Міністерство освіти і науки України
Національний університет «Києво-Могилянська академія»
Факультет правничих наук
Кафедра приватного права

Магістерська робота

освітній ступінь – магістр

на тему: «**ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ЄС Й ОКРЕМИХ КРАЇНАХ-УЧАСНИЦЯХ, США ТА УКРАЇНІ**»

Виконав:
студент 2-го року навчання
спеціальності 081 «Право»
Бартосюк Олександр Валентинович

Керівник:
кандидат юридичних наук, доцент
Смирнова Тетяна Сергіївна

Рецензент:
кандидат юридичних наук, доцент
Цельєв Олексій Вікторович

Магістерська робота захищена з оцінкою
«_____»

Секретар ЕК _____
«____» червня 2020 р.

Київ 2020

ЗМІСТ

ВСТУП……5
РОЗДІЛ 1. ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ЄС……..9
1.1.Аналіз законодавства ЄС у сфері захисту персональних даних…….9
1.1.1.Нормативно-правові акти ЄС у сфері захисту персональних даних…….9
1.1.2.Визначення персональних даних за GDPR……..….10
1.1.3.Принципи регулювання захисту персональних даних відповідно до GDPR..12
1.1.4.Ключові положення GDPR стосовно захисту персональних даних…….16
1.1.5.Випадки застосування штрафних санкцій відповідно до GDPR.……19
1.2.Особливості захисту персональних даних в окремих країнах-учасницях ЄС……22
1.2.1.Особливості регулювання захисту персональних даних у Великобританії.22
1.2.2.Особливості регулювання захисту персональних даних у Німеччині……...25
1.2.3.Особливості регулювання захисту персональних даних у Франції……...27
1.2.4.Особливості регулювання захисту персональних даних в Ірландії……..28
Висновки до розділу 1……...……30
РОЗДІЛ 2. ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У США……..……..32
2.1. Аналіз законодавства США у сфері захисту персональних даних ……..…..32
2.1.1. Нормативно-правові акти США у сфері захисту персональних даних ….32
2.1.2. Перспективи прийняття федерального нормативно-правового акта у сфері захисту персональних даних ……...……..….33
2.1.3. Визначення персональних даних за законодавством США……..35
2.1.4. Ключові положення CCPA стосовно захисту персональних даних …….37
2.2. Особливості регулювання захисту персональних даних California Consumer Privacy Act у порівнянні з General Data Protection Regulation ……44
Висновки до розділу 2……...…54

РОЗДІЛ 3. ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ ……..……..56

3.1. Аналіз українського законодавства у сфері захисту персональних даних та його відповідності нормам General Data Protection Regulation ……..……..56

3.2. Аналіз судової практики стосовно захисту персональних даних та перспективи реформування українського законодавства у сфері захисту персональних даних ……..……68

Висновки до розділу 3……..……..……...…73

ВИСНОВКИ……...……..…….75

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ…….……82

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

GDPR	Загальний регламент про захист персональних даних (англ. «General Data Protection Regulation»)
CCPA	Закон Каліфорнії про захист персональних даних споживачів (англ. «California Consumer Privacy Act»)
ЄРЗД	Європейська рада захисту даних
КУпАП	Кодекс України про адміністративні правопорушення
ЗУ	Закон України

ВСТУП

Актуальність дослідження. У зв'язку із розвитком технологій, питання захисту персональних даних набуває все більшої актуальності. Це відбувається через те, що розвиток технологій та глобалізаційні процеси спричиняють користування більшою кількістю різноманітних сервісів, а користування сервісами - більшу кількість опрацювань персональних даних. У той самий час, оскільки опрацювання здійснюється у набагато більшому обсязі, збільшується кількість порушень при опрацюванні персональних даних, які потенційно можуть спричинити витоки персональних даних та порушення прав людини. Одними з найбільш гучних випадків витоків персональних даних були:

– витік даних Facebook та Cambridge Analytica, що стосується близько 50 000 000 акаунтів [1];

– витік даних Marriott International Inc, що стосується близько 339 000 000 записів гостей з 31 країни [2];

– витік даних British Airways, що стосується близько 500 000 клієнтів [3].

У зв'язку із існуванням зазначених ризиків для суб'єктів персональних даних, держави повинні створити належне та ефективне правове регулювання у сфері захисту персональних даних. Найбільш відомими нормативно-правовими актами, які були прийняті з метою приведення законодавства у відповідність до теперішніх умов опрацювання персональних даних, є GDPR та CCPA.

Оскільки необхідність приведення законодавства у сфері захисту персональних даних у відповідність до сучасних умов розвитку технологій є у всіх країнах (включаючи Україну), а ці нормативно-правові акти слугують орієнтиром для інших країн, є потреба у дослідженні такого регулювання, а також регулювання, яке є наразі в Україні.

У контексті України ця тема є особливо актуальною, оскільки постійно збільшується кількість транскордонних потоків персональних даних між Україною та країнами-учасницями ЄС. Після прийняття GDPR це набуло ще

більшої актуальності, так як однією з особливостей GDPR є його екстериторіальна дія. Іншими словами, GDPR може також застосовуватись до контролерів та операторів, які знаходяться поза межами ЄС.

Таким чином, з метою усунення невідповідності у регулюванні захисту персональних даних, що наразі існує між ЄС та Україною, є потреба у прийнятті оновленого законодавства, яке б відповідало європейським стандартам. З цієї точки зору, є особливо актуальним дослідження провідного світового досвіду, а також відповідності чинного законодавства України до GDPR.

Мета і завдання роботи. Мета цього дослідження полягає у здійсненні системного аналізу та порівнянні нормативно-правового регулювання у сфері захисту персональних даних ЄС, окремих країн-учасниць ЄС, США та України.

Для реалізації цієї мети потрібно вирішити такі завдання:

1) окреслити систему нормативно-правових актів у сфері захисту персональних даних у ЄС, проаналізувати визначення персональних даних у ЄС та здійснити аналіз принципів регулювання захисту персональних даних у ЄС;

2) дослідити ключові положення GDPR стосовно захисту персональних даних та проаналізувати випадки застосування штрафних санкцій за GDPR;

3) окреслити особливості захисту персональних даних у Великобританії, Німеччині, Франції та Ірландії;

4) окреслити систему нормативно-правових актів у сфері захисту персональних даних у США та охарактеризувати потенційні нормативно-правові акти, які б діяли на федеральному рівні;

5) проаналізувати різні варіанти визначень персональних даних (персональної інформації) у США;

6) дослідити ключові положення CCPA стосовно захисту персональних даних й порівняти регулювання захисту персональних даних, яке закріплене GDPR та те, яке закріплене CCPA;

7) дослідити ключові положення українського законодавства у сфері захисту персональних даних, а також порівняти регулювання захисту

персональних даних, яке закріплене ЗУ «Про захист персональних даних» та те, яке закріплене GDPR;

8) здійснити аналіз української судової практики стосовно захисту персональних даних;

9) запропонувати зміни, які потрібно вчинити для належного захисту прав суб'єктів персональних даних в Україні.

Об'єктом дослідження є правовідносини у сфері захисту персональних даних.

Предметом дослідження є норми права у сфері захисту персональних даних у ЄС, окремих країнах-учасницях ЄС, США та Україні; практика застосування таких норм права у ЄС та Україні; статті від фахівців у сфері захисту персональних даних; наукові джерела; рекомендації щодо застосування законодавства у сфері захисту персональних даних.

Методи дослідження. У дослідженні використовуються як загальнонаукові, так і спеціально-наукові методи. Зокрема, було використано діалектичний метод, аналітичний метод, герменевтичний метод, формально-юридичний метод, порівняльно-правовий метод.

Діалектичний метод дозволив дослідити особливості захисту персональних даних в ЄС, окремих країнах-учасницях ЄС, США та Україні та став основою здійснення цього дослідження.

Аналітичний метод допоміг у розробці концепції здійснення дослідження, а також у збиранні, систематизації, обробці та використанні інформації.

Герменевтичний та формально-юридичний метод проявляється у тлумаченні положень нормативно-правових актів ЄС, окремих країн-учасниць ЄС, США та України та практики застосування таких нормативно-правових актів.

За допомогою порівняльно-правового методу було здійснено порівняння положень GPDR та CCPA, а також ЗУ «Про захист персональних даних» та GDPR.

Теоретичну основу дослідження склали праці таких українських та іноземних правників: М.І. Козюбра, Т. Хікман, Д. Габель, С. Хеун, С. Ассіон, В. Гренценберг, Я. Шпіттка, Н. Пуртова, Аксель Фон Вальтер, Д. Лібо-Маріанна, К. Шансе, Б. Портьє, Ж. Реверсак, М. Шмідл, Шон Марі Бойн, Л. Сотто, А. Сімпсон, С. Маллиган, К. Лінебо, В. Фріман, С. Чабінські, П. Пітман, П. Шварц, Д. Солов, М.О. Кравець, В. Головченко, Б. Юнсал, К. О'Коннор та інших.

Наукове та практичне значення дослідження. Теоретичні напрацювання, які розроблені у цій магістерській роботі, можуть бути використані у наукових, законотворчих та навчальних цілях. Зокрема, вони можуть бути використані при: (1) дослідженні регулювання захисту персональних даних у майбутньому, (2) оновленні українського законодавства до сучасних тенденцій та приведенні його у відповідність до положень GDPR, (3) навчанні студентів у вищих навчальних закладах.

Структура роботи. Магістерська робота складається із вступу, трьох розділів, шести підрозділів, тринадцяти частин підрозділів, висновків у кінці кожного розділу, загальних висновків та списку використаних джерел. Загальний обсяг дослідження - 96 сторінок, у тому числі список використаних джерел (130 найменувань) складає 15 сторінок.

РОЗДІЛ 1. ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ЄС

1.1. Аналіз законодавства ЄС у сфері захисту персональних даних

1.1.1. Нормативно-правові акти ЄС у сфері захисту персональних даних

Регулювання в ЄС у сфері захисту персональних даних поділяється на національне та те, яке поширюється на всі країни-учасниці ЄС [4]. При цьому, при застосуванні нормативно-правових актів діє принцип пріоритетності права ЄС [5].

Принцип пріоритетності права ЄС означає те, що нормативно-правові акти ЄС мають перевагу над національними актами окремих країн-учасниць ЄС. Це базовий принцип, який, хоч і не встановлений в угодах ЄС, але був закріплений Судом ЄС, зокрема у справі Flaminio Costa v E.N.E.L. (1964). У рішенні від 15 липня 1964 року за результатом розгляду справи стверджується, що «у випадку суперечності норми окремої країни нормі права ЄС, країни-учасниці ЄС зобов'язані застосовувати норму права ЄС».[1] Разом з цим, те, чи була норма національного права прийнята до чи після норми права ЄС, не має правового значення [5; 6].

Враховуючи вищевикладене, можна стверджувати, що регулювання захисту персональних даних в ЄС є різноманітним та ускладненим, оскільки країни-учасниці ЄС мають своє національне законодавство. Окрім цього, також існує регулювання ЄС, яке має пріоритетність над національними нормативно-правовими актами країн-учасниць ЄС.

Цікаво, що окрім прагнення країн-учасниць ЄС уніфікувати законодавство та затвердити єдине надрегулювання у сфері захисту персональних даних, яке б встановлювало єдині мінімальні стандарти, бажання щодо створення єдиного

[1] Тут і надалі переклад іноземної літератури та нормативних джерел здійснений мною, Бартосюком О.В.

регулювання також є у жителів ЄС, а саме близько 90% населення стверджують те, що вони хотіли б мати однакове регулювання у сфері захисту персональних даних всередині ЄС незалежно від того, де ці дані опрацьовуються [7].

До 25 травня 2018 року, в якості єдиного надрегулювання захисту персональних даних в ЄС, діяла Директива 95/46/ЕС, яка, відповідно до статті 94 GDPR, з цієї дати втратила чинність та була замінена GDPR [8, с. 96]. Окрім того, що змінився зміст регулювання захисту персональних даних, зазначені нормативно-правові акти мають різну юридичну силу. Директиви лише встановлюють певні результати, які повинні бути досягнуті країнами-учасницями ЄС, а шлях досягнення та імплементація визначаються самими країнами [9]. У той самий час, GDPR за своєю юридичною природою є регламентом (англ. «regulation») [8; 10]. Регламенти є обов'язковими для усіх країн-учасниць ЄС без додаткової імплементації у національне законодавство [9]. Таким чином, GDPR не потребує подальшої імплементації країнами-учасницями ЄС і автоматично зменшує рівень їх дискреції щодо виконання GDPR у порівнянні з Директивою 95/46/ЕС, яка діяла до прийняття GDPR.

1.1.2. Визначення персональних даних за GDPR

Визначення персональних даних прямо закріплено в пункті 1 статті 4 GDPR. За своїм змістом, це визначення складається з двох частин - визначення що таке власне персональні дані та хто є фізичною особою, яку можна ідентифікувати. Відповідно до зазначеної статті GDPR, персональними даними є будь-яка інформація, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати. У той же час, фізична особа є такою, якщо її можна прямо або опосередковано ідентифікувати за такими критеріями, як ім'я, ідентифікаційний код, 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 [8, с. 40].

Таким чином, як випливає із зазначеного визначення, не існує виключного переліку що є персональними даними, а що не є ними. Досить часто той факт, чи є та чи інша інформація персональними даними, залежить від контексту та обставин, за яких персональні дані збираються. Наприклад, для багатьох людей є очевидним те, що ім'я певної фізичної особи є її персональними даними. Разом з тим, це не завжди так. Саме по собі ім'я фізичної особи не є персональними даними, оскільки є багато інших осіб з таким ж ім'ям. Якщо ж оцінювати ім'я поруч з іншою інформацією про цю фізичну особу, на кшталт адреси та номеру телефону, то тоді такий обсяг інформації може бути достатнім для ідентифікації конкретної особи та, відповідно, є персональними даними такої фізичної особи [11].

Отже, до поняття персональних даних відноситься інформація, що стосується фізичних осіб, які (1) можуть бути ідентифіковані безпосередньо з відповідної інформації або (2) можуть бути непрямо ідентифіковані з відповідної інформації у поєднанні з іншими даними [12]. Варто зазначити, що персональні дані, які були знеособлені, зашифровані або псевдонімізовані, але можуть бути використані для повторної ідентифікації особи, залишаються персональними даними у відповідності із GDPR. Разом з тим, якщо дані є анонімізованими у такий спосіб, що особа більше не може бути ідентифікованою, такі дані не вважаються персональними. Також необхідно враховувати, що GDPR захищає персональні дані незалежно від технологій та способів їх опрацювання [13].

Незважаючи на досить розгорнуте визначення персональних даних у статті 4 GDPR, воно більш деталізоване у пункті 26 декларативної частини GDPR. Відповідно до цього пункту, використання псевдоніму разом із додатковою інформацією також може вважатись персональними даними, а для визначення ймовірності ідентифікації особи необхідно брати до уваги витрати та період часу, які необхідні для такої ідентифікації, а також наявні технології, які використовуються з цією метою [8, с. 6].

Проаналізувавши вищевикладене, можна стверджувати, що визначення факту, чи є певний перелік даних персональними даними, можливе лише на

підставі індивідуального аналізу та аналізу, який базується на конкретному контексті [14, с. 44].

1.1.3. Принципи регулювання захисту персональних даних відповідно до GDPR

З метою визначення того, чи змінилось стратегічне бачення сфери захисту персональних даних у ЄС із прийняттям GDPR, слід проаналізувати те, чи змінились принципи у цій сфері. Під принципами маються на увазі «найбільш загальні і стабільні вимоги, що уособлюють суспільні цінності, дозволяють відтворити їх при формуванні та дії права, визначаючи його характер і напрями подальшого розвитку» [15, с. 70].

Принципи стосовно опрацювання персональних даних встановлені у статті 5 GDPR. Такими принципами є: законність, правомірність та прозорість; цільове обмеження; мінімізація даних; точність; обмеження зберігання; цілісність і конфіденційність; підзвітність [8, с. 42-43].

Принцип законності, правомірності та прозорості визначає, що (1) опрацювання персональних даних повинно здійснюватися лише у разі відповідності вимогам GDPR та іншого законодавства; (2) при опрацюванні персональних даних усі дії мають здійснюватися у той спосіб, як було повідомлено суб'єкту персональних даних; (3) суб'єкти персональних даних повинні знати яким чином та з якою метою опрацьовуються персональні дані, а також як їх персональні дані будуть використані у майбутньому [16; 17].

Тим не менш, незважаючи на те, що порушення законодавства при опрацюванні персональних даних, яке не стосується їх захисту (наприклад, законодавства у сфері захисту авторських прав), може свідчити про порушення цього принципу, регулятори не можуть накладати штрафи у такому випадку, незважаючи на те, що порушено принцип законності, який встановлений GDPR [18].

Для оцінки дотримання принципу правомірності, необхідно проаналізувати як опрацювання впливає на права та інтереси заінтересованих осіб. Якщо інформація була отримана та використана правомірно стосовно більшості фізичних осіб, але, у той самий час, неправомірно стосовно однієї особи, таке опрацювання не може вважатись правомірним в цілому. При цьому, іноді можуть виникати ситуації, коли опрацювання персональних даних може негативно впливати на особу, але бути одночасно правомірним (наприклад, при накладенні штрафу у зв'язку з порушенням правил дорожнього руху) [18].

Порівняно із Директивою 95/46/ЕС, до цього принципу додалась ознака «прозорості». Таким чином, при опрацюванні персональних даних на контролерів та операторів покладаються додаткові обов’язки щодо повідомлення суб'єктів персональних даних стосовно здійснюваного опрацювання [17; 19].

Принцип прозорості втілений у конкретних вимогах до операторів та контролерів, які визначені в статтях 12-22 GDPR [8, с. 47-54]. Однією із складових цього принципу є обов'язок здійснення взаємодії із суб'єктами персональних даних стисло, прозоро, зрозуміло та доступно. Іншими словами, інформація не повинна містити «надмірно юридичної, технічної чи спеціалізованої мови або термінології» [20]. Для кращого розуміння що таке зрозуміла мова, Європейською Комісією було видано посібник «Як писати зрозуміло» [21].

Принцип цільового обмеження встановлює те, що опрацювання персональних даних може мати місце лише у випадку наявності конкретних, чітко визначених та законних цілей, про які повинно бути повідомлено суб'єкту персональних даних. Персональні дані можуть збиратись та використовуватись лише для виконання тих цілей, на виконання яких такі дані були передані та щодо яких було надано згоду суб'єктом персональних даних. Разом з тим, якщо контролер або оператор матимуть бажання здійснити опрацювання зібраних персональних даних в інший спосіб, ніж в який було повідомлено, таке опрацювання повинно здійснюватися у межах раніше задекларованих цілей, про що також повинно бути повідомлено суб'єкту персональних даних [16; 17].

В цілому, цей принцип майже не зазнав змін у порівнянні з формулюванням, яке було встановлене у Директиві 95/46/ЕС. Разом з тим, у GDPR додається важлива деталь у вигляді відсилки до статті 89 GDPR, яка більш детально описує особливості при зберіганні персональних даних в інтересах суспільства, наукових чи історичних досліджень, а також статистичних цілей, а саме використання псевдонімів або інших способів, що дозволяють виключити ідентифікацію суб'єктів персональних даних [8, с. 94; 19].

Під мінімізацією даних мається на увазі те, що персональні дані повинні збиратись в мінімально можливому обсязі, який необхідний для виконання задекларованих цілей [17]. Зібрані персональні дані повинні бути «достатніми, релевантними, а також необхідними, відповідно до цілей опрацювання» [16].

Як і принцип цільового обмеження, принцип мінімізації даних також не зазнав значних змін. Формулювання щодо стандарту зібрання персональних даних «not excessive» було замінене на «limited to what is necessary». Таке формулювання є більш суворим, адже встановлює вищий стандарт щодо кількості зібраних даних для операторів та контролерів [19].

Принцип точності означає те, що зібрані персональні дані повинні відповідати сучасному стану речей та, у випадку невідповідності, бути оновленими [17]. Контролер або оператор не мають зберігати «застарілі та неактуальні дані, а також зобов'язані забезпечити стирання неточних персональних даних без будь-якої затримки» [16].

Принцип обмеження зберігання означає те, що персональні дані повинні зберігатись лише протягом визначеного терміну, а після його спливу стиратись. Відповідно, оператор та контролер повинні визначити період зберігання персональних даних та мати змогу обґрунтувати, що цей час є необхідним для виконання задекларованих цілей. Разом з тим, існують виключення щодо періоду зберігання персональних даних. Зокрема, дозволяється зберігати персональні дані й після закінчення визначеного строку якщо це необхідно здійснити в інтересах суспільства, наукових чи історичних досліджень, а також статистичних цілей [16; 17].

Порівняно із Директивою 95/46/ЕС, із набранням чинності GDPR потрібно враховувати два нових фактори. По-перше, регулювання подальшого зберігання в інтересах суспільства, наукових чи історичних досліджень уточнене статтею 89 GDPR, про яку було зазначено вище при описі принципу цільового обмеження. По-друге, принцип обмеження потрібно сприймати у контексті права бути забутим, яке детально врегульоване статтею 17 GDPR. Згідно з цим правом, контролер може бути зобов'язаний здійснити стирання персональних даних раніше, ніж у строк, який був ним визначений [8, с. 43, 51; 19].

