізіологічної, розумової, економічної, культурної чи соціальної сутності (англ. *identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*), що містяться у Директиві, Регламент також включає ім'я, дані про місцеперебування, онлайн-ідентифікатор (англ. *name, location data, an online identifier*), а до факторів також відносить ті, що стосуються генетичної сутності (англ. *genetic identity*).

Відтак, можна зробити висновок, що поняття «персональні дані» в Європейському Союзі за своїм змістом є відносно сталим та чітко визначеним. Змінюється тільки список цих ідентифікаторів, за якими особа може бути встановлена, однак він не є вичерпним і законодавство наводить ці ідентифікатори як приклад. У системі Європейського Союзу під персональними даними розуміють будь-яку інформацію про фізичну особу, яка ідентифікована або яку можна ідентифікувати прямо чи опосередковано за певними ідентифікаторами, такими як ім'я, ідентифікаційний номер тощо або за одним чи декількома факторами, що стосуються сутності цієї особи.

1.2.2 Визначення поняття «персональні дані» та відомості, які до нього відносяться, у законодавстві США

Якщо переходити до визначення поняття «персональні дані» у правовій системі США, варто врахувати кілька нюансів. Як відомо, система законодавства США складається із федерального законодавства, законодавства штатів, законодавства округу Колумбія, а також законодавства територій. Окрім того, значна частина американського законодавства є некодифікованою, на відміну від права континентальних держав (в тому числі права Європейського Союзу та держав-членів Європейського Союзу), і складається із судових прецедентів, а судова система є дворівневою: федеральна судова система та судова система штатів [22, с. 69]. У зв'язку з цим деякі питання врегульовуються безпосередньо на рівні штатів, але не мають уніфікованого врегулювання на федеральному рівні. В той же час практика правового регулювання тотожних ситуацій може різнитись у кожному із п'ятдесяти штатів США.

У США відсутнє уніфіковане законодавство в сфері захисту персональних даних. Правове регулювання цих відносин здійснюється відповідно до федерального законодавства, законодавства штатів та інших регуляторних актів, що врегульовують захист персональних даних у в різних сферах діяльності [23, с. 3]. Відтак, відсутній і єдиний підхід до визначення персональних даних, адже та інформація, яка вважається в рамках одного закону персональною і захищається відповідно до норм цього закону, може такою не вважатись відповідно до іншого закону, що врегульовує відносини в іншій сфері (пункт 2.1) [24].

Варто також зазначити, що в законодавстві США, на відміну від українського законодавства та законодавства Європейського Союзу, превалює використання терміну «персональна інформація» (англ. *personal information*), а не персональні дані (англ. *personal data*).

Якщо розглядати федеральне законодавство, то загального акту, який би

визначав основні терміни, принципи та рамки захисту персональних даних, як от Регламент в Європейському Союзі, немає. Натомість, федеральне законодавство містить окремі закони, які визначають захист даних фізичних осіб в конкретно взятих умовах. Значна кількість такого законодавства, як от Закон про контроль над розсилкою непогодженої із отримувачем порнографії та реклами від 2003 року (англ. *Controlling the Assault of Non-Solicited Pornography And Marketing* (*CAN-SPAM*) *Act of 2003*) (далі «CAN-SPAM Act»), що врегульовує питання розсилки спаму, тобто розсилки повідомлень комерційного змісту без погодження із отримувачем, що в тому числі охоплює збирання та використання електронних адрес (емейлів) для розсилки спаму, не дає визначення, що таке персональна інформація через своє вузьке регулювання [25, с. 303; 26].

Схожа ситуація виникає і щодо Закону про приватність в електронній комунікації (англ. *Electronic Communications Privacy Act*), що врегульовує питання несанкціонованого доступу до електронної комунікації осіб, а також Закону про комп'ютерне шахрайство та зловживання (англ. *Computer Fraud and Abuse Act*), що забороняє несанкціонований доступ до комп'ютера чи перевищення меж санкціонованого доступу. Зазначені закони відносять до таких, що врегульовують захист персональних даних, адже IP-адреса комп'ютера чи електронна адреса можуть вважатися персональними даними. Однак, ці закони не містять визначення персональних даних, оскільки врегульовують питання захисту персональних даних дуже опосередковано [25, с. 304].

Закон про модернізацію фінансових послуг, більш відомий як Гремм-Ліч-Блілі Акт (англ. *Gramm-Leach-Bliley Act, GBLA*), що врегульовує захист інформації про фінансовий стан користувачів, надає визначення поняттю «непублічна персональна інформація» (англ. *nonpublic personal information*) під якою має на увазі особисту фінансову інформацію, що ідентифікує особу і яка надана споживачем фінансовій установі; що випливає із будь-якої транзакції із споживачем або будь-якої послуги наданої споживачу; чи іншим чином отриманої фінансовою установою. В оригіналі англійською визначення звучить

наступним чином: *«nonpublic personal information» means personally identifiable financial information (i) provided by a consumer to a financial institution; (ii) resulting from a transaction with the consumer or from a service provided to the consumer; or (iii) otherwise obtained by the financial institution»* (стаття 509 (4)) [27]. Однак, як бачимо, в рамках зазначеного закону персональною інформацією є тільки фінансові дані через спеціальну сферу регулювання – надання фінансових послуг.

Ще одним актом, що дає визначення персональній інформації є Закон про мобільність та підзвітність медичного страхування (англ. *Health Insurance Portability and Accountability Act, HIPAA*) (далі «HIPPA»). HIPAA врегульовує захист медичної звітності та особистих медичних даних пацієнтів і встановлює, які дані вважаються захищеною інформацією про пацієнта (англ. *protected health information*). Як зазначає Міністерство охорони здоров'я і соціальних служб США (англ. *U.S. Department of Health & Human Services Office for Civil Rights*) з посиланням на HIPAA, такими є минулі та актуальні дані про стан здоров'я особи; дані про надання медичних послуг особі; та минулі та актуальні дані про оплату наданих медичних послуг, які надають можливість ідентифікувати особу, або ж є достатня підстава вважати, що особу можна ідентифікувати за такими даними [28, с. 3-4]. Тобто захищаються виключно ті персональні дані, які стосується здоров’я особи, а такі дані як емейл чи адреса проживання самі по собі захищеною інформацією пацієнта не вважатимуться.

Таким чином, можна зробити висновок, що у федеральному законодавстві США відсутнє єдине визначення поняття «персональної інформації». Персональна інформація визначається тільки у спеціальних законах із вузькою сферою регулювання, які відносять до персональної інформації ті відомості, що можуть ідентифікувати особу у конкретній сфері чи відносинах, як от медичні дані чи фінансові дані. Якщо інформація про особу міститиме дані, які не містять медичної чи фінансової інформації, тоді така персональна інформація не попадає під захист зазначених законів.

На рівні законодавства штатів США, деякі штати мають розроблене

законодавство у сфері захисту персональних даних, як загальне, так і таке, що врегульовує збір персональної інформації в конкретно визначеній сфері.

Зокрема, актом загального регулювання є Закон про приватність споживачів у Каліфорнії (англ. *California Consumer Privacy Act, CCPA*) (далі «CCPA»), який також часто називають каліфорнійським GDPR, що був прийнятий у 2018 році в Каліфорнії та набув чинності 1-го січня 2020 року [29]. CCPA встановлює правила поводження із персональною інформацією споживачів, а також права таких споживачів щодо своєї персональної інформації, яка збирається суб'єктами господарювання.

Під «персональною інформацією» в CCPA мається на увазі та інформація, що: «*ідентифікує, стосується, описує або розумним способом може бути асоційована, чи розумним способом пов'язана, прямо чи опосередковано, із конкретним споживачем чи сім'єю*.» В оригіналі визначення звучить наступним чином: «*personal information» means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household*.» Окрім загального визначення, CCPA також наводить невичерпний приклад та список такої інформації, яка може вважатись персональною. Зокрема, CCPA вказує, що така персональна інформація може включати, але не обмежуючись, наступну інформацію як от ідентифікатори (справжнє ім'я, псевдонім, поштова адреса, унікальний персональний ідентифікатор, онлайн-ідентифікатор, IP адреса, електронна пошта, назва особистої сторінки, номер соціального страхування, номер водійського посвідчення, номер паспорту чи інші схожі ідентифікатори), біометрична інформація, геолокація, інформація про працевлаштування та, навіть, історія браузера чи пошуку (стаття 1798.140 (o)) [30].

Якщо порівнювати зазначене визначення із визначенням у Регламенті, одразу можна сказати, що воно є ширшим за обсягом та більш деталізованим. Наприклад, окрім такої характеристики як можливість ідентифікувати особу, інформація щоб вважатись персональною може ще просто асоціюватись, описувати чи бути пов'язаною із конкретною особою. Зазначені характеристики

не завжди тотожні із поняттям ідентифікація, оскільки не завжди опис особи дозволяє її ідентифікувати. Відтак, виходячи із визначення, інформація, яка може бути персональною за CCPA, може не бути персональними даними за Регламентом. Окрім того, CCPA як персональну також вважає інформацію щодо сім'ї (в оригіналі використовується термін «*household*»), коли ж за Регламентом суб'єктом персональних даних завжди є конкретна фізична особа. Також, CCPA містить хоч невичерпний, але таки перелік інформації, яка може вважатись персональною, що також відсутнє у тексті Регламенту, та містить застереження, що персональною не вважається та інформація, яка доступна публічно, тобто легально доступна із федеральних реєстрів, реєстрів штату чи місцевих реєстрів (стаття 1798.140 (o) (2)) [30].

Таким чином, можна зробити висновок, що у штаті Каліфорнія поняття «персональної інформації» відрізняється від поняття «персональних даних», яке застосовне у праві Європейського Союзу, оскільки включає в себе ширше коло відомостей, які можуть вважатися персональною інформацією і, водночас, не бути персональними даними за правом Європейського Союзу.

Визначення «персональної інформації» також можна зустріти у праві штату Массачусетс. У акті 201 CMR 17.00: Стандарти захисту персональної інформації резидентів Співдружності (англ. *201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth*, *201 CMR 17.00*) (далі «201 CMR 17.00») як персональна інформація визначається ім'я та прізвище резидента Массачусетсу, чи ініціал імені та прізвище, у комбінації із відомостями, які стосуються такого резидента. До таких відомостей відносяться номер соціального страхування, номер водійського посвідчення чи виданий штатом номер ідентифікаційної картки, номер фінансового рахунку чи кредитної, дебетової картки, код доступу, персональний ідентифікатор чи пароль, що надають доступ до фінансового рахунку резидента (стаття 17.02) [31]. Із зазначеного визначення вбачається, що обсяг персональної інформації вужчий за обсяг CCPA та Регламенту, оскільки стосується чітко визначеного списку ідентифікаторів, який є значно коротшим за той же ж список, наведений у CCPA.

У штаті Нью-Йорк питання приватності врегульоване у параграфі 899-аа Загального законодавства про господарську діяльність (англ. *General Business Law § 899-aa, GBL*) (далі «GBL»). У цьому законодавстві використовуються два терміни: «персональна інформація» та «приватна інформація». Під персональною інформацією мається на увазі будь-яка інформація, що стосується фізичної особи, її ім'я, номер, персональне позначення чи інший ідентифікатор, що можуть бути використані для ідентифікації цієї особи. В оригіналі визначення звучить наступним чином: «*personal information» shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person*» (стаття 1 (a)) [32]. Приватна інформація, відповідно до GBL, це теж персональна інформація, що складається із будь-якої інформації у поєднані з одним чи більше елементів, коли або персональна інформація або елемент не є зашифрованим або зашифровані, але ключ шифрування є у наявності. До таких елементів даних GBL відносить номер соціального страхування, номер водійського посвідчення чи номер ідентифікаційної картки не водія, номер рахунку, кредитної чи дебетової картки у поєднанні з будь-яким кодом безпеки, кодом доступу чи паролем, що надає доступ до фінансового рахунку особи (стаття 1 (b)) [32].

Наведене визначення приватної інформації та список елементів даних перегукується майже дослівно із визначенням персональної інформації у массачусетському акті 201 CMR 17.00 та списком відомостей і є вужчим, ніж визначення персональної інформації за CCPA. Однак, виділення із поняття «персональної інформації» приватної зустрічається вперше і не відповідає тенденціям федерального законодавства чи законодавства штатів. Цікаво також те, що визначення персональної інформації за GBL є доволі широким і за змістом схожим до визначення у Регламенту через відсилку до імені, номеру особи чи інших даних (ідентифікаторів), за якими особа може бути ідентифікована.

Відтак, з описаної вище інформації можна зробити кілька висновків про поняття «персональної інформації» в США. По-перше, на федеральному рівні відсутнє загальне визначення поняття «персональна інформація», а

законодавство захищає тільки спеціально визначені групи відомостей, що стосуються фізичних осіб. Загальне законодавство, що в тому числі надає визначення поняттю «персональна інформація» більш розвинене на рівні штатів. По-друге, на рівні штатів підхід до визначення поняття персональної інформації також не є уніфікованим, оскільки деякі штати звужують поняття до таких елементів як ім'я у поєднанні із номером соціального страхування чи водійським посвідченням, в той час як інші штати визначають поняття персональної інформації доволі широко та відносять туди великий за обсягом перелік відомостей. Варто також зазначити, що підхід до визначення персональної інформації тільки частково перетинається із підходом Європейського Союзу. Це пояснюється не тільки використанням різних термінів («дані» та «інформація»), але обсягом поняття та його визначеністю. Наприклад, відповідно до Регламенту, інформація обов'язково має ідентифіковувати фізичну особу, а приблизний перелік не наводиться, коли ж відповідно до CCPA окрім ідентифікації така інформація може ще описувати, стосуватись тощо особи і зазвичай наводиться примірний список такої інформації, що може відноситись до персональної.

1.2.3 Визначення поняття «персональні дані» та відомості, які до нього відносяться, у законодавстві України

Українська правова доктрина та законодавство використовують різні терміни на позначення інформації про особу. Наприклад, Закон України «Про інформацію» у статті 11 використовує термін «інформація про особу» і в дужках зазначає «персональні дані». Відповідно до цього визначення: «*інформація про особу (персональні дані) – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована*» (частина 1 статті 11) [33]. Відповідно до наведеної статті, інформація про особу та персональні дані це одне і те ж.

У профільному Законі використовується тільки поняття «персональні дані». Відповідно до Закону: «*персональні дані – відомості чи сукупність*

відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована» (стаття 2) [18]. Тобто Закон повністю відтворює визначення, наведене у Законі України «Про інформацію», але використовує на позначення тільки поняття «персональні дані» без згадки «інформації про особу».

Однак, окрім цих двох понять, які загалом позначають одне і теж, в українському законодавстві, зокрема вже згаданому Законі України «Про інформацію» також використовується поняття «конфіденційна інформація». Відповідно до частини 2 статті 21 Закону України «Про інформацію», конфіденційна інформація це інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень [33]. Тобто, конфіденційна інформація як і персональні дані – це інформація про фізичну особу.

У Законі України «Про доступ до публічної інформації» є ще одне визначення поняття «конфіденційна інформація», яке звучить наступним чином: «*інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов*» (частина 1 статті 7) [34]. Наведений варіант визначення відрізняється від того, який запропонований у Законі України «Про інформацію».

Таким чином, виникає проблема співвідношення між собою понять, які позначають інформацію про фізичну особу, та обсяг захисту, який такий інформації надається.

В українській аналітиці при спробі розібратись у співвідношенні цих понять висувається думка, що не всі персональні дані є конфіденційною інформацією, оскільки вони можуть перебувати у відкритому доступі і бути відкритою інформацією. Наприклад, список осіб, що вступили на бюджетні місця до закладів вищої освіти. В той же час, не вся конфіденційна інформація є персональними даними, якщо це інформація про юридичну особу або за цією інформацією неможливо ідентифікувати фізичну особу. Одночасно, можуть існувати персональні дані, що є конфіденційною інформацією, тобто доступ до

яких є обмеженим [35].

Відтак, в Україні на позначення інформації про фізичну особу використовуються різні терміни, як «інформація про особу», «конфіденційна інформація» та «персональні дані». В той же час ці поняття не є повністю тотожними та підпадають під регулювання різних законодавчих актів, а чітке розмежування понять відсутнє, що може спричинити невизначеність щодо правового режиму, який до такої інформації має застосовуватись.

Якщо ж повертатись до поняття «персональні дані» в Регламенті чи «персональної інформації» у законодавстві США, то саме визначення «персональних даних» у Законі є найбільш схожим до цих понять, оскільки містить в собі такі ж характеристики, яким мають відповідати дані, щоб вважатись персональними. Зокрема, це інформація про фізичну особу та можливість її ідентифікувати.

Закон, як і Регламент, не наводить приблизного, невичерпного чи будь-якого переліку примірних відомостей, що можуть вважатися персональними даними, на відміну від законодавства США. Однак, Конституційний Суд України у рішенні № 2-рп/2012 від 20 січня 2012 року, надаючи своє тлумачення частині першій та другій статті 32 Конституції України, яка закріплює право на повагу до приватного та сімейного життя, надав своє визначення персональним даним і вказав наступне: «*інформація про особисте та сімейне життя особи (персональні дані про неї) - це будь-які відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована*, *а саме: 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. Така інформація про фізичну особу та членів її сім'ї є конфіденційною і може бути поширена тільки за їх згодою, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини» (пункт 3.3) [36]. Конституційний Суд України навів приблизний перелік інформації, яка може вважатись персональною, як от національність, освіта, сімейний стан, релігійній переконання тощо і відніс цю інформацію не тільки до персональних даних, а ще й до конфіденційної інформації, тобто тієї, яка не є відкритою.

Якщо брати до уваги наведені визначення в українському законодавстві, то можна зробити наступні висновки. По-перше, визначення поняття «персональних даних» за українським законодавством в цілому збігається із визначенням поняття «персональні дані» у законодавстві Європейського Союзу, зокрема, із визначенням у Регламенті та Директиві, на основі якої й писався Закон. По-друге, українське законодавство теж не містить відсилання до переліку відомостей, які можуть бути персональними даними, на відміну від законодавства США, якщо не враховувати тлумачення Конституційного Суду України, де перелік таких відомостей теж не є вичерпним. По-третє, в законодавстві України існує кілька визначень, що позначають інформацію про фізичну особу, які не є чітко розмежовані у законодавстві, і можуть одночасно застосовуватись до однієї і тієї ж інформації, що може спричинити проблеми у застосування до такої інформації відповідного правового режиму на основі належного нормативно-правового акту.

