

Київський національний торговельно-економічний університет
Кафедра міжнародного приватного, комерційного та цивільного права

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА
на тему:
ЦИВІЛЬНО-ПРАВОВИЙ ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

студентки 2 курсу 9м групи
спеціальності 081 «Право»
спеціалізації
«Цивільне право і процес»

підпис студента

Степанюк Ірини
Анатоліївни

Науковий керівник
кандидат юридичних наук,
доцент

підпис керівника

Ільченко Ганна
Олександрівна

Гарант освітньої програми
доктор юридичних наук

підпис керівника

Примак Володимир
Дмитрович

Київ 2019

ЗМІСТ

ВСТУП.....	3
РОЗДІЛ 1. Правове регулювання сфери персональних даних в Україні	6
1.1. Поняття та види персональних даних за законодавством України	6
1.2. Суб'єкти правовідносин у сфері персональних даних	16
РОЗДІЛ 2. Особливості цивільно-правового захисту персональних даних	29
2.1. Захист персональних даних в порядку цивільного судочинства	29
2.2. Альтернативні способи вирішення спорів у сфері захисту персональних даних	44
2.3. Міжнародно-правовий захист персональних даних	49
ВИСНОВКИ ТА ПРОПОЗИЦІЇ	57
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	61

ВСТУП

Актуальність теми. Право особи на приватність та невтручання в особисте життя є основоположними правами кожної людини. З розвитком інформаційних технологій, процесом глобалізації та поширенням автоматизованих систем обробки та зберігання інформації набуває особливої актуальності виокремлення категорії персональних даних з більш загальної категорії «приватне життя» та зумовлює необхідність створення механізму захисту інформації, в тому числі і персональних даних. Розвиток цієї проблеми викликає природну необхідність в розробці надійної та дієвої системи захисту персональних даних.

Дане дослідження присвячене аналізу цивільно-правових аспектів, що забезпечують захист персональних даних. Україна тільки приступає до розробки та впровадження у національне законодавство системного підходу до забезпечення захисту персональних даних. Тому впровадження нових та вдосконалення існуючих нормативно-правових актів забезпечить формування комплексної правової системи захисту персональних даних.

З огляду на те, що у національній правовій системі практично відсутній досвід захисту персональних даних, а також у зв'язку з сучасним рівнем розвитку технологій, виникла необхідність в науковому аналізі та осмисленні можливостей юридичної науки щодо забезпечення цивільно-правового захисту персональних даних.

Дослідженням теоретичних