Принцип цілісності та конфіденційності. Відповідно до пункту (f) частини 1 статті 5 GDPR, при опрацюванні персональних даних, оператор та контролер зобов'язані забезпечити належну безпеку, у тому числі проти несанкціонованого чи незаконного опрацювання та проти ненавмисної втрати, знищення чи завдання шкоди [8, с. 43]. Безпечне опрацювання персональних даних повинно бути здійснено за допомогою відповідних організаційних (розробка внутрішніх процедур, інструкцій тощо) й технічних (створення резервних копій, здійснення шифрування, псевдонімізації тощо) заходів [17].

Принцип підзвітності, відповідно до GDPR, вимагає здійснення документації усіх політик, що регулюють збір та опрацювання персональних даних. Крім дотримання принципів опрацювання персональних даних, контролер та оператор також можуть бути зобов'язані відповідними органами влади продемонструвати яким чином зазначені принципи дотримуються [16]. Демонстрація може бути здійснена різними шляхами, зокрема, але не виключно, призначенням посадової особи із захисту персональних даних, складанням внутрішніх інструкцій щодо захисту персональних даних, навчанням персоналу, наданням чіткої інформації суб'єктам персональних даних тощо [17].

Проаналізувавши вищезазначене, крізь призму проаналізованих принципів, можна зробити висновок, що стратегічне бачення у сфері захисту персональних даних в ЄС з прийняттям GDPR та порівняно із Директивою 95/46/ЕС, радикальним чином не змінилось. Також слід зазначити, що зміст

принципів точності й цілісності та конфіденційності не зазнали жодних змін за своєю суттю у порівнянні з Директивою 95/46/ЕС [19].

1.1.4. Ключові положення GDPR стосовно захисту персональних даних

У першу чергу, суб'єкт господарювання, при приведенні своєї діяльності у відповідність до GDPR, повинен з'ясувати чи здійснюється опрацювання персональних даних законно. Про законне опрацювання персональних даних у тексті GDPR вказано неодноразово - зокрема у пункті 40 декларативної частини, а також більш детально у статті 6 GDPR [8, с. 9, 43, 44].

Опрацювання персональних даних є законним, якщо дотримана одна з таких умов: наявність згоди суб'єкта персональних даних; необхідність опрацювання у зв'язку із виконанням договірних зобов'язань (де стороною договору є суб'єкт персональних даних); необхідність опрацювання у зв'язку із виконанням законної вимоги; необхідність опрацювання у зв'язку із захищенням життєво важливих інтересів; необхідність здійснення опрацювання для забезпечення суспільних інтересів; необхідність здійснення опрацювання для цілей законних інтересів контролера або третьої особи, але лише коли такі інтереси не стоять вище за фундаментальні права та свободи суб'єкта персональних даних [8, с. 43; 22, с. 8].

Стосовно наявності згоди суб'єкта персональних даних, суб'єкту господарювання потрібно враховувати, що така згода повинна відповідати певним критеріям. Зокрема, «згода повинна бути вільно наданою, конкретною, інформованою, однозначною та повинна бути отримана шляхом відповіді на запит на таку згоду від контролера, який був би написаний зрозумілою мовою». Окрім відповіді на такий запит, згода може бути також надана стверджувальним актом, наприклад, встановленням «прапорця» в мережі інтернет або підписанням певної форми. Також існують спеціальні правила щодо отримання згоди на опрацювання персональних даних стосовно дитини - у такому випадку повинна бути отримана згода батьків [22, с. 9].

У випадку, якщо стало зрозуміло, що GDPR застосовується до конкретного суб'єкта господарювання, то необхідно встановити яку функцію такий суб'єкт господарювання виконує. Відповідно до норм GDPR, є контролер та оператор, які виконують різні функції [22, с. 9].

Контролер лише визначає цілі та засоби здійснення опрацювання персональних даних, а оператор здійснює опрацювання від імені контролера [22, с. 9]. Наприклад, якщо компанія, яка здійснює продаж віджетів, використовує послуги компанії з автоматизації електронної пошти задля надіслання листів електронною поштою споживачам від свого імені та для відслідковування їх активності, то у цьому випадку компанія, яка здійснює продаж віджетів - контролер персональних даних, а компанія з автоматизації електронної пошти - оператор персональних даних [23].

GDPR встановлює перелік зобов'язань, які повинні бути виконані контролером та оператором персональних даних. Одними з найбільш важливих зобов'язань є: надавати прозору інформацію; забезпечити право на доступ а також портативність даних; забезпечити право бути забутим; забезпечити право на виправлення та право на заперечення [22, с. 10-12].

Інформація повинна надаватись прозоро щонайменше стосовно: інформації про того, хто здійснює опрацювання персональних даних; причини (цілі) такого опрацювання; нормативну підставу опрацювання; інформацію про того, хто буде отримувати персональні дані. У певних випадках може вимагатись також інша інформація для надання, на кшталт контактних даних посадової особи із захисту персональних даних, термін зберігання персональних даних тощо [22, с. 10].

Під правом на доступ розуміється «право отримувати копію персональних даних, які опрацьовуються, а також іншу додаткову інформацію». Це право необхідно забезпечувати для того, щоб суб'єкт персональних даних «розумів як і чому певний суб'єкт господарювання опрацьовує персональні дані, а також щоб він міг перевірити чи здійснюється опрацювання законно» [24].

Разом з тим, GDPR не визначає у якій формі може здійснюватися запит на надання інформації. Таким чином, з прийняттям GDPR застосовується спрощена процедура надсилання такого запиту. Зокрема, такий запит може бути надісланий у будь-якій формі та будь-якій частині організації, а також не повинен обов'язково містити слова «запит на доступ до інформації» [24].

Щодо права на портативність даних, слід зазначити, що обов'язок забезпечити це право покладається на контролера лише у випадку наявності таких законних підстав для опрацювання персональних даних як отримання згоди, виконання договору, а також у випадку здійснення опрацювання автоматизованими засобами. Зазначене право означає можливість суб'єкта персональних даних «отримувати персональні дані, які опрацьовуються, у структурованому, загальновживаному та машиночитаному форматі». Більш того, суб'єкт персональних даних може вимагати передання його зібраних персональних даних іншому контролеру [25].

Під машиночитаним форматом мається на увазі формат, який може бути автоматично зчитаний комп'ютером та опрацьований на ньому. Щодо конкретних найменувань форматів, то йде мова про CSV, JSON, XML та інші формати, які відповідають зазначеним критеріям [26].

Застосовуючи право бути забутим, суб'єкти персональних даних можуть вимагати видалення таких даних. Разом з тим, це право є обмежене та застосовується у виключних випадках, а саме коли: персональні дані більше непотрібні для виконання цілей; суб'єкт персональних даних відізвав згоду на опрацювання; «забуття» є необхідним для виконання певного обов'язку тощо [27].

У той самий час, по відношенню до IT-бізнесу є питання стосовно того, чи необхідно видаляти персональні дані з резервних систем при застосуванні права на забуття. Загалом, це необхідно робити також щодо резервних систем. Тим не менш, у випадку періодичного перезапису та оновлення резервної системи, персональні дані можуть зберігатись до відповідного перезапису або оновлення.

Головне, щоб такі персональні дані не використовувались у відповідний проміжок часу щодо інших цілей, окрім резервного копіювання [27].

GDPR не встановлює вимогу стосовно форми запиту на видалення персональних даних [27]. Разом з тим, вважається за доцільне зберігати структуру із зазначенням інформації про особу, яка подає запит; інформації стосовно суб'єкта персональних даних; причин видалення даних; опису даних, які повинні бути видалені; а також інших деталей [28].

Під змістом права на виправлення, окрім власне виправлення персональних даних, мається також на увазі також можливість доповнення неповних даних. За своєю суттю, забезпечення цього права має тісний зв'язок із принципом точності, про який було зазначено вище [29].

Право на заперечення опрацювання персональних даних означає можливість суб'єкту персональних даних зупиняти або перешкоджати опрацюванню у будь-який час [30]. Таке право у суб'єкта персональних даних виникає у випадку здійснення прямого маркетингу, опрацювання персональних даних для статистичних цілей, публічних інтересів тощо [31]. Також необхідно зазначити, що онлайн сервіси зобов'язані надавати автоматичний спосіб подання заперечення на опрацювання персональних даних [32, с. 1].

1.1.5. Випадки застосування штрафних санкцій відповідно до GDPR

В загальному, більшість штрафних санкцій, які накладались на суб'єктів господарювання, були порівняно незначними та менші, аніж 10 000 євро. Разом з тим, були також випадки накладання штрафів зовсім іншого масштабу [33].

У Німеччині Федеральний уповноважений із захисту даних та свободи інформації (скор. «BfDI») наклав штраф на 1&1 Telecom GmbH у розмірі 9 550 000 євро за порушення статті 32 GDPR, а саме за те, що не були достатньою мірою забезпечені технічні та організаційні заходи з метою забезпечення безпеки інформації [33]. Суть порушення зводиться до того, що особи, які телефонували на службу обслуговування клієнтів компанії, могли отримати вичерпні

персональні дані надавши лише у якості аутентифікації ім'я та дату народження клієнта [34].

Така сума була визначена відповідно до моделі штрафів, згідно з якою визначається «денна ставка», яка повинна виходити зі світового річного обороту відповідної групи компаній. Як наслідок, «денна ставка» є основою для вирахування розміру штрафу. Така модель призводить до того, що навіть незначні порушення з боку великих компаній можуть призвести до великих штрафів, що й сталось у випадку з 1&1 Telecom GmbH [35].

Незважаючи на те, що після накладення штрафу 1&1 Telecom GmbH активно співпрацює з регулятором у сфері захисту персональних даних [34], компанія буде оскаржувати зазначене рішення в суді. В цілому, будуть використовуватись два основні аргументи - (1) такий вид аутентифікації був звичайним на ринку у момент накладення штрафу та (2) розмір штрафу є непропорційним до вчиненого порушення [35].

Це не єдиний випадок накладення штрафу у великому розмірі німецьким регулятором. У жовтні 2019 року Органом із захисту даних у місті Берлін було накладено штраф у розмірі 14 500 000 євро, який на початку розгляду становив суму у розмірі 28 000 000 євро [36]. Цей штраф було накладено на компанію Deutsche Wohnen SE за порушення комплаєнсу із принципами опрацювання персональних даних, про які було зазначено вище [33].

Компанія у сфері нерухомості Deutsche Wohnen SE використовувала систему, що не передбачала можливість видалення персональних даних, які більше не є потрібними. Під час перевірки було також виявлено, що зберігались дані, які навіть не були потрібні для первісного збору, зокрема інформація про особисті та фінансові умови орендарів на кшталт оплати праці, виписок з трудових та навчальних договорів, податкових даних, даних соціального й медичного страхування та банківських виписок [37; 38].

Найбільші штрафи у сфері захисту персональних даних у ЄС накладає британський Інформаційний комісар. Зокрема 08 та 09 липня 2019 року було висловлено намір накласти два штрафи загальною сумою 314 990 200 євро на

компанії Marriott International Inc та British Airways за порушення 32 статті GDPR, а саме за те, що не були достатньою мірою забезпечені технічні та організаційні заходи з метою забезпечення безпеки інформації [33].

Стосовно Marriott International Inc (компанія, яка займається франчайзингом готелів [39]), намір накласти штраф був висловлений за витік близько 339 000 000 записів гостей з 31 країн, який відбувся у листопаді 2018 року [2]. Стосовно ж British Airways (британська авіакомпанія [40]), то такий намір був висловлений через те, що користувачі офіційного веб-сайту авіакомпанії перенаправлялись на веб-сайт шахраїв, які в результаті зібрали персональні дані про більш ніж 500 000 клієнтів [3]. Разом з тим, станом на лютий 2020 року, фактично штраф ще не накладений, оскільки між регулятором та компаніями є угода стосовно продовження регуляторного процесу до 31 березня 2020 року [41].

Найбільшою накладеною санкцією за порушення норм GDPR станом на лютий 2020 року є штраф Національної комісії з питань регулювання інформаційних технологій та прав людини Франції у розмірі 50 000 000 євро на Google LLC [42]. Порушення полягало у складності пошуку інформації стосовно мети збору даних та строків зберігання, а також відомостей про те, яка інформація використовується для налаштування рекламних оголошень. Також користувачі не могли обирати таргетинг на рекламні повідомлення, а був лише один вихід - погоджуватись з політикою конфіденційності Google [43].

Слід зазначити, що штрафи накладаються не лише на приватних суб'єктів господарювання. Зокрема, Комісія із захисту даних Болгарії наклала штраф у розмірі 2 600 000 євро на Орган державних доходів, що є державною установою [33; 44]. Цей штраф був накладений через масштабний витік даних, внаслідок якого стали доступні податкові записи майже всіх дорослих громадян країни [45].

Також необхідно враховувати, що штрафи можуть накладатись не лише на юридичних, а й на фізичних осіб. Зокрема, іспанським регулятором було накладено штраф на фізичну особу у розмірі 10 000 євро за поширення інтимних

фотографій та знімків екрану приватних повідомлень з мобільного додатку WhatsApp без відома цієї особи. Регулятор визначив такі дії як порушення статті 6.1 (a) GDPR, оскільки особою не була надана згода для опрацювання персональних даних [8, с. 43; 46, с. 1, 7].

Якщо проаналізувати випадки застосування санкцій регуляторами різних країн-учасниць ЄС, то слід зазначити, що станом на лютий 2020 року найбільш активним регулятором є іспанський. Тим не менш, максимальний розмір штрафу, який був накладений, становить 250 000 євро, що є незначною сумою у порівнянні з іншими країнами-учасницями ЄС [33].

На початку 2020 року з'явились дискусії щодо можливості персональної відповідальності посадової особи із захисту персональних даних за порушення норм GDPR [47]. Такі дискусії виникли через накладення штрафу на посадову особу із захисту персональних даних Судом східного округу Сеулу в Південній Кореї у розмірі 8 500 доларів США. Причиною накладення штрафу є нездатність посадової особи із захисту персональних даних запобігти витоку персональних даних 465 000 клієнтів та 29 000 співробітників туристичного агентства [48].

Тим не менш, у тексті GDPR нічого не зазначено стосовно персональної відповідальності посадових осіб із захисту персональних даних [8]. Зокрема, статтею 39 GDPR закріплюються завдання такої посадової особи, але без встановлення персональної відповідальності [8, с. 64; 47].

1.2. Особливості захисту персональних даних в окремих країнах-учасницях ЄС

1.2.1. Особливості регулювання захисту персональних даних у Великобританії

Слід зазначити, що у 2020 році Великобританія вийшла з ЄС, тому GDPR у майбутньому буде діяти лише через призму застосування територіальної сфери

дії, яка буде більш детально описана у третьому розділі цієї магістерської роботи [8, с. 39; 49].

Станом на час написання цієї магістерської роботи, окрім GDPR, у Великобританії діє також Закон про захист даних 2018 року. Цей закон є національним актом та був прийнятий у квітні 2016 року, а набув чинності у той ж день, що й GDPR - 25 травня 2018 року. Слід зазначити, що, не дивлячись на вихід Великобританії з ЄС, GDPR все ще буде діяти у перехідний період - до 31 грудня 2020 року [50]. За своєю суттю, Закон про захист даних 2018 року доповнює GDPR й адаптує регулювання ЄС з певними національними особливостями [51].

Додатково до GDPR, Закон про захист даних 2018 року регулює опрацювання персональних даних у сферах імміграції громадян країн, які не є учасницями ЄС; кримінального правозастосування; а також діяльності розвідувальних служб та національної безпеки [52]. Разом з вказаними значними змінами, закон також впроваджує менш значні зміни у порівнянні з GDPR. Зокрема, є зміни щодо віку надання згоди дитиною: якщо у GDPR зазначено, що дитина має право надати згоду на опрацювання персональних даних з 16 років, то закон встановлює мінімально можливий вік на рівні 13 років [53].

Більш того, закон вводить концепцію ігнорування прав суб'єктів персональних даних. У той час, коли, відповідно до GDPR, всі суб'єкти персональних даних мають певний перелік прав, закон дозволяє ігнорувати ці права, якщо дотримання цих прав серйозно «вплине на здатність організації виконувати свої функції під час опрацювання даних для наукових, історичних, статистичних та архівних цілей» [53].

Рівень відповідності Закону про захист даних 2018 року GDPR є особливо актуальним у контексті виходу Великобританії з ЄС. Це пояснюється тим, що якщо країна є учасницею ЄС, то персональні дані у такому випадку можуть передаватись вільно та без будь-яких обмежень, що значно полегшує ведення підприємницької діяльності. Якщо ж країна не є учасницею ЄС, то така країна

повинна забезпечити належний рівень захисту у відповідності до статті 45 регламенту [8, с. 69; 53].

Як вже було зазначено, GDPR буде діяти у перехідний період до 31 грудня 2020 року [50]. Однак оцінка відповідності законодавства Великобританії у сфері захисту персональних даних вимогам законодавства ЄС, у відповідності із статтею 45 GDPR, протягом перехідного періоду не є доцільною, у зв'язку із чинністю норм права ЄС у Великобританії. Таким чином, протягом перехідного періоду у Великобританії не буде визначеності стосовно рівня відповідності захисту персональних даних нормам ЄС [54].

Стан невизначеності посилюється у зв'язку з рішенням Європейського суду з прав людини від 2018 року Big brother watch and others v. the United Kingdom, яким було визнано той факт, що Великобританія порушила права людини при запровадженні системи масового спостереження [54; 55]. У цій справі розглядались такі аспекти спостереження, як перехоплення комунікацій, обмін даними з іншими державами та отримання даних від постачальників послуг зв'язку [55; 56]. При цьому, суд визнав, що було порушення прецедентів, сформовані усталеною судовою практикою за статтею 8 та статті 10 Конвенції про захист прав людини і основоположних свобод (право на повагу до приватного і сімейного життя та свобода вираження поглядів відповідно [57]) у випадку перехоплення комунікацій та отримання даних від постачальників послуг зв'язку. У той самий час, Європейський суд з прав людини не визнав порушення статей 8 та 10 у випадку обміну даних з іншими державами [55; 56].

Наразі Європейською Комісією було визнано такі країни, що мають належний рівень захисту персональних даних: Андорра, Аргентина, Канада (лише комерційні організації), Фарерські острови, Гернсі, Ізраїль, Острів Мен, Джерсі, Нова Зеландія, Швейцарія, Уругвай та Японія [58; 59].

Окрім вищезазначених актів, захист персональних даних у Великобританії також регулюється Положенням про конфіденційність та електронні комунікації 2003 року (скор. «PECR») [60]. Це положення походить від європейської Директиви про конфіденційність 2002/58/ЕС. Воно застосовується у сферах

маркетингу через електронні засоби; використання файлів cookie; безпеки публічних електронних засобів зв'язку; та конфіденційності клієнтів, які використовують комунікаційні мережі, послуги щодо даних про трафік, місцеположення, деталізовані рахунки тощо [61].

1.2.2. Особливості регулювання захисту персональних даних у Німеччині

Не беручи до уваги вихід з ЄС, у Німеччині регулювання захисту персональних даних є подібним до того, яке є у Великобританії. 05 липня 2017 року був опублікований, а разом з GDPR, 25 травня 2018 року, набрав чинності Німецький Федеральний закон про захист даних (нім. «Bundesdatenschutzgesetz») [62]. Цей закон замінює інший закон, який регулював захист персональних даних протягом останніх 40 років. Закон у першу чергу відрізняється від GDPR положеннями про посадову особу з захисту персональних даних, штрафами та нематеріальними збитками. Цікаво, що Німеччина це перша країна серед країн-учасниць ЄС, яка прийняла національне законодавство, яке б імплементувало норми GDPR [63].

Закон встановлює більш жорсткі умови щодо застосування обов'язку призначити посадову особу із захисту персональних даних. Така посадова особа призначається зокрема у разі, якщо організація має «щонайменше десять працівників, які працюють із автоматичним опрацюванням персональних даних» [63]. У той самий час, у статті 37 GDPR вказані більш загальні умови обов'язкового призначення такої посадової особи та без конкретної мінімальної кількості найманих працівників [8, с. 63].

Також закон встановлює штрафи у розмірі до 50 000 євро за дії, які порушують закон, але не порушують норми GDPR. У випадку ж порушення норми, яка встановлена в законі, але є також є у GDPR, буде застосовуватись розмір штрафів, який зазначений у GDPR [63].

Значною новелою, у порівнянні з GDPR, є запровадження інституту нематеріальних збитків (моральної шкоди), тобто збитків, які не піддаються

кількісній оцінці або оцінці в грошах (наприклад, страждання). Це може спричинити додаткові збитки для німецьких компаній, які не привели свою діяльність у відповідність із законодавством у сфері захисту персональних даних [63].