Висновки до Розділу 1

Підсумовуючи, концепція захисту персональних даних почала розвиватись ще на початку XX століття і безпосередньо сформувалась на початку 1980-х років в рамках права на приватність, а саме із статті 8 Конвенції, що чітко прослідковується у практиці ЄСПЛ. Вирішення питань, які стосуються захисту персональних даних фізичних осіб, продовжують розглядати й надалі в рамках

статей, що забезпечують право на приватність.

В той же час, варто пам’ятати, що хоч захист персональних даних та захист права на приватність можуть мати тотожні правові підстави захисту (як статті міжнародних актів), право на захист персональних даних та право на приватність не є тотожними. Зокрема, не завжди персональні дані фізичних осіб покриватимуться захистом приватного життя особи, як і не завжди при втручанні в приватне життя особи відбувається втручання в обробку її персональних даних. Тобто, якщо говорити про співвідношення, ці дві концепції перетинаються між собою, але не є тотожними і не є частинами цілого.

Щодо питання визначення поняття «персональних даних», то у правових системах світу немає єдиного підходу. Україна та Європейський Союз мають спільні підходи до визначення поняття, що зумовлено в тому числі тим, що українське законодавство в сфері захисту персональних даних орієнтується на законодавство Європейського Союзу та наявний там правовий режим у сфері захисту персональних даних. Натомість, у США відсутній єдиний підхід до визначення, що є персональною інформацією, і обсяг інформації, яка захищається, залежить від закону, який застосовується.

Однак, варто зауважити, що всі три наведені системи об’єднує підхід до обов’язкових ознак, якими має бути наділена інформація чи дані, щоб бути персональними: стосуватись фізичної особи, яка ідентифікована або надавати можливість цю особу ідентифікувати за сукупністю цієї інформації чи даних. Відтак, діяльність публічних органів необхідно розглядати в контексті нагляду за дотриманням законодавства, яке врегульовує питання обробки і захисту інформації про фізичних осіб, які ідентифіковані або яких можливо ідентифікувати.

РОЗДІЛ 2. ДІЯЛЬНІСТЬ ПУБЛІЧНИХ ОРГАНІВ У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ЄВРОПЕЙСЬКОМУ СОЮЗІ

Як було згадано у Розділі 1, основні засади діяльності у сфері обробки персональних даних осіб у Європейському Союзі встановлені Регламентом. Здійснюють обробку персональних даних у Європейському Союзі контролери (англ. *controllers*) та оператори (англ. *processors*). Це можуть бути як фізичні, так і юридичні особи, органи публічної влади тощо. Контролери визначають мету та засоби обробки персональних даних. Оператори безпосередньо здійснюють обробку персональних даних від імені контролера (стаття 4 (7), (8)) [19].

Оскільки Європейський Союз є квазі-об'єднанням держав, зі своїм парламентом, урядом та судовою системою, в цьому розділі в межах діяльності публічних органів, розглядатиметься як діяльність на національному рівні держав-членів, так і на наднаціональному, тобто в структурі органів Європейського Союзу.

Відповідно до Регламенту, у державах-членах існують наглядові органи (англ. *supervisory authorities*), які зобов'язані забезпечити нагляд за дотриманням вимог Регламенту. В той же час Регламент передбачає існування центрального органу в Європейському Союзі – це Європейська рада із захисту даних (англ. *European Data Protection Board, EDPB*) (далі «Рада»), до якої входять голови наглядових органів держав-членів (їхні представники), а також Європейський інспектор із захисту даних. У Розділі 2 ми розглянемо, як працюють зазначені органи для забезпечення захисту персональних даних та комплаєнсу із Регламентом, яку роль вони виконують. Відповідно, ми розглянемо діяльність (**2.1**) наглядових органів держав-членів та (**2.2**) діяльність Ради та Інспектора.

2.1 Діяльність наглядових органів держав-членів у сфері захисту персональних даних

У пункті 117 преамбули Регламенту сказано: «*заснування наглядових*

органів у державах-членах, наділених правом виконувати свої завдання та реалізовувати свої повноваження у повній незалежності, є істотним компонентом захисту фізичних осіб у зв'язку з опрацюванням їхніх персональних даних» (пункт 117 преамбули) [19]. Для того, щоб проаналізувати, як працюють ці наглядові органи, ми розглянемо (***2.1.1***) засади та основні принципи функціонування наглядових органів, встановлені Регламентом, а також (***2.1.2***) діяльність наглядових органів держав-членів.

2.1.1 Засади та основні принципи функціонування наглядових органів у Європейському Союзі відповідно до Регламенту

Питання наглядових органів врегульоване і розділі 6 Регламенту. Зокрема, сам розділ має назву «незалежні наглядові органи» (англ. *independent supervisory authorities*), що одразу ж вказує на одну з перших та основних ознак таких органів – їхню незалежність. Відповідно до Регламенту, у кожній із держав-членів має бути незалежний публічний (державний) орган, що здійснюватиме моніторинг за застосуванням Регламенту, а також вноситиме свій вклад у послідовне (англ. *consistent*) застосування Регламенту у Європейському Союзі. Здійснювати функцію моніторингу ці органи будуть в тому числі для забезпечення прав фізичних осіб під час обробки їх персональних даних. Таких органів у державі може бути як один, так і кілька (стаття 51) [18].

Такі наглядові органи прийнято називати органами захисту даних (англ. *Data Protection Authority, DPA*) (далі «DPA») [37]. Хоч сам текст Регламенту згадує наглядовий орган саме як «орган захисту даних» тільки раз, у преамбулі в пункті 104, поза межами Регламенту за наглядовими органами закріпилась саме ця назва. Європейська комісія зазначає, що органи захисту даних здійснюють нагляд через свої повноваження здійснювати розслідування та застосовувати коригувальні (виправні) заходи, а також надають свої експертні поради щодо питань захисту персональних даних та розглядають скарги щодо порушень Регламенту. Окрім цього, вони інформують населення щодо їхніх прав та

обов’язків в контексті захисту персональних даних, встановлюють які операції потребують проведення оцінювання впливу на захист персональних даних [38; 39].

Повна незалежність наглядового органу

Важливою ознакою наглядового органу, як вже було згадано вище, є незалежність. Ця ознака була безпосередньо загадана ще у пункті 121 преамбули Регламенту, у якому було вказано: «…*для забезпечення незалежності наглядового органу, член або члени повинні діяти добросовісно, утримуватися від будь-якої дії, що є несумісною з іншими їхніми обов'язками, та не повинні, протягом строку їхніх повноважень, займатися будь-якою несумісною діяльністю, прибутковою чи ні*» [19]. Зазначені у пункті 121 преамбули умови щодо незалежності були безпосередньо перенесені у статті Регламенту та деталізовані відповідно, як буде показано нижче.

Відповідно до частини 1 статті 52 Регламенту: «*кожний наглядовий орган діє абсолютно незалежно під час виконання своїх завдань та здійснення своїх повноважень згідно з цим Регламентом*» [19]. У наступних частинах статті Регламенту розкрито, що ж саме складає незалежність наглядового органу. Зокрема, це відсутність прямого чи опосередкованого зовнішнього впливу, заборона несумісної діяльності, наявність необхідних людських, технічних, фінансових ресурсів для забезпечення діяльності наглядового органу, обрання свого власного персоналу та незалежний фінансовий контроль за діяльністю наглядового органу і відокремлений публічний річний бюджет (частина 2-5 статті 52) [19].

Наступні статті Регламенту містять вимоги, які гарантують незалежність наглядових органів. Зокрема, це вимоги прозорості процедури призначення членів наглядового органу, їхньої належної компетенції, припинення їхніх повноважень, підстави звільнення (стаття 53) [19]. До цих гарантій також віднесена частина 1 статті 54 Регламенту, яка встановлює обов’язок держав-членів Європейського Союзу забезпечити на рівні законів заснування таких наглядових органів, вимоги до кандидатів в члени наглядового органу та

процедуру призначення, строк повноважень членів та можливість переобрання, обов'язки членів наглядового органу, вимоги щодо несумісності, припинення повноважень [19].

Велика увага врегулюванню питання незалежності наглядового органу не є новинкою Регламенту. Незалежність наглядових органів була свого часу передбаченою ще в частині 2 статті 16 Договору про функціонування Європейського Союзу (англ. *Treaty on the Functioning of the European Union, TFEU*) [40]. Контроль за комплаєнсом у сфері захисту персональних даних був покладений на наглядовий орган у частині 3 статті 8 Конвенції основоположних прав Євпропейського Союзу (англ. *Charter of Fundamental Rights of the European Union*) [41]. Свого часу Директива також встановлювала повну незалежність наглядових органів (пункт 62 преамбули та частина 1 статті 28) [20]. Така повна незалежність (англ. *complete independence*) має бути забезпечена і відповідно до Регламенту (пункт 117 преамбули) [19].

Поняття повної незалежності наглядових органів свого часу розтлумачив Європейський суд справедливості (англ. the *Court of Justice of the European Union, CJEU*). Зокрема, у одній із найбільш цитованих справ, C-518/07 (Європейська комісія проти Німеччини) від 9 березня 2010 року, Європейський суд справедливості встановив що саме розуміють під питанням повної незалежності [42, с. 27]. Зокрема, суд встановив наступне: «*гарантія незалежності національних наглядових органів покликана забезпечити ефективність та надійність нагляду за комплаєнсом положень про захист фізичних осіб при обробці персональних даних і повинна тлумачитися з урахуванням цієї мети… з цього випливає, що під час виконання своїх обов'язків наглядові органи повинні діяти об'єктивно та неупереджено. З цією метою вони повинні залишатися вільними від будь-якого зовнішнього впливу, включаючи прямий або опосередкований вплив держави або земель, а не впливу лише підконтрольних органів*» (параграф 25) [43]. Важливим моментом при визначенні, чи була дотримана повна незалежність, було вирішення питання щодо державної перевірки (англ. *state scrutiny*), якому піддавався наглядовий орган в Німеччині.

Суд вказав, що існує можливість, що органи державної перевірки, які перебували під контролем уряду відповідної Землі, не в змозі діяти об'єктивно щодо питань обробки персональних даних, оскільки уряд може виступати зацікавленою стороною, особливо в питання державно-приватного партнерства та укладених в рамках цього партнерства угод (параграф 34, 35) [43]. Більше того, суд по-факту вказав, що наглядовий орган, має бути відділений від уряду, для забезпечення свої незалежності від «зацікавленого» уряду [42, с. 28], а також вказав, що принцип демократії не виключає можливості існування держаних органів за межами «класичного ієрархічного управління» (параграф 42) [43].

У справі С-614/10 (Європейська комісія проти Австрії) від 16 жовтня 2012 року, Європейський суд справедливості теж розглядав питання незалежності наглядових органів, яке було пов'язане із тим, що хоч наглядовий орган Австрії (нім. *Datenschutzkommission, DSK*) володів операційною незалежністю, вона не є достатньою для забезпечення повної незалежності, яка вимагається відповідно до Директиви (параграф 60, 61) [44]. Зокрема, це питання дуже тісно було пов'язане із незалежністю персоналу та посадових осіб наглядового органу. Суд вказав: «*персонал, який надається в розпорядження офісу ДСК, складається з чиновників Федеральної Канцелярії, які підпорядковуються Федеральній Канцелярії…такий нагляд з боку держави не є сумісним з вимогою незалежності, викладеною у другому підпункті статті 28 (1) Директиви 95/46, який повинен задовільнятися наглядовими органами для захисту персональних даних… Той факт, що офіс складається з посадових осіб Федеральної Канцелярії, яка підлягає нагляду ДСК, несе ризик впливу на рішення ДСК. У будь-якому випадку, така організаційна накладка між ДСК та Федеральною Канцелярією перешкоджає ДСК бути над будь-якими підозрами в упередженості, а тому несумісне з вимогою "незалежності" у значенні другого підпункту статті 28 (1) Директиви 95/46*» (параграф 59, 61) [44].

Якщо знову звернутись до тексту чинного Регламенту, а саме до статей 52-54 Регламенту, можна зробити висновок, що позиція та висновки Європейського суду справедливості щодо повної незалежності наглядових

органів, яких не було в тексті Директиви, були враховані у підготовці тексту Регламенту [19]. Зокрема, частина 2 статті 52 безпосередньо встановлює свободу членів наглядового органу від зовнішнього впливу, прямого чи опосередкованого, як було висловлено Європейським судом справедливості у справі Європейської комісії проти Німеччини [19]. Частина 5 статті 52 встановлює можливість наглядового органу мати власний персонал, який підпорядковується безпосередньому керівництву відповідних членів наглядового органу, тобто враховує позицію суду щодо несумісності вимоги незалежності та підпорядкованості персоналу іншому органу, ніж наглядовий орган [19]. Наступні статті 53 та 54 Регламенту вже встановлюють обов'язок держав-членів цю незалежність забезпечити [19].

Повноваження наглядових органів

Повноваження наглядових органів держав-членів Європейського Союзу викладені у Секції 2 Розділу 6 Регламенту, яка так і називається «Компетенція, завдання та повноваження» [19]. У статтях 55-59 розкривається, яка саме компетенція наглядових органів, які завдання вони повинні вирішувати та якими повноваженнями наділені.

Якщо порівнювати роль наглядових органів відповідно до Директиви та відповідно до Регламенту, то варто зазначити наступне. По-перше, хоч Регламент і базується на основних принципах Директиви, його норми є нормами прямої дії (тобто не передбачають обов'язкової імплементації в національне законодавство держав-членів Європейського Союзу). По-друге, компетенція наглядових органів є розширеною, а повноваження чітко визначеними.

Основне завдання наглядових органів – це забезпечення застосування Регламенту та комплаєнс із Регламентом (частина 1 статті 57) [19], [45, с. 2]. Список завдань, які мають вирішувати наглядові органи, є доволі обширним та довгим і наводиться у статті 57 Регламенту [19]. Зокрема, до цього списку, крім забезпечення застосування Регламенту та комплаєнсу із ним, віднесені завдання щодо моніторингу застосування Регламенту, сприяння обізнанню та розумінню громадськості щодо ризиків та прав, пов'язаних із обробкою персональних

даних, консультування парламенту, уряду, інших органів та установ щодо захисту прав громадян при обробці даних, розгляд скарг суб'єктів даних та проведення розслідування, співпраця із наглядовими органами інших держав, проведення розслідувань щодо застосування Регламенту, сприяти діяльності Європейської ради із захисту персональних даних, а також виконувати інші завдання, які стосуються захисту персональних даних (частина 1 статті 57) [19]. Цей список завдань не є вичерпним і на наглядовий орган можуть бути покладені інші завдання, що стосуються нагляду за захистом персональних даних.

Повноважень наглядових органів у Регламенті згруповані у три основні групи: повноваження з розслідування (англ. *investigative powers*), застосування санкцій та інших заходів впливу до порушників (виправні повноваження) (англ. *corrective powers*), а також дозвільні та консультативні повноваження (англ. *authorization and advisory powers*) (стаття 58) [19], [46, с. 33]. У Директиві були наявні чотири групи: повноваження з розслідування, повноваження втручання, повноваження брати участь у провадженнях та розглядати скарги (частина 3 статті 28) [20].

Перелік повноважень міститься у статті 58 Регламенту. Зокрема, до повноважень з розслідування віднесенні повноваження видавати розпорядження контролеру чи оператору, їхнім представникам, надавати інформацію, необхідну для виконання завдань наглядового органу, проводити аудити захисту персональних даних, здійснювати перегляд сертифікацій, повідомляти контролера або оператора про ймовірне порушення Регламенту, отримувати доступ до приміщень контролера або оператора, доступ до персональних даних та інформації для виконання завдань наглядового органу (частина 1 статті 58) [19].

Серед переліку повноважень з розслідування, важливим є те, що наглядовий орган може як розглядати скарги, так і самостійно починати провадження за наявності підозри у порушенні, а також подавати заяви щодо порушення Регламенту до суду (частина 5 статті 58) [19]; [37].

До виправних повноважень віднесені, зокрема, винесення контролеру або

оператору попереджень про ймовірне порушення, доган якщо обробка порушує Регламент, наказувати контролеру або оператору привести свою діяльність у відповідність Регламенту та попередити суб'єкта персональних даних про порушення, тимчасово обмежувати чи забороняти обробку, накладати адміністративний штраф тощо (частина 2 статті 58) [19].

Саме наявність виправних повноважень це те, що в основному відрізняє статус наглядових органів за чинною редакцією Регламенту від їхнього статусу в часи Директиви. Директива не відносила до повноважень наглядових органів можливість накладати штраф. Такі повноваження могли мати наглядові органи відповідно до національного законодавства держав-членів Європейського Союзу. Натомість Регламент безпосередньо передбачає можливість наглядових органів не просто здійснювати попередження чи догани контролерам та операторам, але й безпосередньо накладати штрафи на контролерів та операторів, які порушили положення Регламенту (частина 2(i) статті 58) [19].

До дозвільних та консультативних повноважень належать в тому числі консультування контролерів відповідно до процедур попередніх консультацій, надавати висновки щодо будь-якого питання, пов'язаного із захистом персональних даних парламентові, уряду тощо, у визначених випадках видавати дозволи на обробку, видавати висновки та затверджувати проєкти кодексів поведінки, здійснювати акредитацію органів сертифікації тощо (частина 2(i) статті 58) [19].

Зазначений перелік повноважень вперше деталізований у Регламенті, адже Директива не встановлювала повноважень наглядових органів щодо здійснення консультацій та дозвільної діяльності, а відсилала до національного законодавства (пункт 54 преамбули) [20].

Важливо зазначити, що компетенція та повноваження наглядових органів в часи Директиви встановлювались національним законодавством держав-членів [47, с. 343]. Натомість, чинний Регламент безпосередньо визначає основну компетенцію, завдання та повноваження, що залишає державам-членам меншу дискрецію у врегулюванні питань, пов'язаних із наглядовими органами у

національному законодавстві. Наприклад, держави-члени не можуть виключити із повноважень наглядових органів повноваження отримувати інформацію від контролерів та операторів, оскільки воно передбачене у Регламенті.