Окрім вказаного, німецький закон приділяє значну увагу системам відео нагляду в публічних місцях. Законом визначено, що такий нагляд є допустимим лише для (1) виконання своїх функцій органами державної влади, (2) визначення того, чи потрібно надавати певний доступ, (3) захисту законних інтересів. При цьому, Федеральний адміністративний суд Німеччини своїм рішенням 27 березня 2019 року постановив, що відеоспостереження, яке здійснюється особами приватного сектору, регулюється статтею 6 GDPR, а не більш послабленими нормами німецького закону, оскільки ці норми є несумісними із GDPR, а саме статтею 6.1 (f) [8, с. 43; 64; 65]. Відповідне послаблення у регулюванні здійснення відео нагляду було запроваджене у зв'язку із терористичними актами та іншими подіями, незважаючи на те, що така міра критикувалась, оскільки запровадження цих норм призведе до «надмірного нагляду» [64].

Варто зазначити, що німецький закон не знижує мінімальний вік надання згоди дитиною на опрацювання персональних даних на відміну від британського національного закону, хоча GDPR дозволяє це робити, відповідно до статті 8 [66, с. 5].

Окрім вказаного закону, 27 червня 2019 року німецьким парламентом також було прийнято Другий закон про адаптацію GDPR, який в загальному вносить зміни до 154 федеральних законів [64].

У листопаді 2019 році незалежні німецькі федеральні та державні органи нагляду за захистом персональних даних опублікували звіт про досвід, який був накопичений при впровадженні норм GDPR. З-поміж іншого, у звіті було зазначено, що прийняття GDPR позитивно вплинуло на обізнаність жителів ЄС стосовно законодавства у сфері захисту персональних даних. Крім цього, регуляторам було надано більше повноважень при виконанні поставлених

завдань. Разом з тим, у звіті констатуються також і проблеми та пропонуються зміни до дев'яти сфер регулювання GDPR [67; 68, с. 4, 5].

Як і Великобританія, Німеччина також прийняла законодавчий акт, який імплементує Директиву 2002/58/ЕС - Федеральний акт про електрозв'язок (нім. «Telekommunikationsqesetz») [69].

1.2.3. Особливості регулювання захисту персональних даних у Франції

Як й інші члени-учасниці ЄС, Франція також оновила внутрішнє законодавство у відповідність до GDPR. Зокрема, був оновлений Закон про інформаційні технології, дані та громадянські свободи № 78-17 від 1978 року, шляхом прийняття Закону про захист персональних даних № 2018-493 від 2018 року. Також був виданий указ № 2018-1125 від 2018 року, який оновлює інші закони у сфері захисту персональних даних з метою імплементації законодавства ЄС у сфері захисту персональних даних та забезпечення відповідності до нього [70].

Основними відмінностями Закону про захист персональних даних від GDPR є таке: (1) закон застосовується до усіх суб'єктів персональних даних, які проживають у Франції, незалежно від місцезнаходження контролера; (2) у певних випадках повинен бути наданий дозвіл на опрацювання персональних даних, що стосуються судимостей та правопорушень; (3) зменшено вік надання згоди на опрацювання персональних даних неповнолітніх до 15 років та запроваджено подвійне надання згоди, якщо особа молодша цього віку - неповнолітнього та батьків; (4) французький регулятор має право накладати додаткові санкції, окрім тих, які встановлені у GDPR; (5) потерпілі мають можливість подавати групові позови та вимагати відшкодування за матеріальні та моральні збитки, які були спричинені порушенням прав у сфері захисту персональних даних [71, с. 20].

Таким чином, якщо певний суб'єкт господарювання, який функціонує в одній з країн-учасниць ЄС та є контролером персональних даних, спрямовує

свою діяльність на резидентів Франції, то такий суб'єкт господарювання буде підпадати під регулювання не лише GDPR, а й французького закону про захист персональних даних та внутрішній закон тієї країни, де такий суб'єкт здійснює свою діяльність [72].

Окрім вищевказаних нормативно-правових актів, у Франції у сфері захисту персональних даних також діє Кодекс з поштових та електронних комунікацій. У цьому кодексі міститься стаття L. 34-5, якою забороняється відсилати факси та електронні повідомлення користувачам без їх попередньої згоди - таким чином була імплементована директива 2002/58/ЕС [73].

1.2.4. Особливості регулювання захисту персональних даних в Ірландії

Як і в проаналізованих вище країнах, Ірландія також прийняла внутрішнє регулювання у сфері захисту персональних даних. Зокрема, 24 травня 2018 року був прийнятий Закон про захист даних 2018 року. Цей закон, з-поміж іншого, «створює Комісію із захисту персональних даних у якості нового регулятора, імплементує європейську Директиву про правозастосування у внутрішнє ірландське законодавство, а також більш детально регулює окремі питання захисту персональних даних у випадках коли GDPR дає таку можливість» [74; 75].

Новий регуляторний орган у сфері захисту персональних даних, відповідно до Закону про захист даних, має більш широкі повноваження на кшталт виконання ордерів на обшук, можливості звертатись з клопотанням до Вищого суду з проханням обмежити або призупинити опрацювання даних у необхідних випадках. Також регулятор може накладати штрафи, але лише після підтвердження окружного суду [76].

Слід зазначити, що парламент Ірландії вирішив не зменшувати вік надання згоди на опрацювання персональних даних неповнолітніми, незважаючи на те, що у першій редакції закону був встановлений вік 13 років. Тим не менш, Верхня палата парламенту Ірландії проголосувала у 55 голосів «за» встановлення 16-

річного віку надання згоди на опрацювання персональних даних неповнолітніми на противагу 51 голосів «проти» [76].

Цікаво також звернути увагу на аргументацію двох протилежних сторін. Меншість верхньої палати аргументувала необхідність отримання згоди дітей з 13 років, стверджуючи, що в мережі інтернет є велика кількість корисних ресурсів, наприклад, освітніх, а також сервісів, що здійснюють надання соціальних послуг тощо. У той самий час, заборона отримання згоди на опрацювання персональних даних до 16 років обмежує право неповнолітніх на отримання корисної інформації. Більшість парламенту, яка вимагала підвищення віку надання згоди на опрацювання персональних даних неповнолітніми до 16 років, аргументувала свою позицію через таргетинг компаній, а також тим, що використання соціальних медіа загрожує індивідуалізму неповнолітніх та є «деструктивним у довгостроковій перспективі» [76].

Разом з тим, законом також передбачена можливість прийняття Кодексу поведінки дітей, який встановлював би гарантії захисту цифрових прав дітей, визначав обсяг інформації, яка має бути надана дітям від контролера, а також спосіб отримання згоди батьків на опрацювання персональних даних дітей [76].

Окрім вищевикладеного, в Ірландії прийнятий акт, який впроваджує норми Директиви 2002/58/ЕС - Положення про конфіденційність. Цим положенням регулюється опрацювання персональних даних за допомогою визначених способів комунікацій, наприклад: телефону, СМС-повідомлень та електронної пошти [77].

При цьому, слід зазначити, що виконання вимог щодо захисту персональних даних компаніями в Ірландії є особливо важливими, адже ірландський регулятор наглядає над такими технічними «гігантами» як Google, Facebook, Microsoft та Twitter [78]. Разом з тим, ірландський регулятор, станом на лютий 2020 року не застосував жодних штрафних санкцій [33].

У той самий час, незважаючи на відсутність штрафних санкцій, ірландський регулятор активно реагує у певних випадках. У зв'язку із запуском сервісу знайомств, компанія Facebook зв'язалась з ірландським регулятором 03

лютого 2020 року - за 10 днів до запуску цього сервісу на ринку ЄС. Разом з тим, компанія не надала жодної документації стосовно оцінки впливу на захист даних або процесів прийняття рішень. 10 лютого 2020 року, зважаючи на запланований запуск сервісу 13 лютого 2020 року, ірландський регулятор здійснив перевірку в офісі Facebook у Дубліні та зібрав необхідну документацію. У зв'язку з цим, компанія Facebook затримала дату запуску сервісу знайомств [79].

ВИСНОВКИ ДО РОЗДІЛУ 1

Регулювання захисту персональних даних у ЄС має ознаки певного дуалізму, оскільки існують нормативно-правові акти як національні, так і ті, які поширюються на всі країни-учасниці ЄС. Разом з тим, слід зазначити, що є також чітка ієрархія - акти ЄС мають перевагу над законодавством окремих держав.

На загальноєвропейському рівні основним нормативно-правовим актом є GDPR, який є обов’язковим для країн-учасниць ЄС без додаткової імплементації у національне законодавство. GDPR набрав чинності 25 травня 2018 та замінив Директиву 95/46/ЕС, зміст якої повинен був додатково імплементуватись у національне законодавство. Разом з тим, країни-учасниці ЄС можуть приймати внутрішні нормативно-правові акти, які адаптують застосування GDPR у конкретній країні.

Слід зазначити, що GDPR не надає виключний перелік персональних даних, а лише встановлює критерії для визначення що є такими даними на підставі індивідуального аналізу та відповідного контексту, що є цілком логічним, зважаючи на появу нових персональних даних із розвитком технологій. Разом з тим, загальний стратегічний напрямок у регулюванні захисту персональних даних не зазнав значних змін. Аналіз здійснювався шляхом порівняння змісту принципів, якими пронизаний текст Директиви 95/46/ЕС та GDPR.

Ключовими положеннями у GPDR для контролера та оператора є таке: (1) обов'язок здійснення опрацювання виключно у законний спосіб; (2) обов'язок

надавати прозору інформацію; (3) обов'язок забезпечити право на доступ та портативність даних; (4) обов'язок забезпечити право бути забутим; (5) а також обов'язок забезпечити право на виправлення та право на заперечення.

Слід зазначити, що регулятори активно накладають штрафні санкції, хоча у більшості випадків розмір штрафів є меншим, ніж 10 000 євро. Разом з тим, накладались також штрафи зовсім іншого масштабу, зокрема: штраф на 1&1 Telecom GmbH у розмірі 9 550 000 євро; на Deutsche Wohnen SE у розмірі 14 500 000 євро; та на Google у розмірі 50 000 000 євро. При цьому, розмір штрафу настільки відрізняється у зв’язку з тим, що його розмір вираховується відповідно до річного обороту відповідної групи компаній. Відповідно, чим більша компанія, тим більший розмір штрафу.

Варто також зазначити, що штрафні санкції можуть накладатись не лише на суб'єктів господарювання, а й на установи та організації. Зокрема болгарським регулятором був накладений штраф у розмірі 2 600 000 євро на Орган державних доходів, внаслідок масштабного витоку даних. Окрім юридичних осіб, санкції можуть бути застосовані також щодо фізичних осіб. Так, іспанський регулятор наклав штраф на фізичну особу у розмірі 10 000 євро за поширення інтимних фотографій та знімків екрану приватних повідомлень з месенджеру WhatsApp.

Національне нормативно-правове регулювання країн-учасниць ЄС (Німеччини, Франції, Ірландії) та Великобританії, хоч і має свої особливості, але концептуально не відрізняється. В усіх цих країнах був прийнятий власний нормативно-правовий акт, який регулює захист персональних даних шляхом доповнення та адаптації норм GDPR з певними національними особливостями. Також в усіх цих країнах був прийнятий акт, який імплементує європейську Директиву про конфіденційність 2002/58/ЕС. У Великобританії GDPR матиме чинність протягом перехідного періоду процедури виходу з ЄС - до 31 грудня 2020 року, а після спливу цього строку GDPR буде діяти на загальних підставах - через призму застосування територіальної сфери дії.

РОЗДІЛ 2. ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У США

2.1. Аналіз законодавства США у сфері захисту персональних даних

2.1.1. Нормативно-правові акти США у сфері захисту персональних даних

Підхід США до регулювання захисту персональних даних значно відрізняється від підходу, який застосовується в ЄС. Відповідно до здійсненого у першому розділі аналізу, у ЄС є нормативно-правові акти, які застосовуються на всій його території. У той самий час, у США застосовується галузевий підхід до регулювання захисту персональних даних. Іншими словами, у США існує комбінація нормативно-правових актів різних рівнів («федеральний та на рівні штатів, адміністративне регулювання та спеціальні галузеві рекомендації»), які застосовуються стосовно певних галузей, як то медицина, освіта, комунікації тощо, та відповідної судової практики [80, с. 299].

Зокрема, на федеральному рівні існують такі нормативно-правові акти, як: Закон «Грамм-Ліч-Блілі» (скор. «GLBA»), Закон про сумісність та підзвітність медичного страхування (скор. «HIPAA»), Закон про справедливу кредитну звітність (скор. «FCRA»), Закон про зв’язок, Закон про захист відеоданих, Закон про сімейні права на освіту та конфіденційність (скор. «FERPA»), Закон про захист персональних даних дітей в Інтернеті (скор. «COPPA»), Закон про конфіденційність електронних комунікацій (скор. «ECPA»), Закон про комп'ютерні шахрайства та зловживання (скор. «CFAA») тощо. Усі ці федеральні нормативно-правові акти регулюють захист персональних даних лише в межах свого предмета регулювання та не застосовуються на міжгалузевій основі [81, с. 7-30].

Особливо важливим федеральним нормативно-правовим актом у сфері захисту персональних даних є Акт Федеральної торгової комісії (скор. «FTC»), відповідно до якого, Федеральна торгова комісія набула повноважень

здійснювати правозастосовні дії для захисту прав споживачів проти «недобросовісних чи оманливих практик» компаній. При чому, під оманливими практиками Федеральна торгова комісія розуміє також відсутність належного захисту персональних даних та, відповідно, має право застосовувати федеральне законодавство у цій сфері. Таким чином, Федеральна торгова комісія є головним (хоч і не єдиним) регулятором у США. Окрім Федеральної торгової комісії, сфера захисту персональних даних регулюється також різними галузевими органами державної влади [82].

Незважаючи на такий сталий галузевий підхід, після прийняття GDPR у ЄС, у 2018 році у штаті Каліфорнія, було прийнято CCPA - нормативно-правовий акт, який регулює права споживачів стосовно «доступу, видалення та обміну особистою інформацією, що збирається суб'єктами господарювання» [83]. CCPA, на відміну від іншого законодавства у США, регулює захист персональних даних у всіх галузях та є схожим у цьому сенсі на GDPR. Цікаво, що після прийняття CCPA, інші штати також запропонували регулювати цю сферу на міжгалузевій основі та навіть були подані законопроекти у Конгрес США, які б регулювали захист персональних даних на федеральному рівні [84].

Станом на лютий 2020 року, окрім штату Каліфорнія, подібні до CCPA нормативно-правові акти на рівні штату були прийняті у штаті Мен та Невада [85]. Закон щодо захисту персональних даних споживачів у мережі інтернет був підписаний губернатором штату Мен у 2019 році та набирає законної сили з 01 липня 2020 року [86]. Закон у штаті Невада був підписаний також у 2019 році та набрав чинності 01 жовтня 2019 року - за три місяці до набрання чинності CCPA [87].

2.1.2. Перспективи прийняття федерального нормативно-правового акта у сфері захисту персональних даних

Необхідно зазначити, що велика кількість нормативно-правових актів у сфері захисту персональних даних та відсутність будь-якої уніфікації значно

ускладнює ведення підприємницької діяльності глобальним суб'єктам господарювання. Зокрема, у вересні 2019 року Сенату США та Палаті представників США було надіслано відкритий лист від провідних компаній в США, включаючи Dell, Amazon, Mastercard, Walmart та інших. У цьому листі зазначається, що необхідне прийняття комплексного та єдиного нормативно-правового акта, який б забезпечував створення єдиного підходу до регулювання захисту персональних даних на національному рівні, а також зростання цифрової економіки [88].

Більш того, до цього листа також був доданий документ під назвою «Стандарти стосовно законодавства про захист персональних даних споживачів», у якому зазначаються положення, які повинні бути враховані при розробці подібного закону. З-поміж іншого, наголошується на тому, що США має бути лідером у цій сфері, регулювання має бути технічно нейтральним та ґрунтуватись на принципах, регулювання цієї сфери повинно бути гармонізоване, а також, що повинна бути досягнена глобальна сумісність регулювання [89, с. 1].

Для досягнення цілі розробки єдиного регулювання, сенатором Марією Кентвел від демократів та сенатором Роджером Вікером від республіканців було презентовано два законопроекти, які мають як схожі, так і відмінні положення - Закон про захист персональних даних споживачів в Інтернеті (скор. «COPRA») та Закон про захист персональних даних споживачів США (скор. «CDPA») відповідно [90; 91; 92].

Ці законопроекти мають досить схожу сферу дії. COPRA застосовується до усіх юридичних осіб, на яких поширюється юрисдикція Федеральної торгової комісії. Разом з тим, республіканський CDPA, окрім юрисдикції Федеральної торгової комісії, також поширюється на юридичні особи, на яких поширюється Закон про комунікації 1934 року, а також на неприбуткові організації [93, с. 2]. Обидва законопроекти мають виключення стосовно малих суб'єктів господарювання, які визначаються ними як ті, які «за попередні 3 роки мали щорічний валовий дохід в середньому у розмірі 25 000 000 доларів США або

менше, опрацьовували персональні дані менше ніж 100 000 осіб або отримували менше 50 відсотків доходу від передачі даних, що охоплюються». Тим не менш, якщо COPRA повністю не застосовується щодо такого бізнесу, то CDPA не застосовується лише в частині певних обов'язків, які витікають з прав суб'єктів персональних даних (наприклад, права на доступ) [90].

2.1.3. Визначення персональних даних за законодавством США

У продовження попереднього пункту, варто зазначити, що як COPRA, так і CDPA мають майже однакове визначення персональних даних (у законопроектах – «covered data») [91, с. 5, 6; 92, с. 2, 3].

Згідно із COPRA, персональними даними вважається «інформація, яка ідентифікує або пов'язана, або в обґрунтованій мірі пов'язана з фізичною особою або із споживчим пристроєм, включаючи вторинні дані». Разом з тим, у це визначення не входить знеособлена інформація, інформація стосовно працівників, а також публічна інформація [91, с. 6].

Відповідно до CDPA, персональними даними вважається «інформація, яка ідентифікує або пов'язана, або в обґрунтованій мірі пов'язана з фізичною особою або із пристроєм, який пов'язаний або в обґрунтованій мірі пов'язаний з фізичною особою». Як і в COPRA, в CDPA також зазначені дані, які не входять у поняття персональних даних. За CDPA не є персональними даними узагальнені дані, знеособлена інформація, інформація стосовно працівників, а також публічна інформація [92, с. 2, 3].

Проаналізувавши ці визначення, можна стверджувати, що, незважаючи на їх схожість, між ними все ж є певні відмінності. Зокрема, COPRA включає у визначення персональних даних вторинні дані, а CDPA не включає у визначення персональних даних узагальнені дані. При цьому, COPRA визначає вторинні дані як «персональні дані, які створюються шляхом отримання інформації, даних, припущень або висновків із фактів, доказів чи іншого джерела інформації або даних про особу, домогосподарство чи пристрій, якими користується особа або

домогосподарство». У той самий час, CDPA визначає узагальнені дані як «інформацію, яка відноситься до групи або категорії осіб або пристроїв, яка не ідентифікує і не пов'язана або в обґрунтованій мірі не пов'язана з будь-якою особою» [91, с. 6-8; 92, с. 2-3].

Стосовно чинних нормативно-правових актів, варто зазначити, що замість терміну «персональні дані» використовується термін «персональна ідентифікаційна інформація» (англ. «personally identifiable information»). Слід також зазначити, що у США відсутнє єдине визначення персональної інформації - воно може відрізнятись в залежності від нормативно-правових актів й конкретних штатів [82].

Загалом у США існує три підходи до визначення персональної ідентифікаційної інформації у різноманітних нормативно-правових актах: тавтологічний підхід, непублічний підхід та підхід конкретного типу [94, с. 1828].

Прикладом тавтологічного підходу може бути визначення персональної ідентифікаційної інформації у Законі про захист інформації у відео (скор. «VPPA»). У цьому законі персональна ідентифікаційна інформація визначається як «інформація, яка ідентифікує особу». У такому визначенні, яке, фактично, є повтором, є свої переваги та недоліки. Перевагою зазначеного визначення та, відповідно, тавтологічного підходу є гнучкість - визначення може саме по собі видозмінюватись у зв'язку з появою нових підходів щодо опрацювання інформації. Недоліком тавтологічного підходу є неможливість виділення персональної ідентифікаційної інформації з-поміж інших видів інформації за допомогою виключно визначення [94, с. 1829].

Визначення персональної ідентифікаційної інформації, які побудовані відповідно до непублічного підходу, визначають радше що не є такою інформацією. Таким чином, за цим підходом персональною інформацією може бути, наприклад, уся інформація, яка не підпадає під поняття публічно доступної або статистичної інформації. До прикладу, згідно із Законом «Грамм-Ліч-Блілі» (скор. «GLBA»), персональною ідентифікаційною фінансовою інформацією є

«непублічна персональна інформація». Тим не менш, у законі не визначено що включає в себе ознака непублічності. Значним недоліком такого підходу є те, що при його застосуванні не враховується ознака «ідентифікаційності». У той самий час, ознака приватності або публічності певної інформації автоматично не означає те, що за допомогою цієї інформації можна ідентифікувати конкретну особу [94, с. 1829-1830].