Однак, деякі держави-члени передбачили у національному законодавстві вимоги, яких мають дотримуватися наглядові органи при отриманні інформації від контролерів та операторів, яка підпадає під дотримання вимог збереження професійної таємниці (питання 15) [48]. Також, деякі держави-члени встановили обмеження щодо можливості накладати штрафи. Наприклад, у Люксембурзі наглядовий орган не може накласти штраф на державу чи органи місцевого самоврядування (питання 17) [48].

Компетенція

Регламент вказує, що наглядові органи мають бути компетентними виконувати ті завдання та здійснювати ті повноваження, які на них накладені Регламентом на території його держави-члена. Випадки, коли справи випадають з компетенції наглядових органів, стосуються, наприклад, обробки даних судами в межах їхніх судових повноважень (стаття 55) [19]. Інші випадки можуть бути передбачені у національному законодавстві.

У Європейському Союзі часто виникають випадки здійснення транскордонної обробки персональних даних, тому Регламент ввів так званий механізм «єдиного вікна» (англ. *one-stop shop mechanism*) для визначення відповідального наглядового органу за захистом персональних даних. Такий механізм дозволяє компаніям, що здійснюють транскордонну обробку персональних даних, обирати керівний наглядовий орган (англ. *lead supervisory authority*), тобто той орган, який першочергово розглядає питання діяльності цієї компанії при транскордонній обробці даних [49].

У контексті транскордонної обробки персональних даних варто згадати так звані відповідні наглядові органи (англ. *supervisory authority concerned*). Такі відповідні наглядові органи – це органи, яких стосуються питання обробки персональних даних, якщо контролер чи оператор мають своє місцезнаходження на території держави-члена цього наглядового органу, суб’єкт персональних

даних держави-члена наглядового органу зазнає чи може зазнавати значного впливу від обробки його персональних даних або скарга була подана до цього наглядового органу [49, с. 9].

Така концепція введена в тому числі з метою забезпечення компетенції відповідних наглядових органів у питаннях, що стосуються обробки персональних даних, наприклад, коли суб'єкт знаходиться поза юрисдикцією керівного наглядового органу. Керівний наглядовий орган та відповідний наглядовий орган зобов'язані співпрацювати. Відповідний наглядовий орган може, наприклад, самостійно вести справу, коли від цього відмовляється керівний орган, попередньо його попередивши (частина 2, 5 статті 56) [19].

Варто зазначити, що вимога співпраці між різними наглядовими органами Європейського Союзу є однією із основних у Регламенті. Така співпраця між наглядовими органами держав-членів в тому числі покликана забезпечити послідовність у застосування Регламенту на території Європейського Союзу, а також для здійснення обміну інформацією та взаємодопомоги при розгляді скарг, інших питань, що стосуються забезпечення застосування Регламенту [37].

Отже, наглядові органи у Європейському Союзі наділені доволі широким спектром повноважень, як повноваження з розслідування, виправні повноваження, так і консультаційні та дозвільні повноваження, а їхня роль та статус, зокрема в контексті обсягу їхніх повноважень, еволюціонували з часів прийняття Директиви до набрання чинності Регламентом. Важливою ознакою цих наглядових органів є їхня незалежність, забезпеченню якої приділяється значна увага. Не менш важливою є співпраця цих наглядових органів для Європейського Союзу, з метою забезпечення послідовності у застосуванні норм Регламенту, а відтак і належного захисту персональних даних.

2.1.2 Діяльність наглядових органів держав-членів

Як вже було зазначено у попередньому підрозділі, кожна із держав-членів повинна мати один чи кілька наглядових органів, які б здійснювали відповідні

функції у сфері захисту персональних даних відповідно до Регламенту та відповідали вимогам повної незалежності. Список цих наглядових органів можна знайти на вебсайті Ради. У кожній із держав створено по одному наглядовому органу, крім Німеччини та Бельгії, де таких органів є декілька [50].

Варто зауважити, що відколи Регламент набрав чинності у 2018 році, кількість повідомлень про порушення захисту персональних даних значним чином зросла, зокрема у Бельгії від 25 у 2017 році до 445 у 2018 році та Люксембургу від 3 у 2017 році до 172 у 2018 році, в тому числі завдяки Регламенту [51, с. 6, 17]. Також відбувся ріст у подачі скарг від суб'єктів персональних даних. У Нідерландах у 2018 році було подано 11 077 скарг, на відміну від 8 360 у 2017 році. У Данії у 2018 році було подано 5 515 скарг проти 2 213 у 2017 році, а в Австрії за 2018 рік надійшло 1 036 скарг проти 156 у 2017 році. Найбільший кількість скарг поданих у 2018 році спостерігалася саме у Нідерландах (на 30% більше в порівнянні з 2016 роком) та Франції (на 44% більше ніж у 2016 році) [52, с. 6-7, 9, 11, 16].

У 2020 році Європейська комісія підготувала звіт за результатами двох років застосування Регламенту. У цьому звіті в тому числі були зазначені результати діяльності наглядових органів держав-членів. Значна увага у звіті була присвячена виправним повноваженням наглядових органів, зокрема застосуванню штрафів та інших санкцій проти контролерів та операторів. Наприклад, Європейська комісія відзначила застосування наглядовими органами адміністративних штрафів, а також відмітила те, що «*інші санкції як от заборона обробки мали такий же ж ефект як і штрафи, якщо не більш стримуючий*» [53].

Також Європейська комісія звернула увагу на співпрацю між наглядовими органами різних держав-членів. У звіті зазначили, що оцінювати як працюють механізми співпраці доволі рано, але наглядовим органам вдалось добре взаємодіяти через механізм «єдиного вікна». Водночас, побудова загальних підходів та культури захисту персональних даних у всьому Європейському Союзі є триваючим процесом. Був відзначений також факт значного збільшення персоналу та бюджету наглядових органів з часу набрання чинності Регламентом

[53]. Наприклад, у Бельгії з 2016 до 2018 року кількість персоналу зросла у майже чотири рази (від 16 до 54), у Нідерландах вдвічі (з 72 до 157). Загалом таке зростання спостерігається у 19 державах і тільки в 5 спостерігалось зменшення кількості персоналу у період з 2016 по 2018 рік [45, с. 5, 7].

У Звіті також зазначили, що імплементація Регламенту була складним процесом для малого та середнього бізнесу, а обмеження на основі розміру операцій не є виправданим та не означає, що менші за розміром операції несуть менший ризик захисту персональних даних [53].

Діяльність наглядових органів у кожній із держав має свої особливості, оскільки в межах національного законодавства можуть встановлюватись специфічні правила діяльності для цих органів.

Наприклад, у Німеччині, як вже було зазначено раніше, є не один наглядовий орган, а декілька, що спричиняє іноді труднощі при збиранні статистичних даних про роботу наглядових органів у Німеччині. Різноманіття наглядових органів зумовлене тим, що Німеччина є федеративною державою, поділеною на Землі (нім. *Länder*), і в кожній цій одиниці є наглядовий орган. Загалом таких наглядових органів є 16, оскільки земель в Німеччині також 16. У кожній із Земель призначається свій наглядовий орган, який має відповідати вимогам Регламенту. У Німеччині прийнято розділяти нагляд за приватним сектором та за публічний сектором, а відтак здійснювати цей нагляд також можуть окремі органи [54]. Окрім наглядових органів у кожній із Земель, в Німеччині також є Федеральний Комісар із захисту персональних даних та свободи інформації (нім. *Bundesbeauftragte für Datenschutz und Informationsfreiheit, BfDI'*), який також діє як наглядовий орган для надавачів телекомунікаційних послуг і представляє Німеччину у Раді. У Німеччині діє спеціальна Конференція із захисту персональних даних, куди входять члени наглядових органів, що здійснюють нагляд як за приватним, так і публічним сектором (нім. *Datenschutzkonferenz, DSK*) [55].

У Бельгії, яка також є федеративною державою, є кілька наглядових органів. У Бельгії є основний наглядовий орган (фр. *Autorité de la protection des*

données), який виконує всі функції покладені на нього відповідно до Регламенту та представляє Бельгію у Європейській раді захисту даних. Окрім того, у Бельгії на федеральному рівні існує також орган контролю за поліцейською інформацією. Окрім цього, існують також регіональні наглядові органи, які здійснюють нагляд в основному за публічними органами [56].

Не менш цікавим є наглядовий орган Великої Британії. І, хоч формально Британія вже не є частиною Європейського Союзу, Офіс комісара з інформаційних питань (англ. *Information Commissioner's Office, ICO*), який залишається наглядовим органом вже після виходу Британії з Європейського Союзу був одним із найактивніших наглядових органів. Його штат налічує більше 500 чоловік [57], орган регулярно видавав тлумачення щодо застосування тих чи інших положень Регламенту та одним із перших роз'яснив особливості обробки персональних даних відповідно до Регламенту під час пандемії [58]. Стратегія Брекзіту в тому числі стосувалась захисту персональних даних та переходу від Регламенту до локального законодавства Великої Британії та ролі британського наглядового органу в ньому. Деякі наглядові органи мали власні розроблені стратегії Брекзіту в контексті захисту персональних даних. Важливим було те, щоб після Брекзіту британський наглядовий орган міг надалі надавати належний захист персональним даним в контексті транскордонної обробки та здійснювати належний нагляд [59, с. 16-20]. Після виходу Великої Британії з Європейського Союзу, британський наглядовий орган не припинив своє існування і далі здійснює свої повноваження з нагляду за захистом персональних даних, володіє повноваженнями з розслідування, виправними повноваженнями та консультаційними. Відтепер у Великій Британії діє власний регулятор, який по-факту є збереженою версією Регламенту Європейського Союзу (англ. *UK-GDPR*) [60], а британський наглядовий орган вже видав інструкцію щодо того, як діє законодавство в сфері захисту персональних даних після Брекзіту [61].

2.2 Повноваження Європейської ради із захисту даних та Європейського інспектора із захисту даних

Відповідно до положень Регламенту, у Європейському Союзі діє Рада, а також Інспектор. У цьому підрозділі ми з'ясуємо, яка їхня роль в сфері нагляду за захистом персональних даних та як вони взаємодіють між собою.

Рада є незалежним органом у Європейському Союзі, який працює в сфері послідовного застосування положень Регламенту у Європейському Союзі, а також співпраці між наглядовими органами Європейського Союзу. Рада прийшла на заміну Робочій групі захисту фізичних осіб у зв'язку із обробкою персональних даних (англ. *Working Party on the Protection of Individuals with regard to the Processing of Personal Data*), яку частіше називають Робочою групою статті 29 (англ. *Article 29 Working Party, Art. 29 WP*) (далі «Робоча група») [62]. Ця Робоча група була створена відповідно до Директиви та проіснувала з 1996 року до 2018 року, коли Регламент набрав чинності. Основні функції цієї Робочої групи також були дорадчими. Після прийняття Регламенту у 2016 році та до набрання ним чинності у 2018 році та до створення Ради Робоча група здійснювала в тому числі тлумачення застосування Регламенту [63].

Діяльність Ради врегульована у Розділі 7 Регламенту, який визначає питання співпраці та послідовності наглядових органів у застосуванні Регламенту. Створення, повноваження та діяльність Європейської ради із захисту персональних даних визначені у статтях 68-76 [19].

Відповідно до статті 68, Рада складається із голів наглядових органів держав-членів та Інспектора або їхніх представників. У зустрічах Ради також може брати участь і Європейська комісія [19].

Основні завдання Ради визначені у статті 70 Регламенту, які окрім вже зазначених завдань нагляду та забезпечення належного застосування Регламенту, в основному складаються із консультативних та дорадчих завдань [19]. Завдання Ради можна згрупувати наступним чином: забезпечення загального інструктажу для тлумачення і просування загального розуміння

законодавства у сфері захисту персональних даних в Європейському Союзі; підготовка висновків для Європейської комісії з питань захисту персональних даних та модернізації наявного законодавства, а також для наглядових органів з метою забезпечення послідовності в питаннях транскордонної обробки персональних даних; прийняття обов'язкових до виконання рішень з метою вирішення спорів між наглядовими органами; просування та підтримка співпраці між наглядовими органами [64].

Очолює Раду Голова Ради, а здійснює аналітичне, адміністративне логістичне забезпечення діяльності Ради її Секретаріат, який надається Інспектором. Важливо, що Регламент розмежовує діяльність персоналу Секретаріату, який забезпечує діяльність Ради та персоналу, який забезпечує діяльність Інспектора.

Процедура голосування у Раді передбачає, що Європейська комісія разом із представниками наглядових органів Ісландії, Ліхтенштейну та Норвегії беруть участь у засіданнях без права голосу [64], на відміну від представників наглядових органів інших держав. Інспектор володіє особливим правом голосу, яке передбачає голосування з тих питань, що стосується застосування принципів та правил до установ Європейського Союзу, його органів, офісів та агентств (частина 6 стаття 68) [19].

За результатами своєї діяльності Рада щорічно готує звіт. У звіті висвітлюється діяльність Ради за рік, прийнятті документи, статистика по наглядових органах у державах-членах, інформація про консультації із заінтересованими особами та основні завдання на наступний рік. У звіті своєї діяльності за 2018 рік, Рада схвалила 16 інструкцій, які були раніше прийняті Робочою групою та розробила ще чотири [65, с. 10]. У звіті за 2019 рік зазначено, що Рада прийняла 5 нових інструкцій [66, с. 12]. Наразі звітів щодо діяльності Ради за 2020 рік ще немає, вони мають бути опубліковані у другій половині травня 2021 року.

Результати роботи Ради можна також оцінити у Звіті. Відповідно до Звіту Європейської комісії, хоч інструкції Ради і визнаються та приймаються

заінтересованими особами, між інструкціями наглядових органів та Ради відсутня послідовність, є потреба в більшій кількості практичних порад та конкретних прикладів, а також потреба в належному забезпеченні ресурсами наглядових органів. Серед пропозицій у Звіті для покращення роботи Ради були, наприклад, заохочення до використання усіх доступних інструментів за Регламентом, підтримка гармонізації застосування Регламенту, встановлення співпраці між наглядовими органами для проведення спільних розслідувань. Також Раді пропонують більше співпрацювати і консультуватись із заінтересованими особами, приймати більш практичні та прості для розуміння інструкції та роз'яснення [53].

Інспектор здійснює свої функції як наглядовий орган щодо установ Європейського Союзу, тобто здійснює моніторинг їхньої діяльності щодо обробки персональних даних [67]. У своїй діяльності Інспектор керується не тільки Регламентом, але й Регламентом (EU) 2018/1725 Європейського Парламенту та Ради щодо захисту фізичних осіб в контексті обробки персональних даних установами Європейського Союзу, органами, офісами та агентствами і щодо вільного руху таких даних від 23 жовтня 2018 року [68].

Основними завданнями Інспектора є: нагляд за обробкою персональних даних установами Європейського Союзу; консультування цих установ з питань обробки персональних даних; моніторинг нових технологій, що можуть впливати на обробку персональних даних; втручання перед Європейським судом справедливості для надання експертної оцінки та тлумачення законів; співпраця з іншими наглядовими органами для просування послідовності [69]. В межах цих завдань Інспектор може видавати висновки, інструкції, коментарі тощо установам Європейського Союзу, видавати розпорядження про приведення роботи установ у відповідність із законодавством, забороняти чи обмежувати обробку персональних даних, накладати адміністративні штрафи [70].

З 2019 року Інспектором є Войцех В'євйуровскі (пол. *Wojciech Wiewiórowski*) [71], його робота забезпечується Секретаріатом, куди входять юристи, ІТ-спеціалісти та адміністративний персонал [69]. На початку

перебування на посаді Інспектора, приймається стратегія на наступні п’ять років (термін перебування на посаді). Щороку Інспектор видає звіт за результатами своєї роботи, де аналізує базові KPI (англ. *key performance indicators*), основні досягнення та виклики минулого року, забезпечення цифрових прав, нагляд за установами Європейського Союзу, міжнародну співпрацю, тощо [72]. Зокрема, за 2020 рік Інспектор видав 65 офіційних та неофіційних висновків, а також кілька десятків інструкцій, в тому числі і як член Ради [72, с. 66].

Роботі Інспектора в Раді присвячений окремий розділ у звіті. Між Радою та Інспектором укладений Меморандум про взаєморозуміння (англ. *Memorandum of understanding*) (далі «Меморандум»), який визначає засади співпраці між цими органами. Зокрема, у Меморандумі визначенні основні принципи співпраці між органами, завдання Секретаріату, його організація, забезпечення конфіденційності, обов’язок Інспектора надати Секретаріат Раді та умови, на яких це здійснюється [73]. У звіті за 2020 рік Інспектор зазначає основні моменти співпраці із Радою, окрім надання Секретаріату, як от розробка та прийняття висновків з питань захисту персональних даних, зокрема, щодо договірних положень у договорах між контролерами та операторами, прийняття першого рішення Ради щодо наглядового органу на основні статті 65 Регламенту, а саме щодо Ірландського наглядового органу і його рішення щодо Твіттеру (англ. *Twitter International Company*) [72, с. 66].

Відтак, Рада та Інспектор здійснюють свої функції на наднаціональному рівні. Функції Ради є в основному консультативними, передбачають моніторинг необхідних оновлень до законодавства, надання роз’яснень тощо, за винятком повноваження розглядати спори між наглядовими органами. Натомість, Інспектор здійснює схожу до національних наглядових органів діяльність за винятком того, що він це здійснює щодо установ Європейського Союзу, а також тісно співпрацює з Радою, зокрема при підготовці висновків, роз’яснень, інструкцій тощо.

Висновки до Розділу 2

Підсумовуючи викладене в цьому Розділі, можна зробити наступні висновки щодо діяльності публічних органів у Європейському Союзі.

Основними суб'єктами виступають наглядові органи держав-членів, Рада та Інспектор. Наглядові органи здійснюють повноваження у сфері розслідування, застосування виправних заходів, надання дозволів та консультацій і в основному здійснюють нагляд за діяльністю контролерів та операторів на території держави-члена наглядового органу. Інспектор також здійснює функції із розслідування, надання дозволів та консультації, застосування виправних заходів, але робить він це щодо установ Європейського Союзу.

Рада в основному займається підготовкою висновків, рекомендацій та переглядом профільного законодавства та розв'язанням конфліктів між наглядовими органами держав. Рада тісно співпрацює із Інспектором, який не тільки надає у її розпорядження Секретаріат, але й бере участь у підготовці документів тощо, особливо в контексті тих питань, що стосуються повноважень Інспектора.