Відповідно до підходу конкретного типу, персональною ідентифікаційною інформацією є та інформація, яка підпадає під певний перелік категорій даних, що складають персональну ідентифікаційну інформацію. До прикладу, відповідно до Положення стосовно повідомлень про порушення у штаті Массачусетс, персональною ідентифікаційною інформацією є «ім’я та прізвище людини, або ім'я та прізвище у поєднанні з номером соціального страхування, номером посвідчення водія, номером фінансового рахунку або номером кредитної чи дебетової картки». Недоліком цього підходу у певних випадках може вважатись те, що він досить обмежуючий по відношенню до визначення персональної ідентифікаційної інформації. У випадку із зазначеним визначенням, до такої інформації входить лише вузький перелік даних, хоча ідентифікувати особу можна й за допомогою інших даних [94, с. 1831-1832].

2.1.4. Ключові положення CCPA стосовно захисту персональних даних

Надалі, при аналізі законодавства США у сфері захисту персональних даних, буде здійснюватися акцент на CCPA, оскільки це є перший нормативно-правовий акт у США, який створив вичерпне регулювання у цій сфері, яке є схожим до GDPR [95]. Крім цього, аналіз чинного CCPA є важливим, оскільки федеральні законопроекти у великій мірі відображують регулювання, яке встановлене CCPA [96]. Також вагомою причиною здійснювати аналіз саме CCPA є та обставина, що у штаті Каліфорнія здійснюється велика кількість опрацювання персональних даних, оскільки цей штат складає 15 відсотків від усієї економіки США. Більш того, якщо б штат Каліфорнія був незалежною

країною, то це була б п'ята економіка у світі - між Німеччиною та Великобританією [97].

Перш за все, слід зазначити, що «CCPA застосовується не до всіх суб'єктів господарювання. Цей нормативно-правовий акт поширюється на підприємства, які (1) здійснюють свою діяльність в межах штату Каліфорнія, (2) збирають персональні дані резидентів Каліфорнії, (3) визначають на власний розсуд (або сумісно з іншими особами) цілі та засоби опрацювання таких даних, а також (4) або мають річний валовий дохід понад 25 мільйонів доларів США з урахуванням інфляції; або щорічно купують, отримують з комерційною метою, продають або діляться персональними даними 50 000 або більше споживачів, домогосподарств чи пристроїв; або отримують 50 або більше відсотків своїх щорічних доходів від продажу персональних даних споживачів» [98, с. 4].

Здійснення діяльності в межах штату Каліфорнії тлумачиться CCPA досить широко [98, с. 4]. При цьому, відповідно до пункту 6 статті 1798.145, CCPA не поширюється на суб'єкти підприємницької діяльності, якщо всі аспекти такої діяльності мають місце поза межами штату [99, с. 17]. Також слід зазначити, що, на відміну від GDPR, у випадку, якщо «представник каліфорнійського бізнесу опрацьовує персональні дані користувачів, які знаходяться в іншій країні, такому бізнесу не потрібно здійснювати комплаєнс з CCPA лише через те, що він знаходиться у штаті Каліфорнія» [98, с. 4].

Під резидентами штату Каліфорнія маються на увазі особи, які (1) постійно перебувають у штаті Каліфорнія, (2) постійно перебувають у штаті Каліфорнія, але тимчасово знаходяться не в межах цього штату [98, с. 5]. Виходячи з цього, суб'єктам господарювання непросто визначати поширення дії CCPA на конкретних користувачів, оскільки потрібно здійснювати аналіз того, чи перебуває той чи інший користувач на території штату Каліфорнії постійно або ж тимчасово [100].

У продовження попереднього пункту про визначення персональних даних згідно з різними нормативно-правовими актами, персональними даними (інформацією), відповідно до пункту (o) статті 1798.140 CCPA, є інформація, яка

ідентифікує, стосується, описує, може бути пов'язана або може бути в обґрунтованій мірі пов'язана, безпосередньо чи опосередковано, з певним споживачем чи домогосподарством [99, с. 13].

Серед іншого, персональними даними можуть бути (1) різні ідентифікатори на кшталт імені, поштової адреси, електронної адреси, номеру паспорта або телефону тощо, (2) характеристика захищених класифікацій відповідно до законодавства штату Каліфорнія чи федерального закону, (3) комерційна інформація, включаючи записи про особисте майно, продукти чи послуги, які були придбані, отримані або розглянуті, а також інші історії покупок чи споживання, (4) біометрична інформація, якою можуть вважатись фізіологічні, біологічні та поведінкові характеристики, включаючи ДНК людини, (5) інформація про мережу інтернет, включаючи історію переглядів, історію пошуку та інформацію про взаємодію споживача з веб-сайтом, додатком чи рекламними оголошеннями, (6) дані геолокації, (7) аудіо, електронні, візуальні, теплові, нюхові або інші подібні відомості, (8) професійна інформація або інша інформація, що стосується зайнятості, (9) інформація про освіту, яка не є публічно доступною, (10) будь-які узагальнення, отримані з будь-якої інформації, визначеної вище, та які були здійснені з метою створення профілю про споживача, що відображає його споживчі вподобання, характеристики, психологічні тенденції, схильності, поведінку, ставлення, інтелект та здібності [98, с. 6-8; 99, с. 13, 14].

До поняття персональних даних не включається публічна інформація. Згідно із пунктом (o)(2) статті 1798.140 CCPA, публічною інформацією вважається інформація, що законно надається з федеральних, місцевих органів влади або органів влади штатів США, за умови існування законних підстав [99, с. 14]. Також винятком із визначення персональних даних є неідентифікована інформація або інформація, яка є частиною сукупної інформації про споживачів [98, с. 8].

Для здійснення комплаєнсу із CCPA, важливо також розуміти чим є збирання персональних даних. Відповідно до пункту (e) статті 1798.140 CCPA,

під цим терміном розуміється придбання, тимчасове користування, збирання, отримання або доступ до будь-якої особистої інформації, що стосується споживача, будь-якими способами. Це визначення включає в себе також отримання інформації від споживача як активно, так і пасивно, або шляхом спостереження за його поведінкою [99, с. 12].

Для можливості практичного здійснення такого комплаєнсу, одним з найважливіших кроків є забезпечення реалізації прав суб'єктів персональних даних. Згідно із CCPA, визначаються такі права суб'єктів персональних даних: право на доступ, право на вимогу видалення персональних даних, право на вимогу розкриття зібраної та поширеної інформації, право на вимогу розкриття категорій проданих персональних даних, право на відмову (opt-out) від продажу персональних даних, право на недискримінацію. Для реалізації цих прав, суб'єкти підприємницької діяльності мають забезпечити два або більше способів подання відповідних вимог, які мають бути верифіковані, але обов'язково за допомогою безкоштовного телефонного зв'язку та веб-сайту (за наявності) [98, с. 22-33].

Крім зазначених вище прав, є лише виключні випадки коли суб'єкти підприємницької діяльності мають право передати персональні дані надавачам послуг (англ. «service providers»). Не менш важливим є те, що суб'єкти підприємницької діяльності мають право за певних умов відмовити у виконанні вимог користувачів [98, с. 34, 35].

Стосовно права на доступ та права на вимогу розкриття зібраної та поширеної інформації, суб'єкти персональних даних мають такі право стосовно: «категорій зібраних персональних даних користувача протягом останніх дванадцяти місяців; конкретних персональних даних, які були зібрані; категорій джерел, з яких збирались персональні дані; цілей збору або продажу персональних даних; категорій третіх осіб, яким поширювались зібрані персональні дані; категорій проданих персональних даних та категорій третіх осіб, яким були продані персональні дані; категорій персональних даних, які розкриваються для бізнес-цілей» [101]. Для обробки вимоги на доступ до

інформації, суб'єктам підприємницької діяльності надається значний обсяг часу - 45 днів, з можливістю збільшити цей час ще на 45 днів, але з відповідним повідомленням про таке збільшення користувача. Вказана у попередньому абзаці інформація повинна бути надана користувачу у портативному та легко доступному вигляді, яку можна «без перешкод» передати до іншого підприємства або організації [98, с. 22, 26].

Стосовно права на видалення персональних даних, слід зазначити, що воно не є абсолютним. Зокрема, виконання такої вимоги не є обов'язковим для суб'єктів підприємницької діяльності у випадку необхідності забезпечення права на свободу слова та інших прав, виконання юридичних зобов'язань, приведення діяльності у відповідність із законодавством тощо. Разом з тим, суб'єкти підприємницької діяльності, у разі надходження такої вимоги, повинні повідомити про неї також надавачів послуг [98, с. 24].

Окремо від права на доступ та права на вимогу розкриття зібраної та поширеної інформації виділяється право на вимогу розкриття категорій проданих персональних даних. Користувач має право дізнатись, окрім зібраних про нього персональних даних, також про категорії проданих персональних даних разом кожній третій особі, а також інформацію про те, які персональні дані були розкриті в комерційних цілях [98, с. 28].

Із правом на вимогу розкриття категорій проданих персональних даних тісно пов'язане право на відмову (opt-out) від продажу персональних даних. Це право означає те, що користувач може у будь-який момент відмовитись від продажу своїх персональних даних третім особам. Суб'єкти господарювання повинні забезпечити таку можливість на веб-сайті шляхом розміщення покликання із текстом «Не продавати мої персональні дані». Зазначене покликання, а також опис цього права мають бути зазначені у політиці конфіденційності. Важливо зазначити, що якщо користувачем було використане це право, то суб'єкт господарювання не може запитувати нову таку згоду на продаж персональних даних протягом 12 місяців. Більш того, у випадку якщо користувачу від 13 до 16 років, то персональні дані не можуть бути продані без

попередньої стверджуючої згоди на такий продаж. У випадку ж якщо користувачем є особа до 13 років, то така згода має бути надана батьками або опікунами. При цьому, використовується презумпція, що, якщо суб'єкт господарювання ігнорує запит віку користувачів, то у такому випадку він знає їх вік [98, с. 30].

Не менш важливим правом, яке мають суб'єкти персональних даних, є право на недискримінацію - суб'єкти господарювання не можуть дискримінувати користувачів, які намагаються реалізувати свої права відповідно до CCPA. Йде мова про такі випадки як «відмова у наданні послуг або продажу товарів, цінова дискримінація (включаючи надання знижок тим користувачам, які не відмовляються від продажу персональних даних), зміна у якості наданих послуг або проданих товарів, а також навіювання того, що користувач, у випадку використання своїх прав, отримає іншу ціну чи рівень наданих послуг або проданих товарів» [98, с. 32].

Разом з тим, існують певні виключення при реалізації цього права. Зокрема, «(1) суб'єкти господарювання можуть встановлювати іншу ціну або надавати різний рівень послуг або товарів у випадку якщо це в обґрунтованій мірі пов'язано з цінністю, яка надається користувачу у зв'язку із використанням або невикористанням персональних даних користувача; (2) суб'єкти господарювання можуть пропонувати фінансові стимули та заохочування для збирання, продажу або видалення персональних даних, але лише у випадку попереднього повідомлення про умови такого заохочення й отримання попередньої згоди з такими умовами; (3) при цьому, фінансове стимулювання не може бути несправедливим, необґрунтованим або ж примусовим» [98, с. 32].

Тим не менш, необхідно зазначити, що суб'єкти підприємницької діяльності мають право за певних умов відмовити у задоволенні вимог користувачів стосовно розкриття або видалення персональних даних. Зокрема, це можливо у випадку, коли про це рішення було негайно повідомлено користувача із зазначенням обґрунтування такої відмови й роз'ясненням права на оскарження. Разом з тим, у випадку наявності політики, у якій зазначені підстави

для відмови у задоволенні запиту користувача, роз'яснення щодо права на оскарження надавати не обов'язково [98, с. 35].

Також суб'єкт підприємницької діяльності може визначити, що запит користувача є очевидно необґрунтованим або надмірним (зокрема, але не виключно, за ознакою повторюваності). У цьому випадку (1) користувачу може бути відмовлено за таким ж порядком, що й у попередньому абзаці, а також (2) з користувача може стягуватись плата у розумному розмірі за виконання його вимог. Можливість визнавати запит користувача необґрунтованим або надмірним є лише у випадку наявності відповідної політики, яка б регулювала це питання. Окрім цього, має існувати ще політика, де б було зазначено чи може суб'єкт господарювання стягувати плату, а також методику вирахування такої суми [98, с. 35].

Як вже зазначалось раніше, є виключний перелік випадків коли суб'єкти підприємницької діяльності мають право передати персональні дані надавачам послуг [98, с. 34]. Під надавачами послуг, згідно пунктом (v) статті 1798.140 CCPA, мається на увазі індивідуальне приватне підприємство, товариство, товариство з обмеженою відповідальністю, корпорацію, асоціацію чи іншу юридичну особу, яка організовується або працює з метою отримання прибутку або фінансової вигоди своїх акціонерів або інших власників, та яка обробляє інформацію від імені бізнесу та якій бізнес розкриває особисту інформацію користувача для ділових цілей відповідно до письмового договору [99, с. 16].

Для того щоб третя особа визнавалась надавачем послуг, вона повинна відповідати таким критеріям: «(1) бути прибутковою організацією, (2) бути оператором для бізнесу, (3) отримувати дані для ділових цілей, а також (4) отримувати дані відповідно до договору. При цьому, важливо, щоб такий договір забороняв постачальнику послуг зберігати, використовувати або розголошувати персональні дані для будь-яких цілей, крім тих, що стосуються цілей надання послуг, які зазначені у договорі, або в інших випадках відповідно до CCPA» [102]. Важливо також зазначити, що суб'єкти господарювання не є

відповідальними за порушення надавачами послуг вимог CCPA та навпаки [98, с. 34].

2.2. Особливості регулювання захисту персональних даних California Consumer Privacy Act у порівнянні з General Data Protection Regulation

Перш за все, слід зазначити, що GDPR поширюється на значно ширше коло суб'єктів, у порівнянні із CCPA. Відповідно до статті 3, GDPR діє стосовно усіх контролерів та операторів, які (1) мають осідок у ЄС, незалежно від того де відбувається опрацювання (в межах ЄС або поза його межами) або (2) не мають осідку в ЄС, але опрацьовують персональні дані у зв'язку із постачанням товарів чи наданням послуг фізичним осіб, які перебувають в ЄС або у зв'язку із моніторингом поведінки таких осіб [8, с. 39, 40; 103, с. 1].

У той самий час, як вже було зазначено раніше, «CCPA застосовується до підприємств, що здійснюють свою діяльність в штаті Каліфорнія та які мають річний валовий дохід понад 25 мільйонів доларів США з урахуванням інфляції; або щорічно купують, отримують з комерційною метою, продають або діляться персональними даними 50 000 або більше споживачів, домогосподарств чи пристроїв; або отримують 50 або більше відсотків своїх щорічних доходів від продажу персональних даних споживачів» [98, с. 4]. Також CCPA поширюється на підприємства, які контролюють підприємства, що підпадають під вказані критерії або контрольовані ними, а також на підприємства, які мають такий ж брендинг, що й підприємства, на які поширюється CCPA [103, с. 1].

Таким чином, якщо CCPA поширюється лише на підприємства, які відповідають одному з вказаних критеріїв, GDPR поширюється, окрім підприємств, на фізичні особи, установи та організації, незалежно від того чи вони створені з метою отримання прибутку, а також незалежно від їх розміру [104, с. 7]. Більш того, GDPR може застосуватись на контролерів або операторів, які здійснюють свою діяльність поза межами ЄС, в той час як CCPA

застосовується лише на підприємства, які здійснюють свою діяльність у штаті Каліфорнія [104, с. 9].

Більш схожі підходи у цих нормативно-правових актах стосовно осіб, які підлягають захисту. Як GDPR, так і CCPA захищають лише фізичних осіб, хоча і визначення того, які саме фізичні особи підлягають захисту, відрізняються. GDPR застосовується стосовно фізичних осіб, «яких ідентифіковано або можна ідентифікувати» без вимоги мати місце проживання чи громадянство ЄС, знаходитись в межах ЄС або за його межами, хоча у таких випадках для застосування GDPR мають бути виконані інші критерії [8, с. 40; 104, с. 7].

CCPA, у свою чергу, захищає споживачів. Під споживачами маються на увазі фізичні особи, які є резидентами штату Каліфорнія. Під резидентами штату Каліфорнія маються на увазі особи, які (1) постійно перебувають у штаті Каліфорнія, (2) постійно перебувають у штаті Каліфорнія, але тимчасово знаходяться не в межах цього штату. Фізичні особи, які не підпадають під визначені критерії, не є резидентами штату Каліфорнія та, відповідно, не є споживачами у розумінні CCPA [104, с. 7].

Отже, як GDPR, так CCPA застосовують відносно осіб, які захищаються, екстериторіальну дію, що зобов'язує здійснювати комплаєнс із цими актами підприємств та інших суб'єктів (стосовно GDPR) також поза межами їх сфери дії [103, с. 2].

Стосовно даних, що підлягають захисту, слід зазначити, що в обох нормативно-правових актах підлягають захисту саме персональні дані (у випадку із CCPA - персональна інформація), визначення яких було надано раніше у цій роботі [103, с. 2]. Разом з тим, якщо GDPR визначені будь-які дії із персональними даними, як «опрацювання», то CCPA розділяє їх на збір, продаж та опрацювання, що створює більш детальне регулювання [104, с. 10].

GDPR охоплює більшу кількість даних своїм регулюванням, оскільки не створює жодних винятків щодо певних категорій даних, хоча й створює винятки стосовно способів опрацювання персональних даних. Зокрема, GDPR не застосовується якщо опрацювання здійснюється за допомогою

неавтоматизованих засобів, а також якщо воно здійснюється фізичною особою для суто особистих чи побутових цілей [104, с. 11, 12].

У свою чергу, CCPA встановлює ряд даних щодо яких не поширюється регулювання, наприклад: медична інформація, публічно опубліковані персональні дані тощо. У багатьох випадках такі виключення пов'язані із потенційним подвійним регулюванням. Зокрема, захист медичної інформації регулюється Законом про конфіденційність медичної інформації та Законом про портативність та підзвітність медичного страхування, що виключає необхідність повторного регулювання CCPA [104, с. 11, 12].

Щодо анонімних, невизначених та псевдонімічних даних, GDPR визнає невизначені дані як персональні дані, а анонімні як не персональні дані. У той самий час, GDPR не надано окреме визначення псевдонімічних даних. У свою чергу, CCPA не обмежує підприємства у збиранні, використанні, зберіганні, продажу та розкриттю інформації про споживача, яка є невизначеною. Разом з тим, для того щоб інформація була визнана невизначеною, встановлені високі стандарти. Щодо псевдонімічних даних, CCPA дає їх визначення, проте чітко не вказує на те, чи є ці дані персональними. Загалом, можна ствердити, що підхід у цьому контексті у GDPR та CCPA є схожими, хоча і регулювання відрізняється у термінологічному сенсі [103, с. 2, 3].

GDPR та CCPA мають схожі та відмінні риси у відношенні до регулювання суб'єктів, які безпосередньо здійснюють опрацювання персональних даних або причетні до цього процесу. GDPR визначає таких осіб як контролери та оператори (англ. «controllers and processors»), а CCPA як підприємства та надавачі послуг (англ. «businesses and service providers») [104, с. 17].

«Контролери за GDPR за визначенням є чимось подібним до підприємств за CCPA, оскільки саме ці суб'єкти є відповідальними за відповідність діяльності до чинного законодавства». Разом з тим, при порівнянні операторів та надавачів послуг, GDPR, у порівнянні із CCPA, накладає більш чіткі обов'язки на операторів, аніж CCPA на надавачів послуг [104, с. 17].

Незважаючи на те, що оператори за GDPR є багато у чому схожими на надавачів послуг за CCPA, GDPR накладає на операторів більший обсяг обов'язків. Такими обов'язками є зокрема: (1) ведення обліку діяльності з опрацювання персональних даних у визначених GDPR випадках, «включаючи наявності більше 250 співробітників або у випадку опрацювання персональних даних, які можуть призвести до порушення прав і свобод суб'єктів персональних даних»; (2) впровадження відповідних технічних та організаційних заходів, включаючи шифрування та псевдонімізацію; (3) здійснення оцінки впливу на захист персональних даних у контексті наданні допомоги контролеру; (4) призначення посадової особи із захисту персональних даних у випадках, передбачених GDPR; (5) повідомлення контролера про витоки персональних даних «без необґрунтованої затримки» [104, с. 19].

Стосовно впливу цих нормативно-правових актів на дітей, варто зазначити, що вони передбачають додатковий захист дітей у контексті опрацювання персональних даних [104, с. 19]. Зокрема, «CCPA забороняє продаж персональних даних фізичних осіб до 16 років без їх згоди». При цьому, якщо особи віком від 13 до 16 років можуть надавати таку згоду самостійно, то стосовно дітей до 13 років необхідна згода батьків. Крім цього, у США існує окремий федеральний нормативно-правовий акт стосовно захисту персональних даних дітей - Закон про захист персональних даних дітей в мережі інтернет (COPPA) [103, с. 4].

Відповідно до GDPR, згода на опрацювання персональних даних також має надаватись починаючи з 16 років. Разом з тим, як вже було раніше зазначено, країни-учасниці мають право понизити цей вік до 13 років. Як і в CCPA, згода на опрацювання персональних даних за особу, яка молодша за вказаний вік, повинна надаватись її батьками. Таким чином, якщо CCPA передбачає необхідність надання такої згоди щодо продажу персональних даних, то GDPR стосовно усього спектру їх опрацювання [103, с. 4].