З основних проблем наявної в Європейському Союзі системи виділяють відсутність послідовності між висновками, роз'ясненнями та іншою діяльністю наглядових органів держав-членів, а також між Радою та наглядовими органами, брак ресурсів для належного виконання своїх функцій, складнощі у імплементації механізмів Регламенту контролерами та операторами.

Відтак, основним фокусом діяльності Ради наразі залишається просування співпраці між наглядовими органами, використання ними всіх доступних відповідно до Регламенту інструментів, розробка доступних для контролерів та операторів роз'яснень та інструкцій і перегляд наявних з цією ж метою, співпраця із заінтересованими особами.

Варто також звернути увагу, що з прийняттям Регламенту зросла ефективність у діяльності наглядових органів держав-членів, про що свідчить, зокрема, ріст кількості переглянути за рік скарг та застосованих

адміністративних штрафів до порушників. В порівнянні з Директивою, у діях наглядових органів присутня більша послідовність у застосуванні Регламенту.

З протилежної сторони, Регламент чинний всього лиш три роки, тому зробити суттєвих висновків щодо змін у системі діяльності публічних органів поки неможливо, попри попередні позитивні результати. Варто також звернути увагу, що хоч ситуація із послідовністю та співпрацею між наглядовими органами, а також обізнаність серед зацікавлених сторін є значно вищою, ніж при Директиві, зазначені сфери й надалі потребують роботи. Як зазначали наявні звіти, у цьому напрямку й надалі виникають труднощі, хоч позитивні зрушення і прослідковуються.

РОЗДІЛ 3. ДІЯЛЬНІСТЬ ПУБЛІЧНИХ ОРГАНІВ У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У США

США є федерацією, відтак закони приймаються як на федеральному рівні Конгресом, так і на рівні федеративних одиниць (штатів) місцевими законодавчими органами. Враховуючи такий державний устрій США, а також відсутність уніфікованого законодавства у сфері захисту персональних даних, про що було зазначено раніше у Розділі 1 цієї роботи, ми розглянемо діяльність публічних органів у сфері захисту персональних даних (**3.1**) на федеральному рівні та (**3.2**) на рівні штатів.

3.1 Діяльність публічних органів у сфері захисту персональних даних на федеральному рівні

У США на федеральному рівні відсутнє уніфіковане законодавство у сфері захисту персональних даних, а відтак і немає акту, на підставі якого діє конкретний орган чи система органів у сфері захисту персональних даних, і який розмежовує повноваження у сфері захисту персональних даних між цими органами.

Найбільш наближеним до здійснення функцій у сфері захисту персональних даних на федеральному рівні є Федеральна торгова комісія (англ. *Federal Trade Commission, FTC*). Федеральна торгова комісія була заснована у 1914 році на підставі Закону про Федеральну торгову комісію (англ. *Federal Trade Commission Act*) [74].

Федеральна торгова комісія частково є своєрідним аналогом Антимонопольного комітету в Україні, тобто здійснює свою діяльність як публічний орган у питаннях, які стосуються дотримання антимонопольного законодавства, а також наділена повноваженнями у сфері захисту прав споживачів (англ. *consumers*) [75]. Повноваження Федеральної торгової комісії зводяться до наступних: запобігати недобросовісній конкуренції, оманливим та

недобросовісним діям, що мають негативний вплив на торгівлю; стягувати грошову компенсацію; визначати, які саме практики є недобросовісними та оманливими; проводити розслідування щодо суб'єктів зайнятих у торгівлі; звітувати та здійснювати рекомендації щодо змін у законодавство тощо [76].

Одним із завдань Федеральної торгової комісії є захист прав споживачів. В обсяг захисту споживачів входить і захист їхньої приватності. Захист приватності споживачів, в тому числі і персональної інформації споживачів, здійснюється Федеральною торговою комісією із 1970х років після прийняття Закону про добросовісну кредитну звітність (англ. *Fair Credit Reporting Act*) [77].

Варто звернути увагу, що із формулювань, які використовуються Федеральною торговою комісією у своїх звітах, аналітиці, складно чітко встановити чи розмежовується концепція захисту приватності (англ. *privacy protection*) споживачів від захисту їхньої персональної інформації. Загалом, формулювання «захист приватності» та «захист персональної інформації» вживаються попеременно, іноді захист персональної інформації вживається як складова захисту приватності. З цього випливає, що у діяльності Федеральної торгової комісії немає чіткого розмежування захисту приватності та захисту персональних даних, як це є, наприклад, у Європейському Союзі.

Федеральна торгова комісія тривалий час займала позицію за якої надавала перевагу підходу саморегулювання у питаннях захисту приватності споживачів. Однак, оцінивши результати та ефективність цього підходу, вирішила діяти активніше у сфері захисту приватності споживачів та розпочала подавати позови проти тих компаній, що порушували політики приватності (англ. *privacy policies*) на підставі здійснення ними недобросовісних та/або оманливих дій та практик [78, с. 3]. Наприклад, якщо компанія не дотримувалась власної політики приватності, то такі дії вважались оманливими (англ. *deceptive*).

Повноваження Федеральної торгової комісії у сфері захисту персональних даних не є конкретно визначеними. Федеральна торгова комісія володіє доволі широкими повноваженнями відповідно до Розділу 5 Закону про Федеральну торгову комісію, який передбачає, що Федеральна торгова комісія може

забороняти дії, які вважаються недобросовісними або оманливими діями чи практиками, які негативно впливають на торгівлю (англ. *unfair or deceptive acts or practices in or affecting commerce*). Такі дії вважаються незаконними (параграф 45 (a) (1)) [79].

Федеральна торгова комісія може визнати недобросовісні дії або практики незаконними тільки в тому випадку, якщо вони завдають чи можуть завдати значної шкоди споживачу, які споживач не може раціональним чином уникнути та які переважають компенсаційні вигоди споживача чи конкуренції (параграф 45 (n)) [79]. Відповідно, застосовуючи таке доволі широке визначення, Федеральна торгова комісія здійснювала свої повноваження в тому числі і щодо дотримання компаніями приватності споживачів у своїй діяльності. Як зазначає Федеральна торгова комісія, в межах Розділу 5 Закону про Федеральну торгову комісію недобросовісними та оманливим діями чи практиками є й недобросовісні та оманливі дії чи практики, які стосуються використання чи захисту персональної інформації споживачів [80].

З огляду на описані вище повноваження Федеральної торгової комісії, їх можна умовно поділити на повноваження у сфері проведення розслідувань та застосування заходів для забезпечення дотримання вимог законів та інших актів (англ. *investigation and enforcement actions*) у сфері захисту персональної інформації споживачів, а також повноваження у сфері роз'яснення щодо застосування законодавства у сфері дотримання приватності споживачів, його оновлення тощо.

Федеральна торгова комісія може проводити розслідування в індивідуальному порядку щодо застосування компаніями раціональних та належних заходів безпеки для захисту персональної інформації споживачів. За наслідком проведення розслідування Федеральна торгова комісія може розпочати адміністративне чи судове провадження, якщо є підстави вважати, що мало місце порушення. В межах провадження Федеральна торгова комісія може добиватись судової заборони чи обмеження дій компанії, виплати відшкодування споживачеві тощо, цивільно-правових стягнень (параграф 45 (b),

(l)) [79]. Одразу можна помітити різницю із повноваженнями наглядових органів у Європейському Союзі, адже можливість накладати штрафи у Федеральної торгової комісії обмежена, оскільки стягнути їх можливо тільки через суд як цивільно-правове стягнення (англ. *civil penalty*).

Федеральна торгова комісія також може видавати інструкції щодо застосування того чи іншого законодавства у сфері захисту персональної інформації споживачів, а також регуляторні акти для врегулювання певних сфер приватності споживачів та їхнього захисту [81, с. 11, 16]. Федеральна торгова комісія проводить аналіз чинного законодавства та готує звіти по ключових питаннях [82].

Зазначені повноваження сформульовані доволі розмито, адже відсутнє чітке розуміння, які саме завдання має виконувати Федеральна торгова комісія в контексті захисту приватності споживачів. Повноваження в зазначеному напрямку не є конкретно визначеними і в цілому витікають із загального повноваження, визначеного у Розділі 5 Закону про Федеральну торгову комісію.

Федеральна торгова комісія забезпечує примусове виконання регламентів у тих сферах діяльності, щодо яких у Федеральної торгової комісії є юрисдикція (телемаркетинг, комерційні повідомлення (спам), приватність дітей), а також застосовувати засоби впливу для захисту приватності споживачів [83]. Тобто, зазначена діяльність здійснюється в межах тих актів, щодо яких Федеральна торгова комісія виступає як наглядовий орган. Федеральна торгова комісія може притягувати до відповідальності за недобросовісні та оманливі дії та практики, що порушують приватність споживачів, а також забезпечувати виконання спеціальних законів, які захищають конкретно визначений вид інформації про споживача, як фінансова інформація, інформація про стан здоров’я, інформація про дітей тощо [84, с. 2].

У своєму щорічному звіті щодо діяльності у сфері приватності та захисту даних за 2019 рік (англ. *Privacy and Data Security Update: 2019*), Федеральна торгова комісія зазначила, що за звітний рік були розпочаті провадження із ряду питань щодо забезпечення приватності у різних індустріях, в тому числі у

соціальних мережах, рекламних технологіях, екосистемі мобільних додатків. Загальна кількість таких справ складає більше 130 справ щодо спаму та шпигунського програмного забезпечення та більше 80 позовів із загальних питань забезпечення приватності [85, с. 2]. На жаль, у звіті не наводиться інформація щодо загальної кількості скарг, які надходять від споживачів, що ускладнює можливість проаналізувати, співвідношення цих скарг до відкритих проваджень.

Серед основних справ Федеральної торгової комісії можна виділити врегулювання конфлікту із Facebook. Компанія мала сплатити 5 мільярдів доларів штрафу за порушення пов'язані із спотворенням інформації щодо контролю, яким користувачі володіють щодо своєї персональної інформації, неспроможністю забезпечити належну програму для захисту приватності користувачів. Зазначена сума штрафу була найбільшою за всю історію Федеральної торгової комісії [85, с. 2].

Ще однією яскравою справою є справа Cambridge Analytica. Як відомо, ця компанія здійснює діяльність в сфері аналітики даних і під час президентських виборів в США працювала з командою Дональда Трампа для здійснення профайлінгу та впливу на виборців [86]. Федеральна торгова комісія подала позов проти Cambridge Analytica та ще двох інших схожих компаній на підставі використання оманливих тактик. Ці тактики використовувались компанією для збору (англ. *harvesting*) даних користувачів у Facebook для подальшого профайлінгу виборців та тарґетування [85, с. 3].

Федеральна торгова комісія також зазначає, що з 2002 по 2019 роки їй вдалось розпочати більше 70 справи проти компаній у зв'язку із неналежним захистом персональних даних споживачів. Усі справи, які були наведені у звіті за 2019 рік щодо порушення режиму захисту персональних даних користувачів, були врегульовані [85, с. 5]. Загалом, багато проваджень, які відкриваються Федеральною торговою комісією, врегульовуються між сторонами без прийняття остаточного рішення по справі судом.

Федеральна торгова комісія може забезпечувати дотримання захисту

персональної інформації споживачів у межах спеціальних федеральних законів [87]. Наприклад, здійснювати нагляд за дотриманням вимог CAN-SPAM Act. Цей закон, як було зазначено у Розділі 1, врегульовує питання розсилки повідомлень комерційного змісту без погодження із отримувачем, що в тому числі охоплює збирання та використання емейлів для розсилки спаму. Федеральна торгова комісія забезпечує виконання положень CAN-SPAM Act компаніями, на яких цей закон поширюється, і може домагатись стягнення штрафів за невиконання положень акту [88]. Окрім цього, Федеральна торгова комісія може видавати інструкції, роз'яснення щодо застосування CAN-SPAM Act та комплаєнсу із ним, в тому числі тих, що стосуються розсилки емейлів [89].

Федеральна торгова комісія розпочинала провадження проти компаній за порушення норм інших законів, в тому числі Закону про добросовісну кредитну звітність, Гремм-Ліч-Блілі Акту, забезпечення виконання норм Закону про захист приватності дітей онлайн (англ. *Childern's Online Privacy Protection Act, COPPA*) (далі «COPPA») [84, с. 2, 3].

Наприклад, для дотримання вимог Гремм-Ліч-Блілі Акту, Федеральна торгова комісія розробила спеціальний інструмент – Правила забезпечення захисту Гремм-Ліч-Блілі (англ. *Gramm-Leach-Bliley Safeguards Rule*). Цей інструмент забезпечує просування та виконання фінансовими установами належних практик безпеки. Зокрема, фінансові установи зобов'язані вчинити певні дії для того, щоб забезпечити наявність належних заходів безпеки, які відповідають їхній господарській діяльності та інформації, яку вони збирають. Наприклад, вони мають призначити працівника, відповідального за забезпечення належного рівня безпеки та аудиту можливих ризиків у системі, які можуть негативно вплинути на безпеку інформації споживача [90, с. 54]. З 2005 року Федеральна торгова комісія відкрила близько 35 справ щодо порушення компаніями Гремм-Ліч-Блілі Акту [85, с. 7].

Загалом, Федеральна торгова комісія приділяє значну увагу захисту фінансової інформації про споживачів в межах спеціальних законів, щорічний звіт включає в себе окремий розділ щодо результатів роботи Федеральної

торгової комісії в сфері забезпечення фінансової приватності [85, с. 7].

Окрім Гремм-Ліч-Блілі Акту, Федеральна торгова комісія здійснює захист фінансової інформації споживачів також в межах інших законів, як от згаданий раніше Закон про добросовісну кредитну звітність. Зазначений закон стосується інформації, яку компанії використовують для визначення кредитоспроможності, права на страхування, можливості працевлаштування чи для перевірки орендарів. В межах зазначеного закону Федеральна торгова комісія розпочала більше ста справ проти компаній, які порушили його норми, а також стягнула близько 40 мільйонів доларів цивільно-правового стягнення [85, с. 7].

Захист приватності дітей, в тому числі їхньої персональної інформації – це ще одна група даних, захисту якої Федеральна торгова комісія приділяє особливу увагу, загалом в контексті вже згаданого закону COPPA. Одна із основних вимог COPPA – це отримання верифікованої від батьків згоди на обробку персональної інформації про дітей до 13 років [85, с. 9]. З 2000 року Федеральна торгова комісія розпочала близько 30 справ щодо порушення компаніями вимог COPPA. Зокрема, у 2019 році Федеральна торгова комісія разом із Генеральним прокурором Нью-Йорку притягнули до відповідальності Google та YouTube через збирання персональних даних про дітей без згоди батьків. Відповідно до рішення, із компаній стягнули 170 мільйонів доларів штрафу, які є рекордною сумою штрафу за порушення COPPA [85, с. 9].

Окрім притягнення компаній до відповідальності за порушення у сфері захисту персональної інформації споживачів, у 2019 році Федеральна торгова комісія також розробила ряд навчальних матеріалів та інструкцій для бізнесу. Ці матеріали стосувались питань кібербезпеки у малих компаніях, приватності та безпеки мобільних пристроїв, крадіжки особистості (англ. *identity theft*) тощо [85, с. 16, 17].

Як бачимо, повноваження Федеральної торгової комісії перетинаються із повноваженнями наглядових органів у Європейському Союзі. Це стосується повноважень щодо здійснення нагляду за дотриманням законодавства у сфері захисту персональних даних (персональної інформації в США), проведення

розслідувань, притягнення порушників до відповідальності, підготовка інструкцій та роз'яснень щодо відповідності вимогам законів у сфері захисту персональної інформації споживачів. Однак, повноваження Федеральної торгової комісії в той же час є розмити та випливають із загальних формулювань, коли ж компетенція наглядових органів у Європейському Союзі є чітко визначеною. Відмінності також полягають у здійсненні повноважень органами. По-перше, притягнення до відповідальності Федеральною торговою комісією часто здійснюється через суд або врегульовується сторонами до отримання остаточного рішення суду по справ (англ. *settlement*), те саме стосується і стягнення штрафів. По-друге, ту саму кількість справ, які були розглянуті чи вирішені з 2002 по 2019 роки Федеральною торговою комісією, наглядові органи в Європейському Союзі розглядають за рік. По-третє, Федеральна торгова комісія не є органом захисту персональної інформації споживачів, адже здійснює свої повноваження в цій сфері переважно в межах Розділу 5 Закону про Федеральну торгову комісію як захист споживачів від недобросовісних та оманливих дій чи практик.

Відсутність уніфікованого законодавства та доволі широкі повноваження Федеральної торгової комісії мають свій негативний вплив на захист персональної інформації у США. Зокрема, деякі компанії оспорювали повноваження Федеральної торгової комісії щодо розслідування питань, які стосуються порушення режиму захисту персональної інформації споживачів, наприклад як це було у справі Федеральної торгової компанії проти компанії Вайндхам (англ. *Federal Trade Commisson v Wyndham Worldwide Corp.*) .) [78, с. 8-10]. І, хоч суд відкинув контраргументи відповідача та відмовив у клопотанні про відхилення позову через брак повноважень Федеральної торгової комісії, що потім підтримав в федеральний апеляційний суд [91], це не вирішило питання наскільки доцільно врегульовувати захист приватності споживачів в межах заборони недобросовісних та оманливих дій та практик відповідно до Розділу 5 Закону про Федеральну торгову комісію.

Окрім Федеральної торгової комісії інші федеральні органи також

здійснюють повноваження щодо забезпечення відповідності вимогам федерального законодавства в межах своєї юрисдикції, однак це в більшості стосується конкретних видів інформації, як от фінансова інформація, інформація про стан здоров'я [83].

Наприклад, за дотримання HIPPA, закону, який врегульовує захист медичної звітності та особистих медичних даних пацієнтів, здійснює нагляд Офіс цивільних прав Міністерства охорони здоров'я та соціальних служб США [92]. Офіс забезпечує виконання Правил приватності та безпеки (англ. *Privacy and Security Rules*) HIPPA через проведення розслідувань поданих скарг, проведення аудиту з комплаєнсу компаній із вимогами Правил приватності та безпеки, проведення навчань для забезпечення комплаєнсу [93].

Наявна система, за якою Федеральна торгова комісія наділена повноваженнями здійснювати нагляд за дотриманням прав споживачів в сфері захисту їхньої приватності та персональної інформації не є досконалою та піддається критиці. Основна критика спрямована на те, що Федеральна торгова комісія не може ефективно забезпечити виконання власних наказів та накладати штрафи у випадку порушень, не розглядає скарги споживачів про недобросовісні та оманливі практики при зборі персональної інформації, трекінгу, профайлінгу, розкритті інформації третім особам. Стверджувана бездіяльність Федеральної торгової комісії призвела до збільшення проблем у сфері приватності, в тому числі трекінгу через кукі-файли, масовому спостереженні за фізичними особами та групами через перехресні пристрої [94].

США лишається однією з небагатьох держав, де немає єдиного органу відповідального за захист персональних даних та уніфікованого законодавства у цій сфері [94; 95]. Для того, щоб виправити ситуацію та покращити захист персональних даних у США пропонується розробити відповідне законодавство на основі вже існуючих у світі регуляторів як Регламент і з врахуванням сучасних технологій [95]. Також пропонується створити відповідний окремий від Федеральної торгової комісії, який би здійснював належний захист, зокрема, через забезпечення справедливості, відповідальності та прозорості, забезпечення

справедливих положень договорів, просування методів підвищення захисту приватності (англ. *privacy enhancing techniques*), забезпечення публічною інформацією щодо питань, які стосуються захисту персональних даних [94].

У 2020 році вже відбувались обговорення запропонованих текстів законопроєктів у сфері приватності та захисту персональних даних. Зазначені проєкти передбачали створення окремого наглядового органу (англ. *data protection authority, DPA*), значним чином концентрувались на зборі інформації технологічними компаніями або встановлювали обмеження щодо збору персональної інформації. Однак, ці проєкти не є досконалими, оскільки не встановлюють переважаючої сили федерального закону над законодавством штатів у сфері захисту персональних даних, що в свою чергу робить законодавство в цій сфері нечітким. Проєкти не акцентують на зборі інформації іншими суб'єктами крім технологічних компаній, як от лікарні, роздрібна торгівля, державні установи. Для розробки належного законодавства, який враховуватиме інтереси всіх сторін, бізнесу, технологічного розвитку та потреб фізичних осіб, законодавчим органам та бізнесу необхідно вступити у відкрите обговорення [96].

Відтак, на федеральному рівні захист персональної інформації в США відрізняється від моделі Європейського Союзу через наявність великої кількості актів, які тільки частково врегульовують питання приватності, та відсутньої єдиної системи нагляду, адже основна діяльність уповноважених на це органів не пов'язана із захистом приватності чи персональних даних. Також, наявна система не є злагодженим механізмом та піддається значній критиці і потребує змін через наразі неможливість ефективно забезпечувати захист персональної інформації, розглядати скарги та накладати штрафи на компанії, які порушують відповідне законодавство. Компаніям в свою чергу складно забезпечувати комплаєнс через відсутність достатніх інструкцій та роз'яснень, а саме законодавство не враховує як використовуються сучасні технології при зборі інформації від осіб.

3.2 Діяльність публічних органів у сфері захисту персональних даних на рівні штатів

На рівні штатів повноваження щодо дотримання прав споживачів у сфері захисту персональної інформації зазвичай належать до повноважень генеральних прокурорів штатів (англ. *State's Attorney General*) [83]. Наприклад, у штаті Міннесота, де існує кілька законів у сфері захисту персональної інформації, притягує до відповідальності за порушення законодавств у цій сфері Генеральний прокурор штату [97].

Схожа ситуація існує в Массачусетсі. У Розділі 1 ми також згадували про спеціальний закон в сфері захисту персональної інформації 201 CMR 17.00, який діє у Массачусетсі. Регуляторним органом є Офіс у справах споживачів та врегулюванні бізнесу (англ. *Office of Consumer Affairs and Business Regulation*) [98]. Однак, притягнення до відповідальності за порушення в сфері приватності та захисту персональної інформації здійснює Генеральний прокурор штату Массачусетс (стаття 6) [99].

На жаль, аналізу діяльності публічних органів у сфері захисту персональної інформації споживачів не наділена належна увага. Більшість матеріалів аналізують відносно новий CCPA, який діє у Каліфорнії з січня 2020 року, але оминають увагою наявні системи захисту в інших штатах. Те саме стосується й самих публічних органів штатів, адже офіси генеральних прокурорів штатів, законодавчих органів чи інших публічних органів не надають інформації щодо відповідальних за захист у сфері персональної інформації органів чи їхніх повноважень, окрім як можливості звернутись до офісу генерального прокурора зі скаргою. Це може свідчити про те, що у штатах відсутні органи, які займаються конкретно наглядом у сфері захисту персональної інформації, а самому захисту персональної інформації не надається відмінного значення від захисту інших прав фізичних осіб.

Як відомо, перший загальний уніфікований закон, спрямований на захист персональної інформації споживачів у США був прийнятий в Каліфорнії у 2018

році та набрав чинності у 2020 року, CCPA. У Каліфорнії нагляд за дотриманням CCPA наразі здійснює Генеральний прокурор штату Каліфорнія. Зокрема, відповідно до норм CCPA, Генеральний прокурор може надавати консультації бізнесу щодо комплаєнсу із CCPA (стаття 1798.155 (a)) [30], накладати цивільно-правові штрафи в сумі від 2 500 до 7 500 доларів (в залежності від характеру порушення) (стаття 1798.155 (b)) [30]. Накладення цивільно-правових штрафів, як і у випадку із Федеральною торговою комісією [100], здійснюється у судовому порядку. Генеральний прокурор штату Каліфорнія подає позов від імені жителів штату Каліфорнія (англ. *in the name of people of the State of California*) до суду для накладення штрафу на порушників CCPA (стаття 1798.155 (b)) [30]. Генеральний прокурор також уповноважений приймати регламенти, інструкції, процедури, переглядати їх для забезпечення належного виконання CCPA, як от надавати визначення певним термінам, приводити у відповідність CCPA із правом штату та федеральним законодавством, встановлювати процедури для забезпечення подання суб'єкти інформації, яку вони зобов'язані надати відповідно до CCPA, встановлювати процедури для забезпечення споживачам можливості користуватись своїми правами відповідно до CCPA тощо (стаття 1798.185 (b)) [30].

Генеральний прокурор Каліфорнії перед набранням чинності CCPA проводив зустрічі із заінтересованими особами, перед тим як узгоджувати фінальні тексти регламентів до CCPA [101]. Генеральний прокурор розробив та прийняв ряд регуляторних актів, останній з яких у березні 2021 року врегульовував можливість споживачів відкликати свою згоду на обробку персональної інформації (англ. *opt-out*) і забороняє так звані «темні патерни» (англ. *dark patterns*), які затримують цей процес [102]. Загалом, робота Генерального прокурора на цій ниві сприймається позитивно [103] і не піддається такій критиці, як робота Федеральної торгової комісії.

У 2020 році був прийнятий Закон Каліфорнії про права на приватність (англ. *California Privacy Rights Act, CPRA*) (далі «CPRA»), який передбачає створення окремого органу, що має здійснювати нагляд за дотриманням CCPA.

Таким органом має бути Агентство із захисту приватності Каліфорнії (англ. *California Privacy Protection Agency, CPPA*) (далі «CPPA»). Закон був прийнятий у листопаді 2020 року і набирає чинності 1 липня 2023 року [104]. Здійснювати свою діяльність CPPA почне через шість місяців після набрання чинності CPRA, тобто вже у 2024 році [105].

До CPPA перейдуть усі адміністративні та інші повноваження, а також юрисдикція щодо застосування та забезпечення виконання CCPA. CPPA управлятиметься радою із п'яти членів, де голову та одного члена призначає Губернатор, ще по одному члену призначає Генеральний прокурор, Комітет Сенату з процедурних питань (англ. *Senate Rules Committee*) та Спікер Законодавчих зборів (англ. *Speaker of the Assembly*) (стаття 1798.199.10) [30]. У березні 2021 року вже були оголошені члени ради CPPA [106].

CPPA також здійснюватиме повноваження, спрямовані на збільшення обізнаності та розуміння громадськості щодо питань, які стосуються захисту персональної інформації, надавати інструкції користувачам щодо їхніх прав та компаніям щодо їхніх обов'язків та відповідальності за законом, слідкувати за розвитком у сфері захисту персональної інформації (стаття 1798.199.40 (d)(e)(f)(h)) [30]. Незважаючи на те, що до CPPA перейде значна кількість повноважень, Генеральний прокурор надалі матиме повноваження направляти до суду справи щодо примусового виконання положень CCPA [102; 106].

Отже, Каліфорнія пішла за моделлю Європейського Союзу та призначила окремий орган, що безпосередньо здійснюватиме тільки нагляд за законодавством у сфері захисту персональної інформації, чиї повноваження стосуватимуться як розслідування випадків порушень, так і надання роз'яснень, видачі інструкцій із застосування законодавства та комплаєнсу тощо.

Висновки до Розділу 3

Підсумовуючи викладене у Розділі 3, можна зробити наступні висновки.

По-перше, діяльність публічних органів у США в сфері захисту

персональної інформації не є достатньо дослідженим предметом. Більшість матеріалів зводяться до аналізу роботи Федеральної торгової комісії як органу на федеральному рівні. Щодо діяльності на рівні штатів, то найчастіше описується система, яка відносно віднедавна наявна у Каліфорнії.

По-друге, діяльність Федеральної торгової комісії однозначно відрізняється від діяльності наглядових органів у Європейському Союзі, адже це не є спеціальний орган нагляду, її повноваження не є чітко визначеними, а обсяг роботи, який здійснюється, є значно нижчим у порівнянні, що безпосередньо впливає на ефективність захисту споживачів та їхньої персональної інформації. Відповідно, це призводить до критики через неможливість забезпечити належний рівень захисту споживачів та поновлення порушених прав. Відтак, наявна система потребує змін, першочергово – прийняття уніфікованого законодавства у сфері захисту персональної інформації та створення єдиного незалежного органу.

По-третє, діяльність публічних органів на рівні штатів є малодослідженою і єдині висновки, які наразі можна зробити, базуються в основному на тому, як діяльність публічних органів організована в Каліфорнії через наявність профільного законодавства. Однак, тут важливо зауважити, що хоч Каліфорнія є одним із перших штатів, де має діяти окремий орган нагляду за дотриманням законодавства у сфері захисту персональних даних, зробити суттєві висновки поки складно, через відсутність звітів чи іншої розгорнутої інформації про кількість розглянутих скарг на порушення законодавства у цій сфері, основні недоліки нового CCPA, що були виявлені за півтора року з часу набрання ним чинності тощо.

По-четверте, через виявлені недоліки як от неактуальне законодавство, низька ефективність захисту, відсутність єдиного наглядового органу та єдиних стандартів захисту персональної інформації, наявна наразі система в США не може слугувати належним прикладом, на чиїй основі можна будувати нагляд за законодавством у сфері захисту персональних даних. В той же час, ця система може бути прикладом того, яких помилок варто уникати щоб забезпечити

належний рівень захисту персональних даних. Поки що США перебувають на стадії обговорення модернізації законодавства. Штат є більш активними в цьому напрямку, оскільки після прийняття CCPA в Каліфорнії запустилась певна ланцюгова реакція в інших штатах, які почали активно розробляти власне законодавство і приймати його, як це є зараз у Нью-Йорку, наприклад. На федеральному рівні проведення реформи законодавства у сфері захисту персональної інформації поки що буксує та не перетнуло стадії обговорення проєктів реформи.

РОЗДІЛ 4. ДІЯЛЬНІСТЬ ПУБЛІЧНИХ ОРГАНІВ У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ. ОСНОВНІ ПРОБЛЕМИ У ЗАБЕЗПЕЧЕННІ ДОТРИМАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ТА ШЛЯХИ ВИРІШЕННЯ.

В Україні основним законом, який регулює відносини у сфері захисту персональних даних є Закон України «Про захист персональних даних». Після набрання чинності Законом нагляд за його дотриманням здійснювала Державна служба України з питань захисту персональних даних (далі «ДСЗПД»). З 2014 року після внесення змін у Закон, нагляд почав здійснювати Уповноважений Верховної Ради України з прав людини (далі «Уповноважений»).

У зв'язку із підписаннями Угоди про асоціацію з Європейським Союзом у 2014 році, Україна взяла на себе ряд зобов'язань щодо наближення власного законодавства до стандартів Європейського Союзу. Угода про асоціацію в тому числі передбачає «*забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема відповідних документів Ради Європи*» (стаття 15) [107]. Як вже згадувалось у попередніх розділах, українське законодавство в сфері захисту персональних даних в основному базується на Директиві, яка втратила свою чинність, адже з 2018 року у Європейському Союзі діє Регламент. Відповідно, Україна повинна наблизити своє законодавство у сфері захисту персональних даних до законодавства Європейського Союзу, в тому числі і щодо питань діяльності публічних органів у сфері забезпечення захисту персональних даних. Наразі, відповідні зміни не були прийняті, а наявна система нагляду піддається критиці через неефективність та невідповідність європейським стандартам.

Відповідно, в межах цього Розділу ми проаналізуємо (**4.1**) діяльність ДСЗПД та (**4.2**) діяльність Уповноваженого, а також (**4.3**) основні проблеми, які виникають у діяльності публічних органів щодо забезпечення виконання норм Закону та шляхи їх подолання.

4.1 Діяльність Державної служби України з питань захисту персональних даних

Закон був прийнятий 1 червня 2010 року і перша редакція передбачала створення уповноваженого державного органу з питань захисту персональних даних, який би здійснював контроль за додержанням законодавства (стаття 22) [108]. Відповідно до першої редакції Закону, уповноважений орган мав бути центральним органом виконавчої влади (стаття 23) [108]. Цей уповноважений орган мав здійснювати завдання, серед яких були контроль за додержанням Закону, реалізація державної політики в сфері захисту персональних даних, реєстрація баз персональних даних та введення Державного реєстру персональних даних (реєстрація баз персональний даних та реєстр були скасовані з 1 січня 2014 року) [109], видача приписів про усунення порушень, розгляд скарг та пропозицій, запитів, звернень тощо (стаття 23) [108].

На виконання вимог Закону, 9 грудня 2010 року був виданий Указ Президента України «Про оптимізацію системи центральних органів виконавчої влади», у якому було постановлено утворити ДСЗПД (пункт 1) [110]. У квітні 2011 року був прийнятий Указ Президента України, яким було затверджено Положення про Державну службу України з питань захисту персональних даних» (далі «Положення») [111], де були затверджені основні завдання, які покладають на ДСЗПД та повноваження, на основі вже закріплених у Законі. Серед повноваження ДСЗПД, можна виділити наступні групи.

Перша – це повноваження у сфері ведення претензійної роботи та перевірок: ДСЗПД розглядала запити, звернення, пропозиції та скарги (пункт 4 (10)) [111], проводила перевірки (пункт 4 (14)) [111], видавала обов'язкові до виконання приписи щодо усунення порушень (пункт 4 (15)) [111], складала адміністративні протоколи про порушення (пункт 4 (16)) [111]. До другої групи можна віднести повноваження, які стосувались введення реєстру баз даних, реєстрація баз даних, видача документів про реєстрацію баз даних (пункт 4 (7-9), (11)) [111].

Третю велику групу складають повноваження консультативного, дорадчого характеру. Зокрема, ДСЗПД узагальнювала практику у сфері захисту персональних даних (пункт 4 (1)) [111], розробка методичних матеріалів, рекомендацій (пункт 4 (4)) [111], типових порядків обробки персональних даних (пункт 4 (5)) [111], підготовка пропозицій, розробка критерії (пункт 4(2),(3)) [111], проводить навчальну, наукову та дослідницьку роботу у сфері захисту персональних даних (пункт 4 (23-25)) [111].

Велика група повноважень ДСЗПД також стосувалась співробітництва з правоохоронними органами (пункт 4(17)) [111], та міжнародного співробітництва, участі у розробці міжнародних договорів тощо (пункт 4 (19-21)) [111].

Якщо проводити паралелі із повноваженнями наглядових органів Європейського Союзу, то можна зробити висновок, що повноваження ДСЗПД є схожими із повноваженнями наглядових органів, зокрема в контексті проведення перевірок та притягнення до відповідальності, а також консультаційної роботи. Однак, не можна стверджувати, що вони є повністю тотожними, адже Положення чітко не розкриває можливості ДСЗПД стягувати штрафи, розслідувати порушення захисту персональних даних та передавати справи до суду.

Ще однією великою відмінністю є те, що ДСЗПД не відповідало європейським стандартам незалежності. Зокрема, голова ДСЗПД був підзвітний Міністру юстиції (пункт 9 (6)) [111], а формування штату та призначення, звільнення керівників та їх заступників відбувалось за погодженням із Міністром юстиції (пункт 9 (13), 12) [111]. Міністр юстиції також погоджував річний план діяльності ДСЗПД (пункт 9 (5)) [111]. Така підзвітність та можливість Міністра юстиції втручатись в кадрові питання ДСЗПД не відповідає проаналізованим у Розділі 2 вимогам незалежності наглядового органу, адже Міністерство юстиції, як і інші органи влади також можуть виступати володільцями або розпорядниками інформації та підлягають перевірці.

Як зазначає Гнатюк С.Л.: «*інституційна організація системи захисту ПД*

в Україні стала предметом найбільш інтенсивних консультацій з ЄК та Євроюстом» [112, с. 44]. Зокрема, Гнатюк С.Л. з посиланням на Лист представництва України при Європейському Союзі «Щодо актуальних питань захисту персональних даних» зазначає, що Євроюст та Європейська Комісія закликали до забезпечення незалежності ДСЗПД і зазначили, що наявність ДСЗПД у системі органів виконавчої влади: «*не надає достатніх гарантій інституційної незалежності цього органу, оскільки за такої моделі зберігається високий ризик зовнішнього тиску та політичного впливу*» [112, с. 44]. Як можливий вихід із ситуації та забезпечення незалежності органу був запропонований варіант переведення уповноваженого органу у сфері захисту персональних даних під юрисдикцію Верховної Ради України [112, с. 44-45].

Однак, незважаючи на питання, які виникали щодо незалежності ДСЗПД, діяльність органу в цілому вважали задовільною, та навіть успішною та фаховою [113], відзначали співпрацю із міжнародними органами, особливо органами Європейського Союзу [113].