У GDPR та CCPA закріплені різні підходи до контролерів та суб'єктів господарювання, які не мають відомостей про те, що вони здійснюють

опрацювання персональних даних саме дітей. Зокрема, GDPR не передбачає жодних виключень для таких контролерів. Більш того, відповідно до GDPR, інформація стосовно опрацювання персональних даних повинна надаватись дітям у «стислій, прозорій, зрозумілій та легкодоступній формі, використовуючи зрозумілу мову, яку дитина може легко зрозуміти». У свою чергу, CCPA закріплено виняток стосовно суб'єктів господарювання, які не мають відомостей про вік дитини. Отже, контролери, які підпадають під регулювання GDPR зобов'язані докласти додаткові зусилля для того, щоб дізнатись справжній вік суб'єкта персональних даних, коли суб'єкти господарювання, що підпадають під вимоги CCPA, не мають такого обов'язку [104, с. 20].

Для порівняння рівня забезпечення прав суб'єктів персональних даних у GDPR та CCPA братимуться до аналізу такі права: право на видалення, право бути проінформованим, право на заперечення, право на доступ, право на недопущення дискримінації та право на портативність персональних даних [104, с. 26-35].

Стосовно права на видалення персональних даних, варто вказати, що в обох нормативно-правових актах це право закріплено: у CCPA це стаття 1798.105, а у GDPR - стаття 17, у якій це право має назву ще як «право бути забутим» [103, с. 5; 99, с. 3, 4; 8, с. 51]. Відповідно до статті 17 GDPR, персональні дані повинні бути видалені, якщо наявна одна з таких шести підстав: (1) немає більше потреби в опрацюванні; (2) суб'єкт персональних даних відкликав згоду і при цьому немає інших підстав для опрацювання; (3) суб'єкт персональних даних проти опрацювання відповідно до статті 21(1) GDPR; (4) персональні дані були опрацьовані у незаконний спосіб; (5) видалення необхідне у зв'язку із необхідністю дотримання встановленого законом зобов'язання; та (6) персональні дані збирали у зв’язку із пропонуванням послуг інформаційного суспільства. Також у частині третій цієї ж статті зазначені випадки, коли це право не застосовується [8, с. 51, 52].

Статтею 1798.105 CCPA передбачено, що користувач має право вимагати у суб'єктів господарювання видалення усіх персональних даних про користувача

та які були отримані від користувача. У той самий час, згідно із цією ж статтею, існують випадки, коли суб'єкти господарювання не повинні задовольняти вимогу про видалення персональних даних [99, с. 3, 4].

Таким чином, у GDPR та CCPA право на видалення персональних даних реалізоване схожим чином, хоча і є певні відмінності. Зокрема, для видалення персональних даних, відповідно до GDPR, повинна бути наявною одна із шести підстав. У той самий час, CCPA не визначає жодних підстав для видалення персональних даних (окрім того, що персональні дані повинні бути зібрані від користувача), що свідчить про більший рівень абсолютності цього права. Разом з тим, CCPA надає більше підстав для суб'єктів господарювання для відмови від реалізації цього права, у порівнянні із GDPR [103, с. 5].

Як у GDPR, так і у CCPA закріплені положення стосовно інформації, яка має бути надана суб'єктам персональних даних у зв'язку з опрацюванням персональних даних. У GDPR це право закріплене у статтях 5, 12, 13, 14, а у CCPA у статтях 1798.100(b), 1798.130(a), 1798.135 [104, с. 28].

В обох нормативно-правових актах передбачений обов'язок інформування суб'єктів персональних даних стосовно категорій опрацьованих (у випадку із GDPR) або зібраних (у випадку із CCPA) персональних даних, а також стосовно цілей опрацювання або використання персональних даних. Крім цього, суб'єкти господарювання та контролери зобов'язані повідомляти суб'єктів персональних даних про їх права та способи їх реалізації, а, відповідно до GDPR, також контактну інформацію посадової особи із захисту персональних даних [104, с. 28].

Відмінності у способі закріплення права бути проінформованим між GDPR та CCPA полягає в такому: по-перше, GDPR передбачає значно ширший перелік інформації, яка має бути надана суб'єкту персональних даних, а, по-друге, CCPA передбачає обов'язок перегляду політики конфіденційності кожні 12 місяців, у той час як у GDPR не закріплений такий обов'язок [104, с. 29].

Право на заперечення також закріплене як в GDPR, так і в CCPA. У GDPR це право передбачене у статті 21, а у CCPA у статтях 1798.120, 1798.135 [104, с.

30]. Відповідно до статті 21 GDPR, суб'єкт персональних даних може заперечувати проти опрацювання його даних, якщо таке опрацювання здійснюється у зв'язку із виконанням завдань у суспільних інтересах, здійснення офіційних повноважень або якщо воно необхідне для цілей законних інтересів контролера або третьої сторони. Крім цього, суб'єкт персональних даних може також заперечувати проти опрацювання, яке здійснюється для цілей прямого маркетингу [8, с. 53].

У той же час, згідно із статтею 1798.120 CCPA, суб'єкт персональних даних має право у будь-який час заборонити суб'єкту господарювання продавати його персональні дані третім особам (right to opt-out). Окрім цього, є також положення стосовно обов'язку повідомлення суб'єктів персональних даних про те, які дані, можливо, будуть продаватись, а також про наявність у суб'єкта персональних даних такого права. Також у тій ж статті передбачена заборона на продаж персональних даних осіб, яким менше 16 років. У статті 1798.135 CCPA більш детально регламентовані додаткові дії, які повинні бути вчинені суб'єктом господарювання на виконання права на заперечення [99, с. 6].

Проаналізувавши спосіб закріплення права на заперечення GDPR та CCPA, слід зазначити, що між цими актами існують значні відмінності. GDPR передбачає вичерпний перелік випадків, коли суб'єкт персональних даних може заперечувати проти опрацювання персональних даних. У той самий час, CCPA передбачає безумовне право на заперечення проти продажу персональних даних третім особам, але жодним чином не регламентує інші способи опрацювання таких даних [104, с. 31].

Щодо права на доступ варто зазначити, що у двох нормативно-правових актах передбачене це право. Зокрема, у GDPR це стаття 15, а у CCPA – 1798.100, 1798.110 та 1798.115 [103, с. 4]. Відповідно до статті 15 GDPR, суб'єкт персональних даних має право на підтвердження факту опрацювання персональних даних, на їх доступ, а також доступ до інформації, перелік якої зазначений у цій статті. Це право може бути реалізоване шляхом надання копій

персональних даних, які опрацьовуються. При цьому, контролер має право на стягнення розумної плати, у зв'язку із адміністративними витратами [8, с. 50, 51].

У статті 1798.100 CCPA передбачене право, за своєю суттю, такого ж змісту, що і у статті 15 GDPR - суб'єкт персональних даних має право на доступ до своїх персональних даних за умови подання відповідного запиту на їх отримання. Разом з тим, у пункті (d) цієї статті передбачено, що суб'єкт персональних даних у будь-який час може запитувати персональні дані, які опрацьовуються, але суб'єкти господарювання не зобов'язані надавати такі персональні дані частіше, аніж двічі на 12 місяців. Крім цього, додатково у статтях 1798.110 та 1798.115 CCPA зазначений перелік інформації, яка повинна бути розкрита суб'єкту персональних даних за його вимогою у зв'язку із збиранням або продажем персональних даних [99, с. 3-6].

Таким чином, право на доступ має схоже вираження у GDPR та CCPA. За CCPA, відмінність полягає в обмеженій кількості надання персональних даних суб'єкту таких даних (а саме не частіше, ніж двічі на 12 місяців), а також у різному переліку додаткової інформації, яка повинна бути розкрита за умови подання відповідного запиту.

Наступне право, закріплення якого аналізується - це право на недопущення дискримінації. Варто зазначити, що в GDPR немає норми, яка б прямо вказувала на застосування цього принципу [104, с. 33]. Разом з тим, непрямо у тексті GDPR можна прослідити те, що організації не можуть дискримінувати суб'єктів персональних даних у зв'язку з реалізацією своїх прав [103, с. 6].

У CCPA це право закріплено у більш очевидний спосіб, а саме у статті 1798.125 [103, с. 6]. Відповідно до цієї статті, суб'єкти господарювання не можуть дискримінувати користувачів у зв'язку із реалізацією прав, які передбачені CCPA. Зокрема, але не виключно, така дискримінація може проявлятись у формі відмови надання товарів чи послуг або встановлення іншої ціни за такі товари чи послуги [99, с. 6, 7].

Отже, як за регулюванням ЄС, так і за регулюванням штату Каліфорнія, суб'єкти господарювання не мають права дискримінувати у різний спосіб

суб'єктів персональних даних у зв'язку із реалізацією своїх прав. Разом з тим, GDPR, на відміну від CCPA, не закріплює норми яка б очевидно забороняла таку дискримінацію, що, на нашу думку, є недоліком GDPR.

Останнє право, яке аналізується у порівняльному аспекті - це право на портативність персональних даних. Це право передбачене як у GDPR (стаття 20), так і у CCPA (стаття 1798.100) [103, с. 5]. У статті 20 GDPR зазначено таке: «суб'єкт даних повинен мати право на отримання його або її персональних даних, які він надав контролеру, в структурованому, загальноприйнятому форматі, що легко зчитується машиною, та мати право на передавання таких даних іншому контролеру без перешкод від контролера, якому було надано персональні дані […]». Тим не менш, право на отримання або передачу персональних даних іншому контролеру може бути реалізоване лише у випадку, (1) якщо опрацювання є автоматизованим та (2) якщо опрацювання здійснюється на підставі згоди суб'єкта персональних даних або якщо таке опрацювання необхідне для виконання договору (контракту), стороною якого є суб'єкт персональних даних [8, с. 52-53].

Відповідно до пункту (d) статті 1798.100 CCPA, персональні дані повинні бути надані у портативному форматі, що дозволяло б суб'єкту персональних даних безперешкодно передавати персональні дані іншому суб'єкту господарювання [99, с. 3].

Аналізуючи форми відображення права на портативність персональних даних, слід зазначити, що це право передбачене у повній мірі як у GDPR, так і у CCPA, хоч і є дві відмінності. Перша відмінність полягає у абсолютності цього права у CCPA, адже GDPR передбачений виключний перелік обставин, за яких персональні дані можуть надаватись у портативному форматі, а, відповідно до CCPA, не передбачено жодних додаткових обставин. Другою відмінністю є те, що GDPR накладає більше обов'язків на контролерів, аніж CCPA на суб'єктів господарювання. Зокрема, за GDPR суб'єкт персональних даних має право вимагати від контролера передачі персональних даних іншому контролеру, а за CCPA на суб'єкта господарювання покладаються обов'язок лише надати

персональні дані у такому форматі, щоб він міг сам передати ці дані іншому суб'єкту господарювання.

Останнім порівняльним аспектом є відповідальність за порушення норм, які передбачені GDPR та CCPA. Питання санкцій передбачене у статтях 83 та 84 GDPR, а також у статті 1798.155 CCPA [103, с. 7]. Відповідно до статті 83 GDPR, накладення адміністративних штрафів повинно здійснюватися, перш за все, у дієвий, пропорційний та стримуваний спосіб. Також у цій статті зазначений перелік критеріїв, на які повинна звертатись «належна увага» при застосування кожного штрафу. Зокрема, але не виключно, такими критеріями є умисність, тяжкість, тривалість правопорушення, категорії персональних даних, щодо яких відбулось порушення тощо. Загалом у статті передбачений різний розмір штрафів стосовно різних правопорушень. Разом з тим, найбільший розмір санкцій складає 20 000 000 євро або 4% від загального глобального річного обігу за попередній фінансовий рік у залежності від того, яка сума є більшою. Окрім цього, відповідно до статті 84 GDPR, країни-учасниці можуть встановлювати додаткові санкції за порушення GDPR, які не встановлені у статті 83 [8, с. 91-93].

Статтею 1798.155 CCPA, у свою чергу, суб'єктам господарювання надається 30 днів для усунення порушення після відповідного повідомлення про наявність порушення. Загалом, розмір штрафних санкцій складає 2 500 доларів США за кожне порушення або 7 500 доларів США за кожне умисне порушення [99, с. 20, 21].

Незважаючи на те, що розмір санкцій, відповідно до обох нормативно-правових актів, є різним, накладення санкцій може спричинити «значну економічну відповідальність» для контролерів та суб'єктів господарювання [103, с. 7]. Також слід звернути увагу на характер застосування відповідальності. За GDPR (на відміну від CCPA) не надається додаткового строку для усунення порушення, що означає більш суворий підхід до потенційних порушників.

ВИСНОВКИ ДО РОЗДІЛУ 2

У США підхід до регулювання захисту персональних даних значно відрізняється від підходу, який існує у ЄС. Зокрема, у США функціонує велика кількість нормативно-правових актів у різних галузях, які одночасно також регулюють питання захисту персональних даних, але лише в межах регульованої галузі. У той самий час, у США відсутній єдиний нормативно-правовий акт на кшталт GDPR.

Разом з тим, тенденція поступово змінюється та у 2018 році у штаті Каліфорнія було прийнято CCPA, який регулює захист персональних у всіх галузях та є у певній мірі схожим до GDPR. Після штату Каліфорнія, подібні міжгалузеві нормативно-правові акти були також прийняті у штатах Мен та Невада.

З метою створення єдиного регулювання, дві партії - демократична та республіканська - презентували два законопроекти, які мають схожі риси - COPRA та CDPA відповідно. Ці законопроекти мають схожу сферу дії, схожі виключення у застосуванні стосовно малих суб'єктів господарювання та майже однакове визначення персональних даних.

Загалом, у США відсутнє єдине визначення персональних даних - воно може відрізнятись в залежності від нормативно-правових актів та штатів. Разом з тим, є три підходи стосовно визначення персональних даних: тавтологічний підхід, непублічний підхід та підхід конкретного типу.

Значну увагу у цьому розділі було приділено аналізу CCPA, оскільки (1) це є перший нормативно-правовий акт у США, який створив вичерпне регулювання у цій сфері; (2) федеральні законопроекти у великій мірі відображують регулювання, яке встановлене CCPA; (3) у штаті Каліфорнія здійснюється велика кількість опрацювання персональних даних, у зв'язку з тим, що цей штат складає 15 відсотків від усієї економіки США.

CCPA поширюється не на усіх суб'єктів господарювання. Його сфера дії обмежена територіально, певним колом суб'єктів персональних даних, а також за

грошовим показником. Іншими словами, CCPA поширюється на суб'єктів господарювання, які здійснюють свою діяльність в межах штату Каліфорнії, збирають персональні дані резидентів цього штату, визначають цілі та засоби опрацювання, а також мають або річний валовий дохід понад 25 мільйонів доларів США, або щорічно купують, отримують з комерційною метою, продають або діляться персональними даними 50 000 або більше споживачів, домогосподарств чи пристроїв, або отримують 50 чи більше відсотків своїх щорічних доходів від продажу персональних даних споживачів.

У порівнянні із GDPR, сфера дії CCPA поширюється на значно вужче коло суб'єктів, хоча й також має ознаки екстериторіальності. Також CCPA має дещо схожий суб'єктний склад осіб, які здійснюють опрацювання персональних даних - у GDPR це контролери та оператори, а у CCPA ті ж функції виконують суб'єкти господарювання та надавачі послуг.

Стосовно закріплених прав суб'єктів персональних даних, варто зробити висновок, що вони є схожими у GPDR та CCPA із незначними відмінностями. Разом з тим, право на недопущення дискримінації прямо не закріплене у тексті GDPR, а у CCPA це право закріплене у більш прямий спосіб.

Щодо розміру штрафних санкцій за порушення законодавства у сфері захисту персональних даних, слід зазначити, що у GDPR і CCPA застосовується різний підхід, але, водночас, обидва підходи потенційно спричиняють значні наслідки для контролерів та суб'єктів господарювання, що створює значний економічний тиск на них. Тим не менш, за CCPA також надається певний строк для усунення порушення, чого немає у GDPR.

РОЗДІЛ 3. ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ

3.1. Аналіз українського законодавства у сфері захисту персональних даних та його відповідності нормам General Data Protection Regulation

Систему українського законодавства у сфері захисту персональних даних складають такі нормативно-правові акти та рішення: Конституція України, ЗУ «Про захист персональних даних», ЗУ «Про інформацію», Цивільний кодекс України, рішення Конституційного суду України, інші акти, у яких поодиноко згадуються норми, що регулюють такі правовідносини, а також міжнародні договори України, згода на обов'язковість яких надана Верховною Радою України [105; 106]. Як видається з цього переліку, в Україні, навіть у порівнянні із законодавством США, є значна кількість нормативно-правових актів, які регулюють питання захисту персональних даних.

На нашу думку, є необхідність приділити значну увагу основоположному нормативно-правовому акту у сфері захисту персональних даних в Україні – ЗУ «Про захист персональних даних». Цей закон було прийнято з метою імплементації положень Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року № 108 та Додаткового протоколу до цієї конвенції щодо органів нагляду та транскордонних потоків даних. Вказана конвенція та додатковий протокол були ратифіковані Верховною Радою України 06 липня 2010 року. Цією ратифікацією «Україна взяла на себе зобов’язання забезпечити право осіб на захист їх персональних даних, яке є невід’ємною складовою більш широкого права – на недоторканість приватного життя, гарантованого статтею 8 Конвенції про захист прав людини і основоположних свобод та статтею 32 Конституції України» [107, с. 1].

Відповідно до статті 2 ЗУ «Про захист персональних даних», персональними даними є відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [108].

Головченко В.В. вважає, що недолік такого визначення полягає у тому, що у ньому відсутні критерії, за якими можна відрізнити персональні дані від іншої інформації, зокрема від конфіденційної [105]. Згідно із статтею 7 ЗУ «Про доступ до публічної інформації», конфіденційною інформацією є 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 [109]. Схоже визначення конфіденційної інформації наведене у ЗУ «Про інформацію». Відповідно до статті 21 цього закону, конфіденційною інформацією є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень [110].

Таким чином, конфіденційна інформація має такі складові: (1) це є інформація, (2) доступ до неї обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, (3) може поширюватись у визначеному ними порядку.

На нашу думку, у визначенні і не має бути визначено критеріїв, за якими персональні дані можна було б чітко відрізнити від іншої інформації (на прикладі конфіденційної), оскільки ці види інформації не є взаємовиключними. Зокрема, у статті 5 ЗУ «Про захист персональних даних» зазначено, що персональні дані можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою [108]. Таким чином, персональні дані можуть бути одночасно конфіденційною інформацію, але не кожні персональні дані є конфіденційною інформацією та не кожна конфіденційна інформація є персональними даними.

Окрім цього, Конституційний суд України у своєму рішенні від 20 січня 2012 року № 2-рп/2012, даючи офіційне тлумачення статті 32 Конституції України зазначив, що персональні дані – «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» [111].

Таким чином, Конституційний суд України надав приклади даних, які слід вважати персональними, а також підтвердив думку, що персональні дані можуть бути одночасно конфіденційною інформацією.

Як вже було зазначено у першому розділі цієї роботи, персональними даними, відповідно до GDPR, є будь-яка інформація, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати [8, с. 40]. Порівнюючи із визначенням персональних даних, яке зазначено в українському законодавстві, слід зазначити, що воно майже не відрізняється від визначення, яке зазначено в GDPR. За своєю суттю, відмінність полягає лише у заміні слова «інформація» на «відомості».

Для того щоб порівняти загальне бачення регулювання захисту персональних даних українського законодавця та бачення, яке передбачене у GDPR, слід порівняти принципи регулювання, які зазначені у статті 6 ЗУ «Про захист персональних даних» із тими, які визначені у GDPR. У статті 6 вказаного закону визначені такі принципи: (1) конкретність і законність цілей; (2) відкритість і прозорість обробки; (3) точність, достовірність та оновлення в міру потреби персональних даних; (4) відповідність, адекватність та ненадмірність

персональних даних стосовно мети обробки; (5) тривалість обробки - не довше, ніж це необхідно для цілей, відповідно до яких персональні дані збирались [108; 112, с. 31]. У статті 5 GDPR зазначені такі принципи: законність, правомірність та прозорість; цільове обмеження; мінімізація даних; точність; обмеження зберігання; цілісність і конфіденційність; підзвітність [8, с. 42, 43].

Принципи, які зазначені у ЗУ «Про захист персональних даних», співпадають з підходом, який був вироблений Європейським судом з прав людини [112, с. 32], а також здебільшого із принципами, які зазначені у GDPR. Зокрема, (1) принципи конкретності і законності цілей, а також відкритості і прозорості обробки перегукуються із принципом законності, правомірності та прозорості у GDPR; (2) принцип точності, достовірності та оновлення в міру потреби персональних даних із принципами точності та мінімізації даних у GDPR; (3) принцип відповідності, адекватності та ненадмірності персональних даних стосовно мети обробки відповідає принципам цільового обмеження та обмеження зберігання за GDPR; а (4) принцип тривалості обробки не довше, ніж це необхідно для цілей, відповідно до яких персональні дані збирались відповідає принципу обмеження зберігання за GDPR. Таким чином, у національному законі відображені усі принципи, які зазначені у GDPR, за винятком принципів цілісності та конфіденційності, а також принципу підзвітності.