Відтак, хоч в Україні, на відміну від США, після прийняття Закону був створений єдиний орган для здійснення нагляду та контролю за дотриманням законодавства у сфері захисту персональних даних, місце органу у системі органів влади та його організація не зовсім відповідали вимогам незалежності, що викликало стурбованість зі сторони Європейського Союзу, а також створювало для України проблему реформування системи та приведення її у відповідність. Варто також зазначити, що з часів існування ДСЗПД не зберіглась інформація про ефективність роботи органу, як от розгляд скарг та кількість відкритих проваджень, що ускладнює можливість проаналізувати безпосередньо ефективність діяльності ДСЗПД у 2011-2013 роках.

4.2. Діяльність Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних

У липні 2013 року був прийнятий Закон України «Про внесення змін до

деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» (далі «Закон про внесення змін»), що набув чинності 1 січня 2014 року [114]. Зміни скасовували обов'язкову реєстрація баз персональних даних та відповідний реєстр, а також повноваження у сфері нагляду та контролю за дотриманням захисту персональних даних передавалось до Уповноваженого (пункт 7, 15 частини I (2)) [114]. Відповідно до Постанови Кабінету Міністрів України від 10 вересня 2014 року «Про оптимізацію системи центральних органів виконавчої влади» було ліквідовано ДСЗПД (пункт 2) [115].

Відповідно до чинної редакції Закону від 23 квітня 2021 року, контроль за додержанням законодавства у сфері захисту персональних даних покладений на Уповноваженого та суди (стаття 22) [18]. У попередній редакції ці повноваження належали окрім ДСЗПД ще іншим органам державної влади та місцевого самоврядування. Змінились і повноваження Уповноваженого в порівнянні із ДСЗПД відповідно до Закону. Зокрема, у Законі чітко вказані повноваження Уповноваженого затверджувати нормативно-правові акти в сфері захисту персональних даних (пункт 4 частини 1 статті 23) [18], надавати рекомендації щодо застосування законодавства (пункт 6 частини 1 статті 23) [18], інформувати про проблеми практичного застосування законодавства та слідкувати за новими практиками, технологіями та тенденціями у сфері захисту персональних даних (пункт 11,12 частини 1 статті 23) [18]. Окрім того, Уповноважений щорічно має виступати із доповіддю про стан додержання прав людини, яка має включати аспекти захисту персональних даних також (частина 2 статті 23) [18].

Уповноважений затвердив кілька документів у сфері захисту персональних даних після того, як до нього перейшли відповідні повноваження. Серед цих документів були Типовий порядок обробки персональних даних, Порядок здійснення Уповноваженим контролю за додержанням законодавства про захист персональних даних (далі «Порядок про здійснення контролю»), який в основному стосується проведення перевірок за додержанням законодавства, та Порядок повідомлення Уповноваженого про обробку персональних даних, яка становить особливий ризик [16]. Уповноважений також періодично затверджує

роз’яснення та рекомендації у сфері захисту персональних даних [117].

Діяльність Уповноваженого забезпечується Секретаріатом Уповноваженого (стаття 10) [118]. У Секретаріаті Уповноваженого утворюються відповідні департаменти, одним з таким департаментів є Департамент у сфері захисту персональних даних (далі «Департамент»). Безпосередньо цей Департамент забезпечує здійснення тих завдань, які покладені на Уповноваженого в сфері захисту персональних даних [119]. До завдань Департаменту віднесені реалізація повноважень Уповноваженого у сфері парламентського контролю, забезпечення розгляду повідомлень, скарг тощо, нормативно-правове забезпечення, нормопроектувальна робота, експертиза законопроєктів, моніторинг стану дотримання захисту персональних даних, забезпечення поновлення порушених прав, просвітницька робота тощо [119].

Значна увага приділяється саме контролю зі сторони Уповноваженого, який здійснюється найчастіше саме у формі до проведення перевірок. Відповідно до Порядку здійснення контролю, перевірка проводиться уповноваженими посадовими особами (пункт 2.1) [116]. За результатами проведення перевірки складається акт (пункт 5.1 Порядку здійснення контролю) [116], а у випадку виявлення порушень також складається припис про усунення порушень (пункт 5.10 Порядку здійснення контролю) [116]. Якщо припис не буде виконаний, тоді Уповноважений чи уповноважена особа складають протокол про адміністративне порушення (пункт 5.15 Порядку здійснення контролю) [116]. Протокол про адміністративне порушення також складаються у випадку виявлення під час перевірки в діях суб’єкта перевірки адміністративних правопорушень за статтею 188^{39} (порушення законодавства у сфері захисту персональних даних) або 188^{40} (невиконання законних вимог Уповноваженого) Кодексу України про адміністративні правопорушення, КУпАП (пункт 5.16 Порядку здійснення контролю) [116]. Такі справи підлягають розгляду у суді (стаття 221) [120]. Тобто, штраф накладається не безпосередньо Уповноваженим чи уповноваженою особою (як наприклад можливо в Європейському Союзі), а саме у судовому порядку.

Окрім адміністративної відповідальності, за порушення захисту персональних даних може наставати кримінальна відповідальність. У Кримінальному кодексі України встановлена відповідальність за порушення недоторканності приватного життя, яке в тому числі включає незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу та незаконну зміну такої інформації (стаття 182) [121]. Як було вказано у Розділі 1 про співвідношення понять конфіденційна інформації та персональні дані, конфіденційна інформація включає в себе персональні дані, відтак за вчинення незаконних дій щодо персональної інформації може наставати кримінальна відповідальність [122]. На жаль, серед доступних матеріалів Уповноваженого відсутня достатня інформація для аналізу щодо кількості перевірок чи опрацювання скарг внаслідок яких осіб притягнули до кримінальної відповідальності чи були відкриті кримінальні провадження за порушення режиму захисту персональних даних чи іншої інформації, яка б вказувала на ефективність діяльності Уповноваженого в зазначеному напрямку. При пошуку у Єдиному реєстрі судових справ вироків за статтею 182 Кримінального кодексу України в контексті персональних даних, база видає всього лиш 23 результати. Такі результати у числах явно свідчать про неефективність кримінального законодавства та правоохоронних органів у забезпеченні захисту персональних даних.

Однозначно вагому частину роботи Уповноваженого складає розгляд скарг про порушення захисту персональних даних. Відповідно до звіту Уповноваженого за 2020 рік, до Уповноваженого надійшло 2 031 повідомлення про порушення прав людини на захист персональних даних, що вдвічі більше ніж у 2019 році (1 061). Ріст такої кількості повідомлень Уповноважений пояснює економічною кризою, викликаною пандемією коронавірусу. Також Уповноважений провів 67 перевірок, серед яких було відкрито 63 провадження та передано до суду 9 протоколів про адміністративне правопорушення [123, с. 21, 22].

Більшість повідомлень стосувались порушення захисту персональних

даних при колекторські діяльності. Уповноважений зазначає, що колекторські компанії вдаються до неправомірної обробки персональних даних в тому числі, особливо телефонних номерів, щоб змусити боржників виконати свої обов'язки перед фінансовими установами. В зазначеному напрямку Уповноваженим було проведено 23 перевірки та порушено 23 провадження проти фінансових компаній та видано 20 приписів, а також здійснювалась співпраця із Національною поліцією України [123, с. 22, 23]. Оскільки Національний банк України здійснює регулювання діяльності небанківських установ, Уповноважений також уклав у 2021 році із ним Меморандум про співпрацю, який в тому числі покликаний захистити осіб від незаконної обробки та поширення їхніх персональних даних [123, с. 24]; (пункт 1.2) [124].

Також повідомлення стосувались порушення захисту персональних даних в Інтернеті, а саме незаконного поширення, в тому числі і державними органами. Зокрема, це стосувалось платформи Prozzoro, яка публікувала персональні дані учасників закупівель, а також незаконного поширення персональних даних у Telegram [123, с. 24, 25]. Ще однак категорія повідомлень стосувались неправомірного витребування згоди осіб на обробку їхніх персональних даних [123, с. 26, 27]. Значна частина повідомлень про порушення також стосувалась доступу осіб до своїх персональних даних [123, с. 33].

Також, Уповноваженим були здійсненні перевірки захисту персональних даних при введенні електронних сервісів та опрацьовувались відповідні нормативно-правові акти, здійснювалась співпраця із іншими органами влади, як Міністерство цифрової трансформації для того щоб забезпечити належний рівень захисту персональних даних осіб при впровадженні зазначених сервісів [123, с. 29-31]. Уповноваженим також проводилась просвітницька діяльність, спрямована на підвищення обізнаності серед населення про персональні дані [123, с. 32].

У звіті Уповноваженого також наводяться рекомендації щодо дій, які варто здійснити, щоб виправити наявні ситуації, що призводять до порушень у сфері захисту персональних даних. Одними з таких рекомендацій є в тому числі ті, які

мають на меті прийняття змін до чинного Закону України «Про захист персональних даних» [123, с. 28], розробка внутрішніх документів у центральних органах виконавчої влади щодо правил обробки та захисту персональних даних [123, с. 34].

Відтак, наявні наразі система нагляду за дотриманням законодавства у сфері захисту персональних даних передбачає парламентський контроль за цією сферою через Уповноваженого, на відміну від ДСЗПД, яка здійснювала нагляд за цією сферою як центральний орган виконавчої влади. На жаль, через відсутність наразі у вільному доступі в мережі звітів ДСЗПД чи іншої інформації щодо ефективності діяльності ДСЗПД протягом 2011-2013 років, порівняти належним чином ефективність роботи Уповноваженого та ДСЗПД ми не можемо. Однак, вартує звернути увагу, що ДСЗПД був спеціальним органом, який здійснював функції у сфері нагляду за забезпеченням захисту персональних даних. Натомість, Уповноважений здійснює нагляд за дотриманням прав людини в Україні, що в тому числі передбачає і нагляд за дотриманням захисту персональних даних. Однак, персональні дані – це тільки одна із сфер, за якими здійснює нагляд Уповноважений.

4.3 Проблеми, які виникають у діяльності публічних органів щодо забезпечення виконання норм Закону та шляхи їх подолання

Як було згадано раніше, наявна система у 2011-2013 році, яка включала в себе діяльність ДСЗПД, піддавалась критиці через відсутність незалежності у діяльності органу, а саме через його інституційну приналежність до системи виконавчих органів. Передача повноважень у сфері нагляду за захистом персональних даних під парламентський контроль, а саме контроль Уповноваженого мала б вирішити цю проблему.

Однак, наявна наразі в Україні система захисту персональних даних і надалі піддається критиці. Критика в основному зумовлена неефективністю захисту персональних даних фізичних осіб, яка випливає як і з специфіки

діяльності Уповноваженого та Департаменту, організації їхньої роботи, так і у зв'язку із недоліками наявного законодавства.

Зокрема, одна із причини неефективності наявної системи – це неможливість притягнути юридичних осіб до відповідальності за порушення захисту персональних даних Уповноваженим, окрім як видачі обов'язкових до виконання приписів. Адміністративна відповідальність, передбачена статтями 188^{39} та 188^{40} КУпАП [125], перш за все застосовується саме до фізичних осіб, а не до юридичних. По-факту, єдиний спосіб змусити юридичну особу відшкодувати завдану нею шкоду за порушення обробки і захисту персональних даних – це подати позов в межах цивільного провадження [9, с. 146; 126, с. 297]. Уповноважений не наділений самостійними повноваженнями накладати штраф при виявленні порушення на юридичних осіб, як це можуть робити, наприклад наглядові органи у Європейському Союзі. Відтак, можливості Уповноваженого щодо притягнення юридичних осіб до відповідальності є обмеженими і полягають тільки у видачі приписів. Однак, примусове виконання приписів Уповноваженого юридичною особою саме по собі важко назвати формою відповідальності за порушення. Як визначено у самому Порядку про здійснення контролю, припис – це вимога Уповноваженого усунути порушення (пункт 1.2) [116]. Тобто, щоб отримати відшкодування за вчинене щодо цієї особи порушення від юридичної особи, фізична особа може тільки звернутись до суду, оскільки повноваження Уповноваженого в даній ситуації обмежені.

Окрім того, навіть наявна система адміністративної відповідальності чи виконання приписів не є ефективною. Зокрема, приписи повинні були б виконувати превентивну функцію, тобто запобігати порушенням законодавства зі сторони інших володільців, але такого ефекту вони не мають [127, с. 97].

Наявна адміністративна відповідальність за порушення законодавства у сфері персональних даних стосується тільки неповідомлення чи несвоєчасного повідомлення Уповноваженого про обробку персональних даних, невиконання приписів Уповноваженого, порушення порядку захисту персональних даних (тільки якщо це призвело до незаконного доступу чи порушення прав суб'єкта

персональних даних) (стаття 188[39] та 188[40]) [125]. Зазначені формулювання звужують відповідальність володільців, оскільки не передбачають відповідальності за порушення прав суб'єкта персональних даних, які в тому числі передбачені у Законі, якщо вони не зумовлені порушенням порядку захисту персональних даних. Також, відсутня відповідальність за неповідомлення суб'єкта про обробку його персональних даних чи відмову в наданні доступу до персональних даних, незаконне поширення персональних даних [127, с. 96-98].

Тобто, наявна наразі система не здатна ефективно захищати права суб'єктів персональних даних, як через недосконаліть законодавства, яке нечітко встановлює відповідальність володільців та розпорядників персональних даних, так і через обмеженні повноваження Уповноваженого щодо притягнення до відповідальності у випадку порушення.

Ще одна причина критики наявної організації нагляду та контролю за законодавством – це відсутність наглядового органу як спеціального органу захисту персональних даних (англ. *Data Protection Authority*) [113]. Як вже згадувалось раніше, Уповноважений здійснює парламентський контроль за додержанням прав людини, а контроль за захистом персональних даних – це одна із сфер його діяльності, яка не є основною, адже Уповноважений здійснює нагляд за додержанням прав людини в загальному.

Крім того, парламентський контроль передбачає підзвітність та підконтрольність Уповноваженого Верховній Раді України, що також в свою чергу викликає питання щодо незалежності Уповноваженого як наглядового органу в сфері захисту персональних даних [128]. Модель Європейського Союзу, на яку орієнтуються в Україні, передбачає можливість наглядового органу здійснювати нагляд за дотриманням законодавства усіма органами, які існують у державі, тобто в тому числі за законодавчою, виконавчою та судовою владою. Натомість здійснення парламентського контролю Уповноваженим не до кінця співпадає із поняттям «повної незалежності» та може мати ризик впливу на Уповноваженого з боку законодавчого органу, тобто Верховної Ради.

Ще одна причина для критики – відсутність належних ресурсів для забезпечення роботи Уповноваженого в контексті нагляду за законодавством у сфері захисту персональних даних. Наявні на даний момент людські, фінансові та інші ресурси в Уповноваженого та Департаменту не забезпечують належний рівень організації роботи, а відтак і ефективність у розгляді скарг, проведенні перевірок, виконанні інших завдань Департаменту та Уповноваженого для забезпечення виконання законодавства про захист персональних даних. Зокрема, у 2019 році Департамент складався всього лиш із 13 осіб, а виділений бюджет складав всього на всього 150 000 євро. Натомість у Великій Британії кількість працівників наглядового органу становила 700 осіб [128].

Відтак, основні проблеми зараз стосуються ефективності діяльності Уповноваженого, яка в тому числі залежить від наявних ресурсів, притягнення порушників законодавства у сфері персональних даних до відповідальності та забезпечення захисту суб'єктів персональних даних.

Серед шляхів вирішення озвучених проблем одним із ключових є реформа українського законодавства у сфері захисту персональних даних. Очевидно, що проблема забезпечення прав суб'єктів персональних даних та виконання і дотримання законодавства є пов'язаною не тільки із недоліками системи нагляду, яка наразі існує, але і з неактуальним законодавством, недієвими механізмами притягнення до відповідальності, а також низькою поінформованістю населення про свої права, в тому числі про право на захист персональних даних.

Обговорення питання зміни законодавства, а саме внесення змін до Закону чи прийняття нової редакції, активно здійснюється в Україні. Наразі створена робоча група, яка складається із Комітету Верховної Ради України з питань цифрової трансформації та Комітету Верховної Ради України з питань прав людини, деокупації та реінтеграції тимчасово окупованих територій у Донецькій, Луганській областях та Автономної Республіки Крим, міста Севастополя, національних меншин і міжнаціональних відносин, представників Секретаріату Уповноваженого, представників Міністерства цифрової

трансформації, представників міжнародних організацій, правників та представників громадянського суспільства [129]. Ця робоча група працює над новим законом у сфері захисту персональних даних. Новий закон має відповідати стандартам Європейського Союзу, а саме Регламенту та Конвенції 108. Під час обговорення проєкту значна увага приділяється також питанню створення незалежного наглядового органу, який би забезпечував виконання та дотримання законодавства у сфері захисту персональних даних [130]. 30 березня 2021 року було представлено законопроєкт про захист персональних даних. Однак, поки фінальний текст не є узгоджений і надати належну оцінку відповідності законопроєкту стандартам Європейського Союзу, Регламенту та Конвенції 108 поки неможливо.

Прийняття нового закону однозначно повинно вирішити питання наглядового органу в Україні. При створенні наглядового органу важливо пам'ятати, що одною із обов'язкових характеристик цього органу є незалежність, тобто відсутність можливості прямого чи непрямого впливу на діяльність цього органу від будь-яких суб'єктів щодо яких цей незалежний наглядовий орган здійснює свої повноваження. Як зазначає Гнатюк С. Л. з посиланням на Лист представництва України при Європейському Союзі «Щодо актуальних питань захисту персональних даних», у 2013 році під час обговорення статусу ДСЗПД та забезпечення незалежності цього органу, ДСЗПД висловили свою позицію, за якої на думку органу необхідно створити державний орган, який володіє спеціальним статусом, за прикладом Антимонопольного комітету України [112, с. 47-48].

У вересні 2020 року був опублікований аналіз законодавства у сфері захисту персональних даних в Україні [131]. В аналізі були висвітлені потенційні шляхи подолання проблем, які існують наразі в законодавстві про захист персональних даних, в тому числі щодо наявної системи нагляду за законодавством. Основні тези в аналізі вказували, що нове законодавство в цілому має базуватись на Регламенті, а наглядовий орган має бути незалежним із ширшими повноваженнями, ніж зараз є в Уповноваженого, а саме

регуляторними та законодавчими [131, с. 3].

Зокрема, пропонується взяти за основу модель наглядового органу Німеччини, а наглядовий орган не має бути керований будь-яким виконавчим органом. Наглядовий орган має очолюватись інспектором, а організаційна структура органу має включати в себе департаменти, які виконуватимуть основні завдання проведення розслідувань порушень та скарг, перевірок, накладення штрафів, розробки нового законодавства та прийняття інструкцій, міжнародного та внутрішнього співробітництва. Крім того, пропонується надати можливість органу наймати необхідну кількість працівників та формувати власний бюджет зокрема зі штрафів [131, с. 51], як це є у Європейському Союзі та США у Каліфорнії відповідно до CCPA. Як бачимо, в основному рекомендації полягають у адаптуванні моделі Європейського Союзу в Україні, зокрема щодо сфери повноважень наглядового органу.

Відтак, основні шляхи вирішення поки полягають у модернізації законодавства та створенні нового наглядового органу, а відбуватись це має на основі Регламенту, Конвенції 108 та практики Європейського Союзу. Україна тісно співпрацює з Європейським Союзом та Радою Європи в зазначеному напрямку. Натомість американська модель за приклад не береться, оскільки США зараз самі стоять на хвилі модернізації власного законодавства та мають власні проблеми із забезпеченням захисту персональної інформації, в тому числі зумовленої відсутністю єдиного наглядового органу. Єдиний приклад, який може братись до уваги, це наявна система захисту персональної інформації та діяльність відповідних органів у Каліфорнії.

Висновки до Розділу 4

Підсумовуючи викладене у Розділі 4, можна зробити наступні висновки.

По-перше, Україна зараз орієнтується на стандарти європейського законодавства, про що свідчать взяті на себе зобов’язання відповідно до Угоди про асоціацію та співпраця із європейськими організаціями. Відтак, аналіз

діяльності публічних органів у сфері захисту персональних даних необхідно здійснювати в контексті відповідності європейським стандартам. Натомість досвід США є корисним тільки в частині майбутньої діяльності CPPA в Каліфорнії, оскільки американська законодавча система захисту персональних даних також перебуває зараз на хвилі реформування через відсутність уніфікованого законодавства та єдиного наглядового органу в сфері захисту персональних даних.

По-друге, з часів прийняття Закону і по сьогоднішній день одним із каменів спотикання в побудові належної законодавчої системи захисту персональних даних залишається організація наглядового органу, його компетенція та місце в системі органів влади. На жаль, ні ДСЗПД, ні Уповноважений не відповідають усім ключовим вимогам, які встановлюються Регламентом та Європейським Союзом, а найбільше вимозі незалежності.

По-третє, робота Уповноваженого у сфері захисту персональних даних наразі не здатна забезпечити ефективний захист суб'єктів персональних даних. Це пов'язано як і з недоліками законодавства, так і з специфікою роботи Уповноваженого та обмеженими ресурсами. Однак, варто відзначити, що в доступних наразі межах Уповноважений намагається здійснювати активну роботу в цій сфері, про що можуть свідчити підписані меморандуми про співпрацю, співпраця із Міністерством цифрової трансформації, результати роботи з розгляду скарг, проведення перевірок та надання рекомендацій.

По-четверте, в Україні однозначно необхідно провести комплексну реформу законодавства у сфері захисту персональних даних та створити наглядовий орган, що повністю відповідає основним вимогам Європейського Союзу. На щастя, активна робота в зазначеному напрямку зараз проводиться Робочою групою. Оцінити наскільки враховано у новому проєкті закону європейський чи інший іноземний досвід поки складно через відсутність проєкту поки що у публічному доступі. Наразі необхідно здійснювати моніторинг роботи Робочої групи та очікувати на безпосередній текст проєкту, після чого вже можна буде надати йому оцінку щодо врахування іноземного досвіду при його розробці.

ВИСНОВКИ

Проаналізувавши діяльність публічних органів у сфері захисту персональних даних у Європейського Союзу, США та України, автором були зроблені наступні висновки.

Право на захист персональних даних як окреме від права на приватність закріпилось у 1980х роках минулого століття із прийняттям Конвенції 108, розвитком практики ЄСПЛ та початком активної роботи в напрямку врегулювання автоматизованої обробки персональних даних у внутрішньому законодавстві. В цілому, у трьох правових системах єдиний підхід до визначення, що таке персональні дані, як інформації про фізичну особу, яка ідентифікована або яку можна ідентифікувати. Однак, у США через відсутність єдиного законодавства у сфері захисту персональних даних, це поняття може звужуватись до специфічної категорії персональних даних в залежності від спеціального закону, який застосовується.

Найкраще доктрина захисту персональних даних розвинена у Європейському Союзі, про що свідчить наявність актуального законодавства, послідовного визначення, що таке персональні дані, та чітке відокремлення захисту персональних даних від захисту права на приватність. У США доктрина захисту персональних даних є менш розвиненою в основному через відсутність чіткого розмежування захисту персональних даних та захисту приватності та відсутності єдиного законодавчого регулювання на федеральному рівні та актуального і послідовного законодавства на рівні штатів. Доктрина, яка наявна в Україні, базується в основному на європейській моделі про що свідчить взяття Директиви як основи для Закону, активна співпраця із Європейським Союзом у напрямку реформування законодавства в сфері захисту персональних даних та взяті на себе зобов'язання відповідно до Угоди про асоціацію.

Щодо діяльності публічних органів у сфері захисту персональних даних зазвичай зводиться до двох великих груп повноважень. Перша – це забезпечення виконання законодавства у сфері захисту персональних даних через проведення

розслідувань порушень, розгляду скарг, проведення перевірок, накладення штрафів тощо. Друга – це видача роз'яснень, інструкцій щодо застосування профільного законодавства, регуляторна діяльність, перевірка актуальності законодавства, регулярний перегляд та підготовка оновлень. Рідше діяльність із ведення реєстрів, видачі дозволів тощо. Обсяг цих повноважень відрізняється у кожній із правових систем та залежить від наявного законодавчого регулювання.

Варто звернути увагу, що часто можна зустріти використання формулювання здійснення «нагляду» або «контролю» публічними органами. На нашу думку, застосування таких формулювань не до кінця відповідає насправді тій ролі, яку виконують публічні органи у сфері захисту персональних даних. Хоч «supervisory» і перекладається як «наглядовий», з наведених повноважень у абзаці вище ми бачимо, що функції публічних органів не звужуються виключно до нагляду, а саме до проведення перевірок та застосування санкцій до порушників.

Щодо безпосередньої діяльності публічних органів, то у Європейському Союзі така діяльність здійснюється на двох рівнях: перший – національний рівень держав-членів; другий – наднаціональний на рівні Європейського Союзу. У Європейському Союзі публічні органи називаються наглядовими і вони є спеціально створеними для забезпечення виконання законодавства у сфері захисту персональних даних. Їхні повноваження є доволі широкими, вони цілком автономні в прийнятті власних рішень та застосуванні санкцій до порушників. Прийняття Регламенту позитивно відзначилось на ефективності роботи публічних органів, про що свідчить кількість розглянутих за рік скарг, збільшення штату та бюджету цих органів. Однак, ключові проблеми як от забезпечення послідовності у діяльності публічних органів держав-членів, співпраця між ними, а також підвищення обізнаності та спрощення розуміння застосування законодавства надалі лишаються, незважаючи на позитивні зрушення після прийняття Регламенту.

У США як на федеральному так і на рівні штатів відсутні спеціальні публічні органи, які здійснюються діяльність виключно у сфері захисту

персональних даних. Ці обов'язки покладаються на органи, які здійснюють діяльність у різних сферах, як от конкурентне законодавство (Федеральна торгова комісія) чи генеральні прокурори на рівні штатів. Оскільки захист персональних даних є тільки однією із складових їхньої діяльності і виключно в межах спеціальних законів, а повноваження не є чітко визначеними, ефективність забезпечення права на захист персональних даних є низькою та неефективною. Така неефективність та невизначеність призводить до критики наявної у США системи. Єдиний наразі штат у США, де були прийняті відповідні кроки для реформування законодавства – це Каліфорнія, однак суттєвих висновків щодо ефективності реформи ми поки зробити не можемо, оскільки публічний орган у цьому напрямку – CPPA – ще не розпочав свою роботу. Окрім того, модель діяльності CPPA та й законодавство в сфері захисту персональних даних загалом у Каліфорнії також схожі на європейську модель.

В Україні теж немає спеціального публічного органу, обов'язки за забезпеченням виконання законодавства здійснює Уповноважений, а спеціального органу не існує із 2014 року. Через обмежені повноваження Уповноваженого та недоліки законодавства, контраверсійні положення та місцями складність застосування на практиці відповідальності до порушників, обмеження в ресурсах діяльність Уповноваженого не є ефективною.

Основні проблеми в Україні щодо діяльності публічного органу у сфері захисту персональних даних стосуються:

1. відсутності незалежного публічного органу відповідно до стандартів Європейського Союзу;
2. неактуальність законодавства та невідповідності його вимогам Регламенту;
3. неефективність виконання повноважень у сфері забезпечення захисту прав суб'єктів персональних даних через труднощі у застосуванні заходів відповідальності до порушників.

Відтак, для подолання цих проблем пропонуємо наступні шляхи вирішення:

1. продовжувати співпрацювати із європейськими партнерами в напрямку розробки нового законодавства та враховувати їхні коментарі щодо відповідності проєктів стандартам Європейського Союзу. На жаль, система США сама перебуває на стадії реформування і запозичити як приклад можливо тільки регулювання діяльності публічного органу у Каліфорнії, яке в тому числі схоже на європейську модель.
2. визначити процедуру створення та організації спеціального публічного органу забезпечення виконання і дотримання законодавства у сфері захисту персональних даних, яка б відповідала вимогам незалежності. Така процедура може включати, наприклад, формування органу (одноособового чи колегіального) за поданням Кабінету Міністрів України, що затверджується Верховною Радою України та які призначаються Указом Президента, як було запропоновано в аналізу законодавства про захист персональних даних. Окрім того, добір штату в орган, його чисельність мають бути незалежними від зовнішнього впливу.
3. надати спеціальному публічному органу забезпечення виконання і дотримання законодавства у сфері захисту персональних даних ширших повноважень у порівнянні з тими, якими володіє зараз Уповноважений, та внести зміни у законодавство, яке встановлює відповідальність за порушення законодавства в сфері захисту персональних даних: розширити підстави притягнення до адміністративної відповідальності, передбачити адміністративну відповідальність для юридичних осіб, надати публічному органу можливість накладати штрафи за порушення законодавства чи інші види відповідальності, як от обмеження чи призупинення обробки персональних даних.
4. прийняти за результатами роботи у пункті 1 новий закон у сфері захисту персональних даних, який би був актуальним та вирішував викладені вище проблеми та встановлював основні засади діяльності публічного

органу у сфері захисту персональних даних, його організацію, повноваження та гарантії, зокрема, гарантії незалежності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What Is Privacy?. URL: https://privacyinternational.org/explainer/56/what-privacy (last accessed: 11.05.2021).
2. Olmstead v. United States, 277 U.S. 438 (1928). URL: https://tile.loc.gov/storage-services/service/ll/usrep/usrep277/usrep277438/usrep277438.pdf (last accessed: 11.05.2021).
3. Warren & Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890).
4. Katz v. United States, 389 U.S. 347 (1967). URL: https://tile.loc.gov/storage-services/service/ll/usrep/usrep389/usrep389347/usrep389347.pdf (last accessed: 11.05.2021).
5. Mirmina S. A. Translating Justice Brandeis's Views on Privacy for the 21st Century. 20 p. URL: https://bir.brandeis.edu/bitstream/handle/10192/31436/LDB100Mirmina.pdf?sequence=1&isAllowed=y (last accessed: 11.05.2021).
6. Конвенція про захист прав людини і основоположних свобод: Конвенція Ради Європи від 04.11.1950 р. № 995_004. URL: https://zakon.rada.gov.ua/laws/show/995_004 (дата звернення: 11.05.2021).
7. Міжнародний пакт про громадянські і політичні права: Пакт Орг. Об'єдн. Націй від 16.12.1966 р. № 995_043. URL: https://zakon.rada.gov.ua/laws/show/995_043 (дата звернення: 11.05.2021).
8. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Конвенція Ради Європи від 28.01.1981 р. № 994_326. URL: https://zakon.rada.gov.ua/laws/show/994_326 (дата звернення: 11.05.2021).
9. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. – К.: К.І.С., 2015. – 220 с.

10. Factsheet – Personal data protection. European Court of Human Rights, 2021. 28 p. URL: https://www.echr.coe.int/Documents/FS_Data_ENG.pdf (last accessed: 11.05.2021).
11. Directorate General Human Rights and Rule of Law. Case Law of The European Court of Human Rights Concerning the Protection of Personal Data. Strasbourg: Council of Europe, 2018. 309 p. URL: https://rm.coe.int/t-pd-2018-15-case-law-on-data-protection-may2018-en/16808b2d36 (last accessed: 11.05.2021).
12. Malone v. The United Kingdom, No. 8691/79 [1984] (Concurring Opinion of Judge Pettiti) ECHR. URL: https://hudoc.echr.coe.int/eng#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-57533%22]} (last accessed: 11.05.2021).
13. Leander v. Sweden, No. 9248/81 [1987] (Judgment) ECHR. URL: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22\%22CASE%20OF%20LEANDER%20v.%20SWEDEN\%22%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-57519%22]} (last accessed: 11.05.2021).
14. Gaskin v. the United Kingdom, No. 10454/83 [1989] (Judgement) ECHR. URL: https://hudoc.echr.coe.int/eng#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-57491%22]} (last accessed: 11.05.2021).
15. Z. v. France, No. 22009/93 [1997] (Judgment) ECHR. URL: https://hudoc.echr.coe.int/eng#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-58033%22]} (last accessed: 11.05.2021).
16. Handbook on European data protection law: 2018 edition. Luxembourg : Publications Office of the European Union, 2018. 402 p. URL: https://www.echr.coe.int/documents/handbook_data_protection_eng.pdf (last accessed: 11.05.2021).
17. Hustinx P. EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation. 2013. 52 p. URL: https://www.statewatch.org/media/documents/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf (last accessed: 11.05.2021).

18. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 11.05.2021).
19. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32016R0679 (last accessed: 11.05.2021).
20. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031–0050. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046 (last accessed: 11.05.2021).
21. Explanatory Report to the 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, 2018, 27 p. URL: https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a (last accessed: 11.05.2021).
22. Ralf Michaels, American Law (United States). Encyclopedia of Comparative Law 2006, p. 66-77. URL: https://core.ac.uk/download/pdf/62562393.pdf (last accessed: 11.05.2021).
23. Hasty R., Dr. Nigel T. W., Subjally M. Data Protection Law in the USA. Advocates for International Development. 2013. 21 p. URL: https://www.neighborhoodindicators.org/sites/default/files/course-materials/A4ID_DataProtectionLaw%20.pdf (last accessed: 11.05.2021).
24. Pittman F. P., Chabinsky S. Data Protection in the USA. ICLG. URL: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa (last accessed: 11.05.2021).

25. Boyne S. M. Data Protection in the United States. The American Journal of Comparative Law. 2018. Vol. 66. P. 299–343.
26. CAN-SPAM Act: A Compliance Guide for Business. Federal Trade Commission. URL: https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business (last accessed: 11.05.2021).
27. Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act) Pub.L. 106–102, 113 Stat. 1338. URL: https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf (last accessed: 11.05.2021).
28. Summary of the HIPAA Privacy Rule: OCR Privacy Brief. United States Department of Health and Human Services (HHS) 25 p. URL: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf (last accessed: 11.05.2021).
29. California Consumer Privacy Act (CCPA) Fact Sheet. California Department of Justice, Office of the Attorney General 3 p. URL: https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf (last accessed: 11.05.2021).
30. California Consumer Privacy Act [1798.100 - 1798.199.100] (2018, Cal. Legis. Serv. Ch. 55, Sec. 3). URL: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 (last accessed: 11.05.2021).
31. 201 CMR 17: Standards for the protection of personal information of residents of the Commonwealth (2009). URL: https://www.mass.gov/doc/201-cmr-1700-standards-for-the-protection-of-personal-information-of-residents-of-the-1/download (last accessed: 11.05.2021).
32. New York General Business Law §899-aa (2012). URL: https://law.justia.com/codes/new-york/2013/gbs/article-39-f/899-aa/ (last accessed: 11.05.2021).

33. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 11.05.2021).
34. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17 (дата звернення: 11.05.2021).
35. Буртник Х. Конфіденційна інформація, інформація про особу та персональні дані: співвідношення і регулювання. URL: https://cedem.org.ua/analytics/konfidentsijna-informatsiya-informatsiya-pro-osobu-ta-personalni-dani-spivvidnoshennya-i-regulyuvannya/ (дата звернення: 11.05.2021).
36. 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 № 2-рп/2012 від 20.01.2012. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12#Text (дата звернення: 11.05.2021).
37. Supervisory authorities: consistency and Data Protection Authorities (DPAs) under GDPR. i-SCOOP. URL: https://www.i-scoop.eu/supervisory-authorities-consistency-and-data-protection-authorities-dpas/ (last accessed: 11.05.2021).
38. What are Data Protection Authorities (DPAs)?. European Commission. URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en (last accessed: 11.05.2021).
39. What is the Role of the Data Protection Authority?. European Commission. URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-role-data-protection-authority_en (last accessed: 11.05.2021).
40. Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, p. 47–390. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT (last accessed: 11.05.2021).

41. Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012P%2FTXT (last accessed: 11.05.2021).
42. Balthasar A. 'Complete Independence' of National Data Protection Supervisory Authorities – Second Try: Comments on the Judgment of the CJEU of 16 October 2012, C-614/10 (European Commission v. Austria), with Due Regard to its Previous Judgment of 9 March 2010, C-518/07 (European Commission v. Germany). Utrecht Law Review. 2013. Vol. 9, no. 3. P. 26–38.
43. The Court of Justice of the European Union, European Commission v. Federal Republic of Germany. Judgment of the Court (GC) of 9 March 2010. Case C-518/07. URL: https://curia.europa.eu/juris/document/document.jsf?text=&docid=79752&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=11508291 (last accessed: 11.05.2021).
44. The Court of Justice of the European Union, European Commission v. Federal Republic of Austria. Judgment of the Court (GC) of 16 October 2012. Case C-614/10. URL: https://curia.europa.eu/juris/document/document.jsf?text=&docid=128563&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=359958;%20https://medium.com/golden-data/commission-v-austria-independence-of-eu-supervisory-authorities-f78efbdea204 (last accessed: 11.05.2021).
45. Report on EU Data Protection Authorities Part 4: Resources. Deloitte Privacy Services – Privacy Response 74 p. URL: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-reports-resources.pdf (last accessed: 11.05.2021).
46. The new European General Data Protection Regulation. Crowell & Moring 40 p. URL: https://www.crowell.com/files/Brussels-EU-Data-Protection-GDPR.pdf (last accessed: 11.05.2021).
47. Giurgiu A., Larsen T. A. Roles and Powers of National Data Protection Authorities Moving from Directive 95/46/EC to the GDPR: Stronger and More

‘European’ DPAs as Guardians of Consistency?. EDPL. 2016. No. 3. P. 342–352. URL: https://orbilu.uni.lu/bitstream/10993/29819/1/Roles%20and%20Powers%20of%20National%20Data%20Protection%20Authorities_EDPL%203_2016.pdf (last accessed: 11.05.2021).