Замість термінів «контролер» та «оператор», які зазначені у GDPR [8], в ЗУ «Про захист персональних даних» використовуються терміни «володілець» та «розпорядник». Відповідно до статті 2 ЗУ «Про захист персональних даних», володільцем персональних даних є фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом [108]. В цілому, сутність володільця за українським законодавством є схожою до сутності контролера за GDPR. Різниця лише полягає у тому, що володілець визначає мету обробки, склад даних та процедури обробки, а контролер, відповідно до статті 4 GDPR - цілі та засоби

здійснення опрацювання [8, с. 40]. На нашу думку, функції володільця в Україні є тотожними функціям контролера у ЄС.

Стаття 2 ЗУ «Про захист персональних даних» визначає розпорядника як фізичну чи юридичну особу, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця [108]. Тут склалась аналогічна ситуація - поняття розпорядника за українським законодавством є аналогічним до поняття оператора за GDPR, адже оператор також опрацьовує персональні дані від імені контролера [8, с. 40].

Стосовно прав, які є у суб'єктів персональних даних, варто зазначити, що вони закріплені у статті 8 ЗУ «Про захист персональних даних» [108]. Коротко ці права вдало згруповані у науково-практичному посібнику, який виданий Радою Європи. Відповідно до цього посібника, суб'єкт персональних даних, за ЗУ «Про захист персональних даних», має такі права: (1) право на доступ до інформації про себе; (2) право на доступ до інформації про третіх осіб; (3) право на зміну, модифікацію, видалення персональних даних; (4) право знати про порядок обробки; (5) право на адекватний захист персональних даних [112, с. 79].

Право на доступ до інформації про себе включає такі складові частини 2 статті 8 ЗУ «Про захист персональних даних»: (1) право знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки; (2) право на отримання інформації про умови надання доступу до персональних даних; (3) право на доступ до своїх персональних даних; (4) право за запитом отримувати відповідь про те, чи обробляються його персональні дані, а також отримувати зміст таких персональних даних [108].

Найбільше складові права на доступ до інформації схожі на положення, які закріплені у статтях 12-15 GDPR, у яких передбачено перелік інформації, який має бути наданий суб'єкту персональних даних у разі збирання персональних даних, а також складові права на доступ до інформації [8, с. 47-51].

Відповідно до частини 2 статті 8 та частини 2 статті 12 ЗУ «Про захист персональних даних», право на доступ до інформації про третіх осіб включає: (1) право знати про місцезнаходження або місце проживання (перебування)

володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам; (2) право отримувати інформацію про третіх осіб, яким передаються його персональні дані; (3) право повідомлятись про володільця персональних даних, склад та зміст зібраних персональних даних, свої права, визначені законом, мету збору персональних даних та осіб, яким передаються його персональні дані [108]. У GDPR схожі права закріплені у тих ж 12-15 статтях [8, с. 47-51].

Та ж стаття 8 ЗУ «Про захист персональних даних» визначає, що суб'єкт персональних даних має право на пред'явлення вмотивованої вимоги щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними. Більш детально це право визначене у статтях 15 та 20 ЗУ «Про захист персональних даних» [108]. Це право кореспондує із правом на виправлення та правом на стирання (або правом бути забутим), які закріплені у статтях 16, 17 GDPR [8, с. 51, 52].

Право на зміну за українським законодавством відрізняється від права на виправлення за GDPR. У статті 20 ЗУ «Про захист персональних даних» визначено, що для зміни персональних даних необхідне подання вмотивованої письмової вимоги [108]. У той самий час, відповідно до статті 16 GDPR, контролер повинен здійснити виправлення без обов'язкового подання саме письмової вимоги, що, на нашу думку, відповідає вимогам часу [8, с. 51]. Порівнюючи право на видалення, яке закріплене у статті 15 ЗУ «Про захист персональних даних» та статті 17 GDPR, слід зазначити, що GDPR встановлює більшу кількість підстав для видалення персональних даних. Разом з тим, GDPR закріплює перелік винятків, коли вказані підстави можуть не застосовуватись та персональні дані не видалятись, а національне законодавство таких підстав не встановлює [8, с. 51, 52; 108].

Право знати про порядок обробки закріплене у тій ж статті 8 ЗУ «Про захист персональних даних». У цій статті серед іншого зазначено, що суб'єкт персональних даних має право знати механізм автоматичної обробки

персональних даних [108]. У той самий час, у GDPR таке право відсутнє, у тому числі у змісті права на отримання інформації та права на доступ [8].

Право на адекватний захист персональних даних включає в себе, відповідно до статті 8 ЗУ «Про захист персональних даних», (1) право на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи; (2) право на звернення із скаргами на обробку своїх персональних даних до Уповноваженого або до суду; (3) право на застосовування засобів правового захисту в разі порушення законодавства про захист персональних даних [108]. У GDPR також зазначені механізми захисту персональних даних, а саме: право на подання скарги до наглядового органу (стаття 77), право на дієвий судовий засіб правового захисту проти наглядового органу (стаття 78) та право на дієвий судовий засіб правового захисту проти контролера або оператора (стаття 79) [8, с. 89, 90]. Таким чином, як в національному законодавстві, так і в GDPR регулюється питання механізмів захисту персональних даних, хоч і в різний спосіб.

Незважаючи на схожість закріплених прав у національному законодавстві України та GDPR, більшість прав, які закріплені у ЗУ «Про захист персональних даних» мають декларативний характер та, на відміну від GDPR, не деталізуються в окремих статтях [8; 108]. На нашу думку, це є значним недоліком, адже недостатня деталізація дозволяє тлумачити володільцям та розпорядникам права суб'єктів персональних даних на власний розсуд, що однозначно не сприяє захисту прав таких суб'єктів.

Окрім власне українських нормативно-правових актів, до українських юридичних осіб також застосовуються норми GDPR, положення якого були проаналізовані у першому розділі. Умови щодо застосування положень GDPR до українських юридичних осіб в жодній мірі не відрізняються від умов

застосування положень GDPR щодо юридичних осіб будь-якої іншої країни, яка не є країною-учасницею [113].

Підставою для застосування є екстериторіальна сфера дії GDPR, яка закріплена у статті 3 GDPR:

«Цей Регламент застосовують до опрацювання персональних даних в контексті діяльності осідку контролера або оператора в Союзі, незалежно від того, чи відбувається власне опрацювання в межах Союзу чи ні.

Цей Регламент застосовують до опрацювання персональних даних суб'єктів даних, які перебувають у Союзі, контролером або оператором, який має осідок поза межами Союзу, якщо опрацювання даних пов'язано з:

(a) постачанням товарів чи наданням послуг таким суб'єктам даних у Союзі, незалежно від того, чи вимагають оплату від таких суб'єктів даних; або

(b) моніторингом поведінки суб'єктів даних, якщо така поведінка має місце у межах Союзу» [8, с. 39, 40].

Якщо юридична особа встановлює ту обставину, що вона підпадає під дію однієї з вищевказаних частин статті 3 GDPR, «то неважливо в якому статусі по відношенню до опрацьованих персональних даних вона перебуває - чи то в статусі оператора, чи то в статусі контролера» [114]. З тексту GDPR можна виокремити два критерії, за наявності одного з яких він застосовується екстериторіально: «критерій осідку» (англ. «establishment criterion») та «критерій таргетування» (англ. «targeting criterion») [115, с. 3].

Стосовно критерію осідку, слід зазначити, що аналізуючи частину 1 статті 3 GDPR, можна виокремити такі концепції:

1. «осідок»;
2. «опрацювання персональних даних в контексті діяльності осідку контролера або оператора в Союзі»;
3. «незалежно від того, чи відбувається власне опрацювання в межах Союзу чи ні» [116, с. 1].

Відповідно до рішень Суду Європейського Союзу, поняття «осідок» тлумачиться досить широко. Суд у справі Weltimmo постановив, що будь-яка

«реальна та ефективна діяльність, навіть мінімальна», яка здійснюється через стійку організацію може бути достатньою для того, щоб відповідати поняттю «осідок» у праві захисту персональних даних ЄС [116, с. 1, 2; 117]. При цьому, у пункті 22 преамбули GDPR зазначено, що не є визначальним фактором яким чином здійснюється така організація - через відділення чи через філію із статусом юридичної особи [8, с. 5]. Фактично суд визначив, що достатньо, щоб контролер:

1. «здійснював управління веб-сайтом, який «в основному або повністю спрямований» на конкретну країну-учасницю;
2. призначив представника у країні-учасниці, яка несе відповідальність за стягнення заборгованості, що виникає внаслідок діяльності, і за представництво контролера даних в адміністративних і судових процесах, пов'язаних з обробкою відповідних даних» [118].

Більш того, Європейська рада захисту даних (далі - ЄРЗД) визначає, що за певних обставин, присутність у ЄС навіть одного працівника або агента компанії, яка не зареєстрована у ЄС, «може бути достатньою підставою для визнання таких відносин «стійкою організацією», якщо такий працівник або агент діє з достатньою мірою постійності». Тим не менш, «необхідно наголосити на тому, що таке визнання повинно бути зроблене окремо у кожній справі стосовно (1) міри постійності організації та (2) ефективного здійснення діяльності у країні-учасниці, враховуючи особливості ведення господарської діяльності та надання відповідних послуг» [115, с. 5; 116, с. 2].

Стосовно концепції «опрацювання персональних даних в контексті діяльності осідку контролера або оператора в Союзі», ЄРЗД зазначила, що якщо існує «нерозривний зв’язок між осідком у ЄС та обробкою даних, що здійснюється суб’єктом, який не є членом ЄС, GDPR буде застосовуватись до такої обробки даних, незважаючи на те, що суб'єкт господарювання ЄС не відіграє ролі в обробці персональних даних» [115, с. 7, 116, с. 3].

Наприклад, «у справі Google Spain SL проти EFPD громадянин Іспанії звернувся до Google з вимогою не відображати певну інформацію стосовно

нього. Тим не менш, така діяльність здійснюється Google Inc., яка розташована у США». Google Spain SL лише займається маркетинговою діяльністю, не пов'язана з пошуком даних та, відповідно, опрацюванням персональних даних. «Суд Європейського Союзу визнав, що існує нерозривний зв'язок між діяльністю Google Spain SL та Google Inc., оскільки маркетингова діяльність є одним з способів надання послуг з пошуку економічної рентабельності, а пошукова система, своєю чергою, засобом, за допомогою якого здійснюється така маркетингова діяльність», й, таким чином, існує нерозривний зв'язок між цими юридичними особами [116, с. 3; 119].

Третя концепція «незалежно від того, чи відбувається власне опрацювання в межах Союзу чи ні» означає те, що «GDPR застосовується до суб'єкта господарювання, що має осідок у ЄС і здійснює обробку персональних даних у контексті своєї діяльності, навіть якщо така обробка відбувається поза межами ЄС» [116, с. 3].

Таким чином, допускається застосування GDPR щодо суб'єктів господарювання не-членів ЄС (у тому числі щодо України) навіть при мінімальній діяльності, яка здійснюється через стійку організацію, незалежно від того чи опрацювання персональних даних здійснюється у ЄС чи поза його межами.

Стосовно ж критерію таргетування, слід зазначити, що для того, щоб повною мірою розкрити зазначений критерій, слід розтлумачити такі поняття:

1. «суб'єкти даних, які перебувають у Союзі»;
2. «пропонування товарів чи надання послуг суб'єктам даних у Союзі»;
3. «моніторинг поведінки суб'єктів даних» [116, с. 3].

ЄРЗД зазначає, що «суб'єкти даних, які перебувають у Союзі» не обмежуються громадянством, місцем проживання або іншим типом правового статусу», «а вимога щодо знаходження суб'єкта даних на території ЄС має бути визначена саме в момент, коли пропонуються товари чи послуги або здійснюється моніторинг поведінки, незалежно від тривалості такої пропозиції чи моніторингу» [115, с. 13; 116, с. 4].

Однак, слід зазначити, що GDPR не застосовується лише через опрацювання персональних даних громадян ЄС або осіб, що мають відповідне місце проживання. У випадку обробки даних, продажу товару або надання послуг поза межами ЄС без відповідної рекламної кампанії або будь-якої іншої таргетингової діяльності, які спрямовані на осіб з ЄС, GDPR до такої компанії застосовуватись не буде [116, с. 4].

Стосовно поняття «пропонування товарів чи надання послуг суб'єктам даних у Союзі» має важливе значення та обставина, що таке постачання або надання може здійснюватись також безкоштовно, однак це не буде жодним чином впливати на застосування GDPR [116, с. 4].

Також необхідно враховувати те, що, відповідно до пункту 23 декларативної частини GDPR для встановлення факту пропонування товарів або постачання послуг контролером або оператором поза межами ЄС суб'єктам персональних даних, що перебувають у ЄС, необхідно переконатися у тому, чи є очевидним те, що контролер або оператор передбачає постачання послуг суб'єктам персональних даних в одній або декількох країнах-учасницях ЄС [8, с. 5].

Більш того, згідно із тим ж пунктом 23 декларативної частини GDPR, власне доступність у рамках Союзу веб-сайту контролера, оператора або посередника, електронної адреси чи іншої контактної інформації, або використання мови, що є загальновживаною в третій країні, де має осідок контролер, є недостатньою умовою для встановлення такого наміру; такі фактори як використання мови або валюти, що є загальноприйнятими в одній або декількох державах-членах, із можливістю замовити товари чи послуги тією іншою мовою, або згадування споживачів чи користувачів, що перебувають у Союзі, підтверджують те, що контролер передбачає надання товарів або постачання послуг суб'єктам даних у Союзі [8, с. 5].

Щодо «моніторингу поведінки суб'єктів даних», то не кожне збирання та аналіз інформації суб'єктів ЄС буде вважатись моніторингом у контексті застосування Регламенту [115, с. 18; 116, с. 6]. Зокрема, за пунктом 24

декларативної частини GDPR, необхідно встановити, чи є фізичні особи об’єктами відстежування в Інтернеті, у тому числі, чи може мати місце подальше використання методик опрацювання персональних даних, що складаються з профайлінгу фізичної особи, зокрема для прийняття рішення щодо неї або нього чи для проведення аналізу, або передбачення її або його особистих переваг, поведінки чи ставлення [8, с. 6].

Так як вказане у попередньому абзаці цієї роботи застереження не є таким, з якого можна чітко зрозуміти що мається на увазі, ЄРЗД надає приклади моніторингу: «(1) поведінкова реклама; (2) гео-локалізаційна діяльність, зокрема для маркетингових цілей; (3) онлайн-відстеження за допомогою використання файлів cookie або інших методів, наприклад, відбитків пальців; (4) послуги персоналізованої дієтичної та медичної аналітики в Інтернеті; (5) відеонагляд; (6) маркетингові дослідження та інші поведінкові дослідження на основі особистих профілів; (7) відслідковування або регулярне звітування про стан здоров'я людини» [115, с. 18; 116, с. 6].

Отже, аналізуючи таргетинговий критерій, очевидним є те, що його застосування є гнучким, містить багато оціночних суджень та вирішується у кожному випадку окремо.

До прийняття GDPR країнам-учасницям важко було змусити дотримуватись законодавства із захисту персональних даних контролерів та операторів за межами ЄС [113]. Зокрема, відповідно до вимог Директиви 95/46/ЄС, яка діяла до прийняття GDPR, норми щодо захисту персональних даних застосовувались лише до суб’єктів, що знаходяться на території ЄС та Європейської Економічної Зони, а GDPR ж у повній мірі відрізняється у цьому контексті та поширюється на весь світ, включаючи Україну [114].

3.2. Аналіз судової практики стосовно захисту персональних даних та перспективи реформування українського законодавства у сфері захисту персональних даних

Відповідальність за порушення законодавства у сфері захисту персональних даних передбачена у статті 188-39 Кодексу України про адміністративні правопорушення (далі - КУпАП). Загалом цієї статтею передбачена відповідальність за такі порушення:

– Неповідомлення або несвоєчасне повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних або про зміну відомостей, які підлягають повідомленню згідно із законом, повідомлення неповних чи недостовірних відомостей;

– Невиконання законних вимог (приписів) Уповноваженого Верховної Ради України з прав людини або визначених ним посадових осіб секретаріату Уповноваженого Верховної Ради України з прав людини щодо запобігання або усунення порушень законодавства про захист персональних даних;

– Недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб’єкта персональних даних [120].

Для цілей написання цієї роботи найбільш доцільно проаналізувати судову практику стосовно останнього пункту. За порушення цієї норми встановлена відповідальність у вигляді накладення штрафу на громадян у розмірі від ста до п’ятисот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян - суб’єктів підприємницької діяльності - від трьохсот до однієї тисячі неоподатковуваних мінімумів доходів громадян. За повторне таке порушення передбачена відповідальність у вигляді штрафу від однієї тисячі до двох тисяч неоподатковуваних мінімумів доходів громадян [120]. Оскільки у пункті 5 підрозділу 1 розділу XX «Перехідні положення» Податкового кодексу України зазначено, що для цілей застосування неоподаткованого мінімуму доходів

громадян використовується сума в розмірі 17 гривень, межі відповідальності за порушення цієї частини статті 188-39 КУпАП становлять від 1700 до 34000 гривень, що очевидно не співвідноситься із розмірами штрафних санкцій, які закріплені у GDPR та CCPA [121; 8, с. 91-93; 99, с. 20, 21].

Слід також зазначити, що, відповідно до статті 255 КУпАП, уповноважені особи секретаріату Уповноваженого Верховної Ради України з прав людини або представники Уповноваженого Верховної Ради України з прав людини мають право складати протоколи про адміністративне правопорушення за статтею 188-39 КУпАП, але, згідно із статтею 221 КУпАП, саме судді районних, районних у місті, міських чи міськрайонних судів розглядають справи про адміністративні правопорушення за цією статтею [122]. Всього у Єдиному державному реєстрі судових рішень є 115 постанов, де б застосовувалась частина 4 статті 188-39 КУпАП [123].

У постанові Коломийського міськрайонного суду Івано-Франківської області від 13 березня 2020 року у справі № 346/5963/19 висвітлено одразу дві проблеми, з якими стикаються учасники правовідносин у сфері захисту персональних даних: (1) відповідальність за поширення публічно доступної інформації, яка вважається персональними даними та (2) реальність притягнення до адміністративної відповідальності в силу строків накладення адміністративного стягнення [124].

Суть справи полягає у тому, що керівник Управління освіти Коломийської міської ради поширив персональні дані певної особи у соціальній мережі «Facebook». Цими діями керівник не забезпечив належний рівень захисту персональних даних та порушив частину 3 статті 10 та частину 1 статті 24 ЗУ «Про захист персональних даних», та, відповідно, підлягає відповідальності за частиною 4 статті 188-39 КУпАП [124].

Стосовно проблеми відповідальності за поширення публічно доступної інформації, яка вважається персональними даними, слід зазначити, що керівник поширив інформацію про особу, яка є у відкритому доступі (зокрема, місце проживання), оскільки особа є співзасновником громадської організації та

фізичною особою-підприємцем, а тому такі відомості містяться Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань [125]. В результаті, суд визнав керівника винним у вчиненні адміністративного правопорушення, аргументуючи це тим, що на таке поширення персональних даних особою не було надано згоду [124].

У ЗУ «Про захист персональних даних» не зазначено про те, що персональні дані, які стали публічною інформацією, є випадком, стосовно якого не застосовується дія закону [108]. Разом з тим, на нашу думку, це є недоліком українського законодавства, а суд повинен був спиратись при вирішенні спору на фундаментальні права людини, а також на загальні принципи права. Також недоліком є те, що у Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань публікується інформація про місце проживання (місцезнаходження) особи. Очевидно, що така інформація є персональними даними, оскільки фізична особа у цьому випадку є ідентифікована.

Інша проблема, яка висвітлюється у цьому судовому рішенні є реальність притягнення до адміністративної відповідальності в силу строків накладення адміністративного стягнення. Незважаючи на те, що керівника було визнано винним у вчиненні адміністративного правопорушення, провадження було закрите у зв'язку із закінченням на момент розгляду справи строків накладення адміністративного стягнення [124]. Відповідно до статті 38 КУпАП, адміністративне стягнення може бути накладено не пізніш як через три місяці з дня вчинення правопорушення, що є надзвичайно малим строком, враховуючи, що розгляд справ за статтею 188-39 КУпАП здійснюється у судах. Таким чином, постає питання про реальність та невідворотність покарання за порушення цієї норми КУпАП, особливо якщо враховувати, що у цей строк, окрім судового розгляду, також складається протокол Уповноваженим [120; 122].

Окрім цього, цей строк є недостатнім зважаючи на те, що інколи протоколи про адміністративне правопорушення надходять до суду із недоліками. Зокрема, згідно із постановою Жовтневого районного суду міста Маріуполя Донецької

області від 17 січня 2020 року у справі № 263/16968/19, було надіслано протокол до суду із недоліками, а також згодом інший протокол, який також виявився із недоліками. Як наслідок, суд постановив повернути матеріали адміністративної справи до Секретаріату Уповноваженого Верховної Ради України для належного оформлення [126]. Таким чином, три місяці майже минули й, відповідно, адміністративне стягнення не було накладено [120; 123].