48. Dr. Gabel D., Hickman T. GDPR Guide to National Implementation. White & Case. 13 November 2019. URL: https://www.whitecase.com/publications/article/gdpr-guide-national-implementation#q15 (last accessed: 11.05.2021).
49. Guidelines for identifying a controller or processor’s lead supervisory authority. Article 29 Data Protection Working Party, 2017, 16/EN WP 244 rev.01 12 p.
50. European Data Protection Board. Our Members URL: https://edpb.europa.eu/about-edpb/about-edpb/members_en (last accessed: 11.05.2021).
51. Report on EU Data Protection Authorities Part 2: Reported Personal Data Breaches. Deloitte Privacy Services – Privacy Response 20 p. URL: https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-risk-report-on-eu-data-protection-authorities-part-2.pdf (last accessed: 11.05.2021).
52. Report on EU Data Protection Authorities Part 3: Received Complaints. Deloitte Privacy Services – Privacy Response 29 p. URL: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-part3-received-complaints.pdf (last accessed: 11.05.2021.
53. Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation. Communication from the Commission to the European Parliament and the Council, 2020, COM/2020/264 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264 (last accessed: 11.05.2021).
54. Data protection authorities in Germany. Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen. URL:

https://www.ldi.nrw.de/LDI_EnglishCorner/mainmenu_DataProtection/Inhalt2/authorities/authorities.php (last accessed: 11.05.2021).

55. National Data Protection Authority. Germany. Data Protection Laws of the World. DLA Piper. URL: https://www.dlapiperdataprotection.com/index.html?t=authority&c=DE (last accessed: 11.05.2021).
56. National Data Protection Authority. Belgium. Data Protection Laws of the World. DLA Piper. URL: https://www.dlapiperdataprotection.com/index.html?t=authority&c=BE&c2= (last accessed: 11.05.2021).
57. History of the ICO. Information Commissioner's Office. URL: https://ico.org.uk/about-the-ico/our-information/history-of-the-ico/ (last accessed: 11.05.2021).
58. Data protection and coronavirus – advice for organisations. Information Commissioner's Office. URL: https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/coronavirus-recovery-data-protection-advice-for-organisations/ (last accessed: 11.05.2021).
59. Report on EU Data Protection Authorities Part 5: Guidance Issued. Deloitte Privacy Services – Privacy Response 40 p. URL: https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/risk-reports-privacy-and-data-protection-guidance-issued.pdf (last accessed: 11.05.2021).
60. Guide to the UK General Data Protection Regulation (UK GDPR). Information Commissioner's Office. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ (last accessed: 11.05.2021).
61. Information rights after the end of the transition period – Frequently asked questions. Information Commissioner's Office. URL: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/transition-period-faqs/ (last accessed: 11.05.2021).

62. EDPB – Former Article 29 Working Party. Privacy Rules. URL: https://www.privacyrules.com/privacy-global-expertise/edpb-article-29-working-party-0001323.html (last accessed: 11.05.2021).
63. Article 29 Working Party/European Data Protection Board. Guidance, Opinions. Future of Privacy Forum. URL: https://fpf.org/article-29-working-partyeuropean-data-protection-board/ (last accessed: 11.05.2021).
64. Who we are. European Data Protection Board. URL: https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en (last accessed: 11.05.2021).
65. European Data Protection Board 2018 Annual Report. Cooperation & Transparency. EDPB, 2019. 32 p. URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_annual_report_2018_-_digital_final_1507_en.pdf (last accessed: 11.05.2021).
66. European Data Protection Board 2018 Annual Report. Working Together for Stronger Rights. EDPB, 2020. 47 p. URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_annual_report_2019_en.pdf.pdf (last accessed: 11.05.2021).
67. Our Role as a Supervisor. European Data Protection Supervisor. URL: https://edps.europa.eu/data-protection/our-role-supervisor_en (last accessed: 11.05.2021).
68. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.), OJ L 295, 21.11.2018, p. 39–98. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725 (last accessed: 11.05.2021).
69. About. European Data Protection Supervisor. URL: https://edps.europa.eu/about-edps_en (last accessed: 11.05.2021).

70. Frequently Asked Questions. European Data Protection Supervisor. URL: https://edps.europa.eu/frequently-asked-questions_en (last accessed: 11.05.2021).
71. Wojciech Wiewiórowski. European Data Protection Supervisor. URL: https://edps.europa.eu/about-edps/members-mission/supervisors/wojciech-wiewi%C3%B3rowski_en (last accessed: 11.05.2021).
72. Annual Report 2020. European Data Protection Supervisor. 2021, 122 p. URL: https://edps.europa.eu/system/files/2021-04/2021-04-19-annual-report-2020_EN.pdf (last accessed: 11.05.2021).
73. Mémorandum of Understanding between the European Data Protection Board and the European Data Protection Supervisor. URL: https://edpb.europa.eu/sites/default/files/files/file1/memorandum_of_understanding_signed_en.pdf (last accessed: 11.05.2021).
74. Our History. Federal Trade Commission. URL: https://www.ftc.gov/about-ftc/our-history (last accessed: 11.05.2021).
75. About the FTC. Federal Trade Commission. URL: https://www.ftc.gov/about-ftc (last accessed: 11.05.2021).
76. Federal Trade Commission Act. Federal Trade Commission. URL: https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act (last accessed: 11.05.2021).
77. Protecting Consumer Privacy and Security. Federal Trade Commission. URL: https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security (last accessed: 11.05.2021).
78. Stevens G. The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority. Congressional Research Service. 2014. 15 p. URL: https://fas.org/sgp/crs/misc/R43723.pdf (last accessed: 11.05.2021).
79. Federal Trade Commission Act, 15 U.S.C. §§ 41-58. 1914. URL: https://www.ftc.gov/sites/default/files/documents/statutes/federal-trade-

commission-act/ftc_act_incorporatingus_safe_web_act.pdf (last accessed: 11.05.2021).

80. Division of Privacy and Identity Protection. Federal Trade Commission. URL: https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-privacy-and-identity (last accessed: 11.05.2021).
81. Privacy & Data Security Update: 2018. Federal Trade Commission. 16 p. URL: https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf (last accessed: 11.05.2021).
82. FTC Policy Work. Federal Trade Commission. URL: https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security/ftc-policy-work (last accessed: 11.05.2021).
83. National Data Protection Authority. United States. Data Protection Laws of the World. DLA Piper. URL: https://www.dlapiperdataprotection.com/index.html?t=authority&c=US#:~:text=The%20FTC%20has%20jurisdiction%20over,deceptive%20trade%20practices%2C%20including%20materially (last accessed: 11.05.2021).
84. Attachment A to FTC Privacy Shield Letter. The EU-U.S. Privacy Shield Framework in Context: An Overview of the U.S. Privacy and Security Landscape. 5 p. URL: https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q10 (last accessed: 11.05.2021).
85. Privacy & Data Security Update: 2019. Federal Trade Commission. 18 p. URL: https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf (last accessed: 11.05.2021).
86. Cadwalladr C., Graham-Harrison E. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. the Guardian. 2018. 17

March. URL: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (last accessed: 11.05.2021).

87. Privacy and Security Enforcement. Federal Trade Commission. URL: https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last accessed: 11.05.2021).
88. Brennan M. W. Complying with the CAN-SPAM Act. The Practical Guidance Journal. 2016. 11 August. URL: https://www.lexisnexis.com/lexis-practical-guidance/the-journal/b/pa/posts/complying-with-the-can-spam-act (last accessed: 11.05.2021).
89. CAN-SPAM Rule. Federal Trade Commission. URL: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/can-spam-rule (last accessed: 11.05.2021).
90. Muris T. J. The Federal Trade Commission and the Future Development of U.S. Consumer Protection Policy. 84 p. URL: https://core.ac.uk/download/pdf/76622959.pdf (last accessed: 11.05.2021).
91. FTC v. Wyndham Worldwide Corp. 799 F.3d 236 (3d Cir. 2015). Brief. Law School Case Brief. URL: https://www.lexisnexis.com/community/casebrief/p/casebrief-ftc-v-wyndham-worldwide-corp (last accessed: 11.05.2021).
92. HIPAA Enforcement. Health Information Privacy. U.S. Department of Health & Human Services. URL: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html#:~:text=HHS'%20Office%20for%20Civil%20Rights,privacy%20practices%20of%20covered%20entities (last accessed: 11.05.2021).
93. Enforcement Process. Health Information Privacy. U.S. Department of Health & Human Services. URL: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html (last accessed: 11.05.2021).
94. The U.S. Urgently Needs a Data Protection Agency. Electronic Privacy Information Center. URL: https://epic.org/dpa/ (last accessed: 11.05.2021).

95. Cohen G. 4 Reasons the United States Needs Federal Privacy Legislation Now. Privitar. November 2, 2020. URL: https://www.privitar.com/blog/united-states-federal-privacy-legislation/ (last accessed: 11.05.2021).
96. Meehan M. The Need for Unified Data Protection in the U.S. Nextgov. September 21, 2020. URL: https://www.nextgov.com/ideas/2020/09/need-unified-data-protection-us/168643/ (last accessed: 11.05.2021).
97. Cohen M. Minnesota - Sectoral Privacy Overview. OneTrust Data Guidance. URL: https://www.dataguidance.com/notes/minnesota-sectoral-privacy-overview (last accessed: 11.05.2021).
98. 201 CMR 17.00: Standards for the Protection of Personal Information of MA Residents. Mass.gov. URL: https://www.mass.gov/regulations/201-CMR-1700-standards-for-the-protection-of-personal-information-of-ma-residents (last accessed: 11.05.2021).
99. Massachusetts General Laws Chapter 93H: Security Breaches. URL: https://malegislature.gov/laws/generallaws/parti/titlexv/chapter93h (last accessed: 11.05.2021).
100. A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority. Federal Trade Commission URL: https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority (last accessed: 11.05.2021).
101. Gates M. CCPA Deep Dive: How California is Enforcing its Major Privacy Law. ASIS. December 1, 2020. URL: https://www.asisonline.org/security-management-magazine/articles/2020/12/ccpa-deep-dive-how-california-is-enforcing-its-major-privacy-law/ (last accessed: 11.05.2021).
102. Forman D. New CCPA Regulations Issued by California Attorney General. JDSPURA. March 24, 2021. URL: https://www.jdsupra.com/legalnews/new-ccpa-regulations-issued-by-7332146/ (last accessed: 11.05.2021).
103. Mahoney M. Consumer Reports praises the California Attorney General for cracking down on dark patterns. Consumer Reports. March 16, 2021. URL: https://advocacy.consumerreports.org/press_release/consumer-reports-praises-

the-california-attorney-general-for-cracking-down-on-dark-patterns/ (last accessed: 11.05.2021).

104. California Privacy Rights Act: An Overview. Privacy Rights Clearing House. December 10, 2020. URL: https://privacyrights.org/resources/california-privacy-rights-act-overview (last accessed: 11.05.2021).
105. De la Torre L., Brown G. What is the California Privacy Protection Agency?. IAPP. November 23, 2020. URL: https://iapp.org/news/a/what-is-the-california-privacy-protection-agency/ (last accessed: 11.05.2021).
106. California Officials Announce California Privacy Protection Agency Board Appointments. Office of Governor. March 17, 2021. URL: https://www.gov.ca.gov/2021/03/17/california-officials-announce-california-privacy-protection-agency-board-appointments/ (last accessed: 11.05.2021).
107. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: міжнародний договір від 27.06.2014 р. № 984_011. URL: https://zakon.rada.gov.ua/laws/show/984_011 (дата звернення: 11.05.2021).
108. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI у редакції від 01.06.2010 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17/ed20100601#Text (дата звернення: 11.05.2021).
109. Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних: Закон України від 03.07.2013 р. № 383-VII. URL: https://zakon.rada.gov.ua/laws/show/383-18 (дата звернення: 12.05.2021).
110. Про оптимізацію системи центральних органів виконавчої влади: Указ Президента України від 09.12.2010 р. № 1085/2010. URL: https://zakon.rada.gov.ua/laws/show/1085/2010 (дата звернення: 12.05.2021).
111. Про Положення про Державну службу України з питань захисту персональних даних: Указ Президента України від 06.04.2011 р. №

390/2011. URL: https://zakon.rada.gov.ua/laws/show/390/2011 (дата звернення: 12.05.2021).

112. Гнатюк С. Л. Особливості захисту персональних даних у сучасному кіберпросторі: правові та техніко-технологічні аспекти: аналіт. доп. / С. Л. Гнатюк. – К. : НІСД, 2014. – 92 с. – (Сер. «Інформаційні стратегії», вип. 3). URL: https://niss.gov.ua/sites/default/files/2015-01/Druk_Gnatuk1.indd-8b6f2.pdf (дата звернення: 12.05.2021).
113. Мельник О., Ізотов Д. GDPR та Україна: quo vadis?. Юридична Газета. 2018. № 46. URL: https://vkp.ua/publication/gdpr_ta_ukraina_quo_vadis (дата звернення: 11.05.2021).
114. Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних: Закон України від 03.07.2013 р. № 383-VII. URL: https://zakon.rada.gov.ua/laws/show/383-18 (дата звернення: 12.05.2021).
115. Про оптимізацію системи центральних органів виконавчої влади : Постанова Каб. Міністрів України від 10.09.2014 р. № 442 : станом на 20 лют. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/442-2014-п (дата звернення: 12.05.2021).
116. Про затвердження документів у сфері захисту персональних даних: Наказ Уповноваж. Верхов. Ради України з прав людини від 08.01.2014 р. № 1/02-14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14 (дата звернення: 12.05.2021).
117. Роз’яснення та рекомендації. Уповноважений Верховної Ради України з прав людини. URL: https://www.ombudsman.gov.ua/ua/page/zpd/obrobka/roziasnenia-ta-recomendation/ (дата звернення: 12.05.2021).
118. Про Уповноваженого Верховної Ради України з прав людини : Закон України від 23.12.1997 р. № 776/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/776/97-вр (дата звернення: 12.05.2021).

119. Інформація про Департамент у сфері захисту персональних даних. Уповноважений Верховної Ради України з прав людини. URL: https://www.ombudsman.gov.ua/ua/page/zpd/info/ (дата звернення: 12.05.2021).
120. Кодекс України про адміністративні правопорушення (статті 213 - 330): Кодекс України від 07.12.1984 р. № 8073-X. URL: https://zakon.rada.gov.ua/laws/show/80732-10 (дата звернення: 12.05.2021).
121. Кримінальний кодекс України : Кодекс України від 05.04.2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 12.05.2021).
122. Відповідальність за порушення закону про персональні дані. Центр демократії та верховенства права. 3 липня 2012 року. URL: https://cedem.org.ua/news/vidpovidalnist-za-porushennya-zakon-2/ (дата звернення: 12.05.2021).
123. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні: 2020 рік. Уповноважений Верховної Ради України з прав людини. Березень 2021 року. 355 с. URL: https://ombudsman.gov.ua/files/2021/zvit_2020_rik_.pdf (дата звернення: 12.05.2021).
124. Меморандум про співробітництво між Уповноваженим Верховної Ради України з прав людини та Національним Банком України. 5 лютого 2021 року. URL: https://ombudsman.gov.ua/images/2021/february/%D0%9C%D0%B5%D0%BC%D0%BE%D1%80%D0%B0%D0%BD%D0%B4%D1%83%D0%BC_%D0%9D%D0%B0%D1%86%D0%91%D0%B0%D0%BD%D0%BA_2021.pdf (дата звернення: 12.05.2021).
125. Кодекс України про адміністративні правопорушення (статті 1 - 212-24): Кодекс України від 07.12.1984 р. № 8073-X. URL: https://zakon.rada.gov.ua/laws/show/80731-10 (дата звернення: 12.05.2021).

126. Самойленко Ю.С. Адміністративно-правові засоби захисту персональних даних. Юридичний науковий електронний журнал. 2019. № 4. С. 294-297. URL: http://www.lsej.org.ua/6_2019/72.pdf (дата звернення: 12.05.2021).
127. Бем М.В., Городиський І.М. Стандарти захисту персональних даних в соціальній сфері / М. В. Бем,, І. М. Городиський. – Львів: б.в., 2018. - 110 с.
128. Kobrin A., Korchynskyi D., Nekrutenko V. Ukrainian GDPR: The reality and future of privacy legislation in Ukraine. IAPP. September 28, 2020. URL: https://iapp.org/news/a/ukrainian-gdpr-the-reality-and-future-of-privacy-legislation-in-ukraine/ (last accessed: 12.05.2021).
129. Продовжується робота над розробкою нової редакції Закону України «Про захист персональних даних». Уповноважений Верховної Ради України з прав людини. 11 червня 2020 року. URL: https://www.ombudsman.gov.ua/ua/all-news/pr/prodovzhu%D1%94tsya-robota-nad-rozrobkoyu-novo%D1%97-redakcz%D1%96%D1%97-zakonu-ukra%D1%97ni-pro-zaxist-personalnix-danix/ (дата звернення: 12.05.2021).
130. New Draft Law of Ukraine on personal data protection – expert consultations with support of joint EU and CoE project. Council of Europe Office in Ukraine. 20 November 2020. URL: https://www.coe.int/en/web/kyiv/-/new-draft-law-of-ukraine-on-personal-data-protection-expert-consultations-with-support-of-join-eu-and-coe-project (last accessed: 12.05.2021).
131. Sayenko Kharenko. Analysis of Data Privacy Laws and Legislation in Ukraine Final Report (the «Memorandum»). Kyiv, 14 September 2020. URL: https://ecpl.com.ua/wp-content/uploads/2020/09/ENG_09142020-_CEP_Final-Report.pdf (last accessed: 12.05.2021).