Ще однією проблемою притягнення до відповідальності за статтею 188-39 КУпАП є те, що суб'єктами відповідальності за КУпАП є лише фізичні особи [127, с. 75]. Наявність цієї проблеми висвітлено у постанові Київського апеляційного суду від 17 грудня 2019 року у справі № 756/12839/19. Постановою суду першої інстанції було визнано винним у вчиненні адміністративного правопорушення та накладено адміністративне стягнення у вигляді штрафу у розмірі 5100 гривень на начальника відділу з комунікації ПрАТ «ДТЕК КИЇВСЬКІ ЕЛЕКТРОМЕРЕЖІ». Суть порушення полягала у тому, що на офіційному сайті компанії були розміщенні персональні дані певної особи без її згоди. Рішення суду першої інстанції було оскаржено у Київському апеляційному суді [128].

Апелянт посилався на такі аргументи: (1) при розгляді справи у суді першої інстанції, його не було повідомлено про розгляд справи, чим були порушені його права; (2) не лише в апелянта є доступ до розміщення матеріалів на сайті компанії; (3) судом не було визначено час вчинення та виявлення правопорушення; (4) є сумніви у допустимості поданих доказів, на яких ґрунтувалось рішення суду першої інстанції [128].

Як наслідок, суд апеляційної інстанції задовольнив апеляційну скаргу, посилаючись на те, що «саме в разі коли до службових обов`язків посадової особи входить забезпечення дотримання установлених правил, недодержання яких ставиться у провину складеним протоколом, така особа повинна бути притягнута до адміністративної відповідальності, в тому числі за порушення, передбачене ч. 4 ст. 188-39 КУпАП». Разом з тим, у положенні відділу з комунікацій не зазначено обов'язок апелянта додержання встановленого

законодавством про захист персональних даних порядку захисту персональних даних. Таким чином, «припущення, що таке недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних сталось з вини особи, яка притягається до адміністративної відповідальності, не підтверджується жодним доказом, а отже, застосовуючи стандарт доведеності вини поза розумним сумнівом, слід усі сумніви з цього приводу тлумачити на користь апелянта» [128].

На нашу думку, підхід, який є у GDPR та CCPA, коли суб'єктом відповідальності може бути юридична особа [8, с. 91-93; 99, с. 20, 21], є більш ефективним, оскільки у суду в такому разі немає завдання встановити конкретну особу, яка вчинила правопорушення, що спрощує можливість притягнення до відповідальності.

Варто також зазначити, що окрім того, що судових справ, де розглядалось б питання порушення законодавства у сфері захисту персональних даних та було ухвалено постанову, всього 115, справ, де було б накладено адміністративне стягнення - ще менше. Із 115 ухвалених постанов, лише згідно з 10 постановами винних було притягнуто до адміністративної відповідальності за частиною 4 статті 188-39 КУпАП. При цьому, розмір штрафу жодного разу не перевищив 5100 гривень. Більшість інших проваджень були закриті, у зв'язку з закінченням строків, передбачених статтею 38 КУпАП [123].

Здійснивши аналіз національного законодавства та судової практики, для належного захисту персональних даних в Україні, на нашу думку, слід вчинити такі дії: (1) оновити законодавство до стандартів GDPR; (2) створити незалежного регулятора із повноваженнями притягнення до відповідальності; (3) вивести норми стосовно відповідальності з дії КУпАП із створенням можливості притягнення до відповідальності юридичних осіб (на кшталт антимонопольного законодавства [129]); (4) збільшити розмір штрафних санкцій щодо юридичних осіб; (5) врегулювати питання поширення персональних даних, які є одночасно є у публічному доступі.

В рамках реформування національного законодавства у сфері захисту персональних даних, у серпні 2018 року при Секретаріаті Уповноваженого було створено Координаційну раду з удосконалення законодавства про захист персональних даних. Як результат роботи цієї Координаційної ради разом із експертами проекту Twinning, який був створений з метою «посилення інституційного потенціалу Секретаріату Уповноваженого Верховної Ради України з прав людини» [130], було розроблено проект нової редакції ЗУ «Про захист персональних даних», у якому враховуються новели GDPR. Разом з тим, робота над цим проектом все ще триває [107, с. 2, 3].

ВИСНОВКИ ДО РОЗДІЛУ 3

Система українського національного законодавства у сфері захисту персональних даних містить в собі значну кількість нормативно-правових актів, включаючи Конституцію України, закони України, рішення Конституційного суду України, а також міжнародні договори України, згода на обов'язковість яких надана Верховною Радою України. Разом з тим, профільним законом у цій сфері є ЗУ «Про захист персональних даних», який було прийнято з метою імплементації міжнародних зобов'язань.

Визначення персональних даних закріплене у профільному законі із певною конкретизацією Конституційного суду України. При цьому, визначення, яке закріплене у національному законодавстві, незважаючи на його критику, майже не має відмінностей від визначення, що закріплене у GDPR.

Порівнюючи принципи, які зазначені у ЗУ «Про захист персональних даних» та GDPR, слід зробити висновок, що у національному законі відображені усі принципи, які зазначені у GDPR, за винятком принципів цілісності та конфіденційності, а також принципу підзвітності.

Окрім цього, у національному законі та GDPR схожий суб'єктний склад. Замість термінів «контролер» та «оператор», які зазначені у GDPR, в ЗУ «Про

захист персональних даних» використовуються терміни «володілець» та «розпорядник», що за своєю суттю є майже тотожними поняттями.

В цілому, права суб'єктів персональних даних є також значною мірою схожими у цих нормативно-правових актах. Разом з тим, національним законом передбачене право знати механізм автоматичної обробки персональних даних, у той час як GDPR таке право не передбачається.

Зважаючи на принцип екстериторіальності, через призму критерію осідку й критерію таргетування, до українських суб'єктів також застосовуються норми GDPR. У той самий час, умови застосування GDPR до українських суб'єктів не відрізняються від умов застосування до суб'єктів з будь-якої іншої країни, яка не є членом ЄС.

У цьому розділі також було проаналізовано судову практику стосовно статті 188-39 Кодексу України про адміністративні правопорушення у межах відповідальності за недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб’єкта персональних даних.

У результаті аналізу судової практики, було виявлено проблеми, що стосуються особливостей притягнення до адміністративної відповідальності винних осіб, невідворотності покарання, а також невеликого розміру штрафних санкцій.

ВИСНОВКИ

Здійснене у цій магістерській роботі дослідження стосовно особливостей правового регулювання захисту персональних даних у ЄС, окремих країнах-учасницях ЄС, США та Україні дозволило сформувати такі висновки.

1. Нормативно-правові акти у ЄС у сфері захисту персональних даних поділяються на ті, що діють на території всього ЄС, та національні (діють лише в межах окремої країни-учасниці ЄС). При цьому, регулювання, що діє на території всього ЄС, має пріоритетну силу над національним законодавством країн-учасниць ЄС. До 25 травня 2018 року на території ЄС у сфері захисту персональних даних діяла Директива 95/46/ЕС, яка втратила чинність із прийняттям GDPR. При цьому, GDPR не потребує подальшої імплементації країнами-учасницями ЄС і автоматично зменшує рівень їх дискреції щодо виконання GDPR у порівнянні з Директивою 95/46/ЕС.

Відповідно до пункту 1 статті 4 GDPR, персональними даними є будь-яка інформація, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати. Не існує виключного переліку інформації, яка вважається персональними даними. Більш того, певні категорії інформації можуть вважатись персональними даними в одній ситуації, але не вважатись такими в іншій. Основним критерієм оцінки того, чи вважається певна інформація персональними даними, є та обставина, чи достатньо цих даних для ідентифікації певної фізичної особи.

У статті 5 GDPR закріплені такі принципи опрацювання персональних даних: законність, правомірність та прозорість; цільове обмеження; мінімізація даних; точність; обмеження зберігання; цілісність і конфіденційність; підзвітність. Після проведеного аналізу, зроблено висновок, що концептуально за своїм змістом принципи, які закріплені у GDPR, майже не відрізняються від тих, що закріплені у Директиві 95/46/ЕС. Крім цього, зміст принципів точності й цілісності та конфіденційності не зазнали жодних змін за своєю суттю у порівнянні з Директивою 95/46/ЕС.

2. На нашу думку, для контролерів та операторів найбільш важливими положеннями GDPR щодо захисту персональних даних є те, що (1) опрацювання персональних даних має бути законним, (2) згода суб'єкта персональних даних на опрацювання персональних даних має відповідати встановленим GDPR критеріям, (3) оператори та контролери зобов'язані забезпечити суб'єктам персональних даних надання прозорої інформації, право на доступ й портативність даних, право бути забутим, право на виправлення та право на заперечення.

Застосування штрафних санкцій згідно із положеннями GDPR здійснюється у різних розмірах. Значна відмінність у розмірах штрафів спричиняється застосовною моделлю штрафів. Штрафні санкції вираховуються відповідно до світового річного обороту відповідної групи компаній. Так, більшість штрафних санкцій є порівняно незначними та не перевищують 10 000 євро. Разом з тим, є також поодинокі випадки накладення багатомільйонних штрафів на такі компанії й установи як 1&1 Telecom GmbH, Deutsche Wohnen SE, Marriott International Inc, British Airways[2], Google LLC та Орган державних доходів Болгарії. Штрафні санкції можуть бути накладені, окрім приватних суб'єктів господарювання, також на державні установи та фізичних осіб.

3. На основі здійсненого аналізу національного законодавства у сфері захисту персональних даних Великобританії, Німеччині, Франції та Ірландії, варто зазначити, що воно хоч і має певні особливості, але концептуально не відрізняється. У проаналізованих країнах був прийнятий власний нормативно-правовий акт, який регулює захист персональних даних шляхом доповнення та адаптації норм GDPR з певними національними особливостями. Також в усіх цих країнах був прийнятий акт, який імплементує європейську Директиву про конфіденційність 2002/58/ЕС. У Великобританії GDPR матиме чинність протягом перехідного періоду процедури виходу з ЄС - до 31 грудня 2020 року,

[2] Стосовно Marriott International Inc та British Airways британським регулятором був висловлений намір накласти штрафи

а після спливу цього строку GDPR буде діяти на загальних підставах - через призму застосування територіальної сфери дії.

4. У США підхід до регулювання захисту персональних даних значно відрізняється від підходу, який існує у ЄС. Зокрема, у США функціонує велика кількість нормативно-правових актів у різних галузях (наприклад, медицина, освіта тощо), які одночасно також регулюють питання захисту персональних даних, але лише в межах регульованої галузі. Також у США відсутній єдиний нормативно-правовий акт на кшталт GDPR. Разом з тим, тенденція поступово змінюється та у 2018 році у штаті Каліфорнія було прийнято CCPA, який регулює захист персональних у всіх галузях та є у певній мірі схожим до GDPR. Після штату Каліфорнія, подібні міжгалузеві нормативно-правові акти були також прийняті у штатах Мен та Невада.

На федеральному рівні підхід також починає змінюватись. З метою створення єдиного регулювання, дві партії - демократична та республіканська - презентували два законопроекти у сфері захисту персональних даних, які мають схожі риси - COPRA та CDPA відповідно. Ці законопроекти мають схожу сферу дії, схожі виключення у застосуванні стосовно малих суб'єктів господарювання та майже однакове визначення персональних даних.

5. У США замість терміну «персональні дані» здебільшого використовується термін «персональна ідентифікаційна інформація» (англ. «personally identifiable information»). Загалом, у США відсутнє єдине визначення персональних даних (інформації) - воно відрізняється в залежності від нормативно-правових актів та штатів. Разом з тим, є три підходи стосовно визначення персональних даних: тавтологічний підхід, непублічний підхід та підхід конкретного типу.

6. На нашу думку, для суб'єктів господарювання найбільш важливими положеннями CCPA щодо захисту персональних даних є те, що (1) CCPA застосовується лише до суб'єктів господарювання, які відповідають визначеним критеріям, (2) суб'єкти господарювання зобов'язані забезпечити суб'єктам персональних даних право на доступ, право на вимогу видалення персональних

даних, право на вимогу розкриття зібраної та поширеної інформації, право на вимогу розкриття категорій проданих персональних даних, право на відмову (opt-out) від продажу персональних даних та право на недискримінацію.

У порівнянні із GDPR, сфера дії CCPA поширюється на значно вужче коло суб'єктів, хоча й також має ознаки екстериторіальності. Тим не менш, CCPA має дещо схожий суб'єктний склад осіб, які здійснюють опрацювання персональних даних - у GDPR це контролери та оператори, а у CCPA ті ж функції виконують суб'єкти господарювання та надавачі послуг.

Стосовно закріплених прав суб'єктів персональних даних, варто зробити висновок, що вони є схожими у GPDR та CCPA із незначними відмінностями. Зокрема, право на недопущення дискримінації прямо не закріплене у тексті GDPR, а у CCPA це право закріплене у більш прямий спосіб. Щодо розміру штрафних санкцій за порушення законодавства у сфері захисту персональних даних, слід зазначити, що у GDPR і CCPA застосовується різний підхід, але, водночас, обидва підходи потенційно спричиняють значний економічний вплив на контролерів та суб'єктів господарювання. Разом з тим, за CCPA надається певний строк для усунення порушення, чого немає у GDPR.

7. Особливістю системи регулювання у сфері захисту персональних даних в Україні є значна кількість джерел. Разом з тим, є також і профільний нормативно-правовий акт, який сконцентрований на регулюванні захисту персональних даних - ЗУ «Про захист персональних даних».

На нашу думку, для володільців та розпорядників найбільш важливими положеннями українського законодавства щодо захисту персональних даних є те, що вони мають забезпечити суб'єктам персональних даних право на доступ до інформації про себе, право на доступ до інформації про третіх осіб, право на зміну, модифікацію, видалення персональних даних, право знати про порядок обробки та право на адекватний захист персональних даних.

Система регулювання у сфері захисту персональних даних в Україні ще більше ускладнюється у зв'язку з тим, що GDPR застосовується до українських контролерів та операторів через призму принципу екстериторіальності. Умови

застосування GDPR до українських суб'єктів не відрізняються від умов застосування до суб'єктів з будь-якої іншої країни, яка не є членом ЄС.

Стосовно порівняння регулювання захисту персональних даних, яке закріплене ЗУ «Про захист персональних даних» та того, яке закріплене GDPR, слід зазначити таке:

– визначення, яке закріплене у національному законодавстві, незважаючи на його критику, майже не має відмінностей від визначення, що закріплене у GDPR;

– у національному законі відображені усі принципи, які зазначені у GDPR, за винятком принципів цілісності та конфіденційності, а також принципу підзвітності;

– у національному законі та GDPR схожий суб'єктний склад - замість термінів «контролер» та «оператор», які зазначені у GDPR, в ЗУ «Про захист персональних даних» використовуються терміни «володілець» та «розпорядник», що за своєю суттю є майже тотожними поняттями;

– права суб'єктів персональних даних є значною мірою схожими у цих нормативно-правових актах, хоча національним законом передбачене право знати механізм автоматичної обробки персональних даних, у той час як GDPR таке право не передбачається.

8. У результаті аналізу судової практики, було виявлено такі проблеми: (1) притягнення до відповідальності за поширення публічно доступної інформації, яка вважається водночас також персональними даними, (2) відсутність невідворотності притягнення до адміністративної відповідальності в силу строків накладення адміністративного стягнення, (3) неможливість притягнення юридичної особи до відповідальності, (4) максимальний призначений розмір штрафу становить лише 5 100 гривень, (5) лише згідно з 10 постановами винних було притягнуто до адміністративної відповідальності за частиною 4 статті 188-39 КУпАП.

9. Здійснивши аналіз національного законодавства та судової практики, для належного захисту персональних даних в Україні, на нашу думку, слід вчинити такі дії.

(1) Оновити законодавство до стандартів GDPR.

Незважаючи на схожість закріплених прав у національному законодавстві України та GDPR, більшість прав, які закріплені у ЗУ «Про захист персональних даних» мають декларативний характер та, на відміну від GDPR, не деталізуються в окремих статтях. На нашу думку, це є значним недоліком, адже недостатня деталізація дозволяє тлумачити володільцям та розпорядникам спосіб реалізації прав суб'єктів персональних даних на власний розсуд, що однозначно не сприяє захисту прав таких суб'єктів.

Окрім цього, у національному законодавстві слід також закріпити принципи цілісності, конфіденційності та підзвітності, а також встановити підстави коли персональні дані можуть не видалятись за вимогою суб'єкта персональних даних.

(2) Створити незалежного регулятора із повноваженнями притягнення до відповідальності.

Враховуючи неефективність діяльності Уповноваженого Верховної Ради України з прав людини та суду, необхідно створити спеціалізовану установу, яка б вирішувала питання захисту персональних даних на кшталт тих, які існують у проаналізованих у цій роботі країнах-учасницях ЄС. Для належної ефективності такого органу, слід надати йому можливість накладати штрафні санкції на осіб, які порушують законодавство у цій сфері.

(3) Вивести норми стосовно відповідальності з дії КУпАП із створенням можливості притягнення до відповідальності юридичних осіб.

У зв'язку із тим, що, відповідно до КУпАП, накласти штрафні санкції можливо лише на посадових осіб юридичних осіб, а не на юридичну особу, у судовій практиці є проблема реальності притягнення до відповідальності за порушення законодавства у сфері захисту персональних даних, оскільки інколи неможливо встановити конкретну особу, яка винна у порушенні прав суб'єктів

персональних даних у той час, коли юридичну особу можна було б притягнути до відповідальності в аналогічній ситуації.

Окрім цього, реальність притягнення до відповідальності за КУпАП також ставиться під сумнів у зв'язку із застосуванням строків накладення адміністративного стягнення, які є надмалими та становлять всього три місяці з дня вчинення адміністративного правопорушення. Як наслідок, більшість проваджень закриваються за цією підставою, яка передбачена у статті 38 КУпАП.

(4) Збільшити розмір штрафних санкцій щодо юридичних осіб.

Однією з причин неефективності захисту прав суб'єктів персональних даних в Україні є невеликий розмір штрафних санкцій - максимальний призначений розмір штрафу становить лише 5 100 гривень, а максимальна межа в КУпАП становить 34 000 гривень. На нашу думку, розмір санкцій потрібно збільшити, але лише після встановлення можливості притягнення до відповідальності юридичних осіб. Доречним вважається підхід, який закріплений у GDPR у вигляді певного відсотку від річного фінансового обігу.

(5) Врегулювати питання поширення персональних даних, які одночасно є у публічному доступі.

В Україні такими персональними даними є, зокрема, дані про фізичну особу-підприємця, які опубліковані у Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань (наприклад, дані про місцезнаходження особи). За національною судовою практикою поширення таких даних без згоди суб'єкта персональних даних є порушенням ЗУ «Про захист персональних даних», що не відповідає принципу справедливості.

На нашу думку, лише за умови втілення цих рекомендацій можливий ефективний захист прав суб'єктів персональних даних, що водночас також відповідало б європейським стандартам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. URL: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (last accessed: 18.04.2020).

2. Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach: an official website of the Information Commissioner's Office. URL: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/ (last accessed: 18.04.2020).

3. British Airways faces record £183m fine for data breach. URL: https://www.bbc.com/news/business-48905907 (last accessed: 18.04.2020).

4. Preparing for the challenges and opportunities posed by GDPR. URL: https://tmt.bakermckenzie.com/en/thought-leadership/gdpr-national-legislation-survey (last accessed: 18.04.2020).

5. Precedence of European law: an official website of the European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14548 (last accessed: 17.01.2020).

6. Judgment of the European Court of Justice in case Flaminio Costa v. E.N.E.L. of 15 July 1964, court case No. 6/64. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61964CJ0006 (last accessed: 25.02.2020).

7. Data protection in the EU: an official website of the European Union. URL: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en (last accessed: 17.01.2020).

8. 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). URL: https://zakon.rada.gov.ua/laws/show/984_008-16 (дата звернення: 30.04.2020).

9. Difference between a Regulation, Directive and Decision. URL: https://www.usda-eu.org/eu-basics-questions/difference-between-a-regulation-directive-and-decision/ (last accessed: 17.01.2020).

10. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (last accessed: 17.01.2020).

11. The GDPR: What exactly is personal data? URL: https://www.itgovernance.eu/blog/en/the-gdpr-what-exactly-is-personal-data (last accessed: 20.02.2020).

12. What is personal data? : an official website of the Information Commissioner's Office. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/ (last accessed: 20.02.2020).

13. What is personal data? : an official website of the European Union. URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en (last accessed: 20.02.2020).

14. Purtova N. The law of everything. Broad concept of personal data and future of EU data protection law. Law, Innovation and Technology, Vol. 10, No. 1. P. 40-81.

15. Козюбра М.І., Погребняк С.П., Цельєв О.В., Матвєєва О.І. Загальна теорія права: підручник. Київ: Ваіте, 2015. 392 с.

16. 7 principles of the GDPR and what they mean. URL: https://www.amara-marketing.com/travel-blog/7-principles-of-the-gdpr-and-what-they-mean (last accessed: 17.01.2020).

17. The GDPR fundamental principles. URL: https://www.datainspektionen.se/other-lang/in-english/the-general-data-protection-regulation-gdpr/the-gdpr-fundamental-principles/ (last accessed: 17.01.2020).

18. Principle (a): Lawfulness, fairness and transparency: an official website of the Information Commissioner's Office. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/ (last accessed: 20.02.2020).

19. Gabel D., Hickman T. Chapter 6: Data Protection Principles – Unlocking the EU General Data Protection Regulation. URL: https://www.whitecase.com/publications/article/chapter-6-data-protection-principles-unlocking-eu-general-data-protection (last accessed: 17.01.2020).

20. Transparency and the GDPR: Practical guidance and interpretive assistance from the Article 29 Working Party: an official website of the International Association of Privacy Professionals. URL: https://iapp.org/news/a/transparency-and-the-gdpr-practical-guidance-and-interpretive-assistance-from-the-article-29-working-party/ (last accessed: 20.02.2020).

21. How to write clearly: an official website of the European Union. URL: https://op.europa.eu/en/publication-detail/-/publication/c2dab20c-0414-408d-87b5-dd3c6e5dd9a5/language-en (last accessed: 20.02.2020).

22. The GDPR: new opportunities, new obligations: an official website of the European Union. URL: https://ec.europa.eu/info/sites/info/files/data-protection-factsheet-sme-obligations_en.pdf (last accessed: 17.01.2020).

23. Data Controllers and Processors. URL: https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/ (last accessed: 17.01.2020).

24. Right of access: an official website of the Information Commissioner's Office. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/ (last accessed: 17.01.2020).

25. Right to data portability: an official website of the Information Commissioner's Office. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/ (last accessed: 17.01.2020).

26. Machine readable: Open Data Handbook. URL: https://opendatahandbook.org/glossary/en/terms/machine-readable/ (last accessed: 17.01.2020).

27. Right to erasure: an official website of the Information Commissioner's Office. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/ (last accessed: 17.01.2020).

28. Everything you need to know about the "Right to be forgotten". URL: https://gdpr.eu/right-to-be-forgotten/ (last accessed: 17.01.2020).

29. Right to rectification: an official website of the Information Commissioner's Office. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/ (last accessed: 17.01.2020).

30. Right to object: an official website of the Information Commissioner's Office. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/ (last accessed: 17.01.2020).

31. The GDPR Right to Object Explained. URL: https://www.hipaajournal.com/gdpr-right-to-object/ (last accessed: 17.01.2020).

32. Rights to object. URL: https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/33--guide-to-the-gdpr--rights-to-object.pdf?la=en (last accessed: 17.01.2020).

33. GDPR Enforcement Tracker. URL: https://www.enforcementtracker.com/ (last accessed: 06.02.2020).

34. BfDI imposes Fines on Telecommunications Service Providers: an official website of the European Union. URL: https://edpb.europa.eu/news/national-news/2019/bfdi-imposes-fines-telecommunications-service-providers_en (last accessed: 17.01.2020).

35. Heun S., Assion S. GDPR fine against a telecommunications provider in Germany - here are the key facts. URL:

https://www.lexology.com/library/detail.aspx?g=d0b2808c-1d5f-4629-8d26-34cdb74c8bf7 (last accessed: 17.01.2020).

36. Berlin Commissioner Issues Fine to Deutsche Wohnen SE. URL: https://www.huntonprivacyblog.com/2019/11/06/berlin-commissioner-issues-fine-to-deutsche-wohnen-se/ (last accessed: 17.01.2020).

37. Berlin Commissioner for Data Protection Imposes Fine on Real Estate Company: an official website of the European Union. URL: https://edpb.europa.eu/news/national-news/2019/berlin-commissioner-data-protection-imposes-fine-real-estate-company_en (last accessed: 17.01.2020).

38. Germany: Berlin Data Protection Authority imposes eur 14.5 million fine for "data cemetery". URL: https://blogs.dlapiper.com/privacymatters/germany-berlin-data-protection-authority-imposes-eur-14-5-million-fine-for-data-cemetery/ (last accessed: 17.01.2020).

39. Marriott International (MAR). URL: https://www.forbes.com/companies/marriott-international/#5b2f5c2e4fa0 (last accessed: 24.02.2020).

40. About British Airways: an official website of British Airways. URL: https://www.britishairways.com/en-gb/information/about-ba (last accessed: 24.02.2020).

41. UK data watchdog kicks £280m British Airways and Marriott GDPR fines into legal long grass. URL: https://www.theregister.co.uk/2020/01/13/ico_british_airways_marriott_fines_delayed/ (last accessed: 17.01.2020).

42. GDPR Fines Tracker & Statistics. URL: https://www.privacyaffairs.com/gdpr-fines/ (last accessed: 06.02.2020).

43. Google оштрафовано на €50 млн за порушення норм GDPR. URL: https://yur-gazeta.com/golovna/google-oshtrafovano-na-50-mln-za-porushennya-norm-gdpr.html (дата звернення: 25.02.2020).

44. За НАП: Официалният уебсайт на Национална агенция за приходите. URL: https://www.nap.bg/page?id=680 (последен достъп: 17.01.2020).

45. Breach Saga: Bulgarian Tax Agency Fined; Pen Testers Charged. URL: https://www.bankinfosecurity.com/bulgaria-fines-tax-office-penetration-testers-charged-a-13000 (last accessed: 17.01.2020).

46. Resolución de procedimiento sancionador No. PS/00334/2019. URL: https://www.aepd.es/es/documento/ps-00334-2019.pdf (último acceso: 25.02.2020).

47. CPO held liable for breach: Could it happen to you? : an official website of the International Association of Privacy Professionals. URL: https://iapp.org/news/a/south-korean-cpo-liability-charge-an-unwelcome-sight-globally/ (last accessed: 06.02.2020).

48. South Korean Court Imposes Personal Liability on Privacy Officer for Data Breach. URL: https://www.huntonprivacyblog.com/2020/01/09/south-korean-court-imposes-personal-liability-on-privacy-officer-for-data-breach/ (last accessed: 06.02.2020).

49. The UK has left the EU: the United Kingdom public sector information website. URL: https://www.gov.uk/transition?gclid=Cj0KCQiAqNPyBRCjARIsAKA-WFz78MmsKrTtqLmoW2OSzw_hzZ-brSsH6rx4IXkcbnFx6rp-m0QZbk0aAh7vEALw_wcB&gclsrc=aw.ds (last accessed: 25.02.2020).

50. UK Data Protection Act 2018 (DPA ACT) | 2020 Update. URL: https://www.cookiebot.com/en/data-protection-act-2018/ (last accessed: 06.02.2020).

51. About the DPA 2018: an official website of the Information Commissioner's Office. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/about-the-dpa-2018/ (last accessed: 25.02.2020).

52. The GDPR vs the DPA – What Exactly Is the Difference? URL: https://semafone.com/gb/blog-gb/the-gdpr-vs-the-dpa-what-exactly-is-the-difference/ (last accessed: 06.02.2020).

53. What is the difference between the DPA 2018 and the GDPR? (and why does it matter?). URL: https://www.dpocentre.com/difference-dpa-2018-and-gdpr/ (last accessed: 06.02.2020).

54. Digital Brief: The Brexit Edition. URL: https://www.euractiv.com/section/digital/news/digital-brief-the-brexit-edition/ (last accessed: 25.02.2020).

55. Judgment of the European Court of Human Rights in case Big Brother Watch and others v. the United Kingdom of 13 September 2018. URL: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-186048%22]} (last accessed: 25.02.2020).

56. Some aspects of UK surveillance regimes violate Convention. URL: https://www.euractiv.com/wp-content/uploads/sites/2/2018/09/Big-Brother-Watch-and-Others-v.-the-United-Kingdom-complaints-about-surveillance-regimes.pdf (last accessed: 25.02.2020).

57. Конвенція про захист прав людини і основоположних свобод: Міжнародний договір від 04.11.1950 р. № 995_004. Дата оновлення: 02.10.2013. URL: https://zakon.rada.gov.ua/laws/show/995_004 (дата звернення: 25.02.2020).

58. Brexit, GDPR and data protection: what happens if the UK becomes a third country? URL: https://dpnetwork.org.uk/brexit-gdpr-data-protection-uk/ (last accessed: 25.02.2020).

59. European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows: an official website of the European Union. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421 (last accessed: 25.02.2020).

60. An overview of UK Data Protection Law. URL: https://www.itgovernance.co.uk/data-protection (last accessed: 06.02.2020).

61. What are PECR? : an official website of the Information Commissioner’s Office. URL: https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/ (last accessed: 06.02.2020).

62. Data protection laws of the world: Germany. URL: https://www.dlapiperdataprotection.com/index.html?t=law&c=DE (last accessed: 06.02.2020).

63. EU GDPR vs. German Bundesdatenschutzgesetz – Similarities and Differences. URL: https://advisera.com/eugdpracademy/knowledgebase/eu-gdpr-vs-german-bundesdatenschutzgesetz-similarities-and-differences/ (last accessed: 06.02.2020).

64. Schmidl M., Anna von Dietze. Germany - National GDPR Implementation Overview. URL: https://www.dataguidance.com/notes/germany-national-gdpr-implementation-overview (last accessed: 25.02.2020).

65. Urteil vom 27.03.2019 - BVerwG 6 C 2.18. URL: https://www.bverwg.de/de/270319U6C2.18.0 (letzter Zugriff: 25.02.2020).

66. Dr. Axel Freiherr von dem Bussche. German Implementation of the GDPR. URL: https://deutschland.taylorwessing.com/en/documents/get/1739/german-implementation-of-the-gdpr.pdf_show_on_screen (last accessed: 06.02.2020).

67. Germany publishes GDPR implementation report: an official website of the International Association of Privacy Professionals. URL: https://iapp.org/news/a/germany-publishes-gdpr-implementation-report/ (last accessed: 25.02.2020).

68. Report on Experience Gained in the Implementation of the GDPR: Independent German Federal and State Data Protection Supervisory Authorities. URL: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/12/Evaluation-Report-German-DPAs-Clean.pdf (last accessed: 25.02.2020).

69. Germany: Data Protection 2019. URL: https://iclg.com/practice-areas/data-protection-laws-and-regulations/germany (last accessed: 06.02.2020).

70. Data protection laws of the world: France. URL: https://www.dlapiperdataprotection.com/index.html?t=law&c=FR (last accessed: 06.02.2020).

71. Saarinen M., Auvray E., Cruchet F. Data protection in France: overview. URL: https://www.lw.com/thoughtLeadership/data-protection-in-france-overview (last accessed: 06.02.2020).

72. France: new data protection law has been adopted. URL: https://blogs.dlapiper.com/privacymatters/france-new-data-protection-law-has-been-adopted/ (last accessed: 06.02.2020).

73. France: Data Protection 2019. URL: https://iclg.com/practice-areas/data-protection-laws-and-regulations/france (last accessed: 06.02.2020).

74. Overview of the General Data Protection Regulation (GDPR). URL: https://www.citizensinformation.ie/en/government_in_ireland/data_protection/overview_of_general_data_protection_regulation.html (last accessed: 06.02.2020).

75. Data Protection Act 2018. URL: http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html (last accessed: 06.02.2020).

76. GDPR with an Irish flavour – the Irish Data Protection Act 2018. URL: https://inplp.com/latest-news/article/gdpr-with-an-irish-flavour-the-irish-data-protection-act-2018/ (last accessed: 06.02.2020).

77. Data Protection Legislation: an official website of the Data Protection Commission (DPC). URL: https://www.dataprotection.ie/en/legal/data-protection-legislation (last accessed: 06.02.2020).

78. 'We have a huge problem': European tech regulator despairs over lack of enforcement. URL: https://www.politico.com/news/2019/12/27/europe-gdpr-technology-regulation-089605 (last accessed: 06.02.2020).

79. DPC statement on Facebook dating feature: an official website of the Data Protection Commission (DPC). URL: https://www.dataprotection.ie/en/news-media/press-releases/dpc-statement-facebook-dating-feature (last accessed: 25.02.2020).

80. Shawn Marie Boyne. Data Protection in the United States. The American Journal of Comparative Law, Vol. 66. P. 299-343.

81. Data Protection Law: An Overview: Congressional Research Service. URL: https://fas.org/sgp/crs/misc/R45631.pdf (last accessed: 27.02.2020).

82. Chabinsky S., Pittman P. USA: Data Protection 2019. URL: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa (last accessed: 27.02.2020).

83. California Consumer Privacy Act (CCPA): an official website of the Attorney General - Xavier Becerra. URL: https://oag.ca.gov/privacy/ccpa (last accessed: 27.02.2020).

84. Sotto L., Simpson A. Data Protection & Privacy. URL: https://gettingthedealthrough.com/area/52/jurisdiction/23/data-protection-privacy-united-states/ (last accessed: 27.02.2020).

85. State Comprehensive-Privacy Law Comparison: an official website of the International Association of Privacy Professionals. URL: https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law.pdf (last accessed: 27.02.2020).

86. Governor Mills Signs Internet Privacy Legislation: an official website of the State of Maine. URL: https://www.maine.gov/governor/mills/news/governor-mills-signs-internet-privacy-legislation-2019-06-06 (last accessed: 27.02.2020).

87. New Nevada Privacy Law Takes Effect in October - Comparison of Nevada Law to CCPA. URL: https://www.akingump.com/en/experience/practices/cybersecurity-privacy-and-data-protection/ag-data-dive/new-nevada-privacy-law-takes-effect-in-october-comparison-of.html (last accessed: 27.02.2020).

88. The letter to congressional leaders by the Members of the Business Roundtable of 10 September 2019. URL: https://s3.amazonaws.com/brt.org/BRT-CEOLetteronPrivacy-2.pdf (last accessed: 03.03.2020).

89. Framework for consumer privacy legislation. URL: https://s3.amazonaws.com/brt.org/privacy_report_PDF_005.pdf (last accessed: 03.03.2020).

90. O'Connor C. In Search Of A Federal Data Privacy Law. URL: https://www.lexology.com/library/detail.aspx?g=0704a74a-d140-4e3d-a934-d395f3580769 (last accessed: 03.03.2020).

91. The Bill «To provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement». URL: https://www.cantwell.senate.gov/imo/media/doc/COPRA%20Bill%20Text.pdf (last accessed: 03.03.2020).

92. The Bill «To establish consumer data privacy and security protections». URL: https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/12/Nc7.pdf (last accessed: 03.03.2020).

93. COPRA and CDPA: Similarities, Gray Areas and Differences: an official website of the International Association of Privacy Professionals. URL: https://iapp.org/media/pdf/resource_center/COPRA_CDPA_Comparison_WP.pdf (last accessed: 03.03.2020).

94. Schwartz P., Solove D. The PII problem: privacy and a new concept of personally identifiable information. New York University Law Review, Vol. 86. P. 1814-1894.

95. California's Privacy Law Goes Into Effect Today. Now What? URL: https://www.wired.com/story/ccpa-guide-california-privacy-law-takes-effect/ (last accessed: 04.03.2020).

96. Consumer Online Privacy Rights Act Offers CCPA-Style Privacy Protections for All U.S. Citizens. URL: https://www.hipaajournal.com/consumer-online-privacy-rights-act/ (last accessed: 04.03.2020).

97. California. URL: https://www.forbes.com/places/ca/ (last accessed: 04.03.2020).

98. California Consumer Privacy Act: A Compliance Guide. URL: https://www.skadden.com/-/media/files/publications/2019/03/cybersecurity_california_privacy.pdf?la=en (last accessed: 05.03.2020).

99. SB-1121 California Consumer Privacy Act of 2018. URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121 (last accessed: 05.03.2020).

100. Defining “Consumer” Under The California Consumer Privacy Act. URL: https://www.lexology.com/library/detail.aspx?g=8bb9d29c-233c-4115-81b3-fff70056da5d (last accessed: 05.03.2020).

101. CCPA Guide. URL: https://www.iubenda.com/en/help/19133-ccpa-guide#rights-of-the-consumer (last accessed: 09.03.2020).

102. What is a ‘service provider’ under CCPA? URL: https://medium.com/golden-data/what-is-a-service-provider-under-ccpa-93d65c6b9a33 (last accessed: 18.03.2020).

103. CCPA and GDPR Comparison Chart: an official website of the International Association of Privacy Professionals. URL: https://iapp.org/media/pdf/resource_center/CCPA_GDPR_Chart_PracticalLaw_2019.pdf (last accessed: 20.03.2020).

104. Comparing privacy laws: GDPR v. CCPA. URL: https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf (last accessed: 20.03.2020).

105. Головченко В. Правові основи захисту персональних даних. URL: https://yur-gazeta.com/publications/practice/inshe/pravovi-osnovi-zahistu-personalnih-danih.html (дата звернення: 18.04.2020).

106. Все що потрібно знати про збір та обробку персональних даних: офіційний веб сайт Печерського районного суду міста Києва. URL: https://pc.ki.court.gov.ua/sud2606/gromadyanam/1/23776/ (дата звернення: 18.04.2020).

107. Відповідь Секретаріату Уповноваженого Верховної Ради України з прав людини на депутатське звернення народного депутата України Жупанина Андрія Вікторовича № 33.6/393/1/19/26.5 від 09.01.2020. URL: https://drive.google.com/open?id=1rMG9kOJeFp2EoT2Am0z_aqtzA0fsx-vK (дата звернення: 18.04.2020).

108. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. Дата оновлення: 20.03.2020. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 18.04.2020).

109. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. Дата оновлення: 01.12.2019. URL: https://zakon.rada.gov.ua/laws/show/2939-17#n87 (дата звернення: 18.04.2020).

110. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. Дата оновлення: 21.12.2019. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 18.04.2020).

111. 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 від 20.01.2012 р., судова справа № 2-рп/2012. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12 (дата звернення: 18.04.2020).

112. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. Київ: К.І.С., 2015. 220 с.

113. GDPR Top Ten: #3 Extraterritorial applicability of the GDPR. URL: https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-privacy-gdpr-top-ten-3-extraterritorial-applicability-of-the-gdpr.html (last accessed: 18.04.2020).

114. Територія застосування GDPR. URL: https://legalitgroup.com/teritoriya-zastosuvannya-gdpr/ (дата звернення: 18.04.2020).

115. Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation of 16 November 2018. URL: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf (last accessed: 18.04.2020).

116. Ünsal B., Yaşar M. Territorial Scope of the GDPR. URL: https://www.lexology.com/library/detail.aspx?g=e7d7d2a9-cee5-4e17-a371-2c7dd2c6822d&utm_source=lexology+daily+newsfeed&utm_medium=html+email+-+body+-+general+section&utm_campaign=lexology+subscriber+daily+feed&utm_

content=lexology+daily+newsfeed+2019-04-08&utm_term= (last accessed: 18.04.2020).

117. Judgment of the Court of Justice of the European Union in case Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság of 01 October 2015. URL: http://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=EN (last accessed: 18.04.2020).

118. The extra-territorial scope of the EU's GDPR. URL: https://www.freshfields.com/en-gb/our-thinking/campaigns/digital/data/general-data-protection-regulation/ (last accessed: 18.04.2020).

119. Judgment of the Court of Justice of the European Union in case Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González of 13 May 2014. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131 (last accessed: 18.04.2020).

120. Кодекс України про адміністративні правопорушення (статті 1 - 212-21): Закон України від 07.12.1984 р. № 8073-X. Дата оновлення: 28.04.2020. URL: https://zakon.rada.gov.ua/laws/show/80731-10 (дата звернення: 02.05.2020).

121. Податковий кодекс України: Закон України від 02.12.2010 р. № 2755-VI. Дата оновлення: 02.04.2020. URL: https://zakon.rada.gov.ua/laws/show/2755-17 (дата звернення: 18.04.2020).

122. Кодекс України про адміністративні правопорушення (статті 213 - 330): Закон України від 07.12.1984 р. № 8073-X. Дата оновлення: 28.04.2020. URL: https://zakon.rada.gov.ua/laws/show/80732-10#n34 (дата звернення: 02.05.2020).

123. Єдиний державний реєстр судових рішень. URL: http://reyestr.court.gov.ua/ (дата звернення: 18.04.2020).

124. Постанова Коломийського міськрайонного суду від 13.01.2020 р., судова справа № 346/5963/19. URL: http://reyestr.court.gov.ua/Review/88214446 (дата звернення: 18.04.2020).

125. Про державну реєстрацію юридичних осіб, фізичних осіб - підприємців та громадських формувань: Закон України від 15.05.2003 р. № 755-IV. Дата оновлення: 28.04.2020. URL: https://zakon.rada.gov.ua/laws/show/755-15 (дата звернення: 02.05.2020).

126. Постанова Жовтневого районного суду м. Маріуполя Донецької області від 17.01.2020 р., судова справа № 263/16968/19. URL: http://reyestr.court.gov.ua/Review/86969362 (дата звернення: 18.04.2020).

127. Кравець М.О. Адміністративна відповідальність юридичних осіб. Актуальні проблеми вітчизняної юриспруденції. 2017. № 4. С. 75-78.

128. Постанова Київського апеляційного суду від 17.12.2019 р., судова справа № 756/12839/19. URL: http://reyestr.court.gov.ua/Review/86645786 (дата звернення: 18.04.2020).

129. Про захист економічної конкуренції: Закон України від 11.01.2001 р. № 2210-III. Дата оновлення: 13.02.2020. URL: https://zakon.rada.gov.ua/laws/show/2210-14#n454 (дата звернення: 18.04.2020).

130. Про проект: Офіційний веб сайт Twinning Ombudsman. URL: http://www.twinning-ombudsman.org/uk/about-us/about-project/ (дата звернення: 18.04.2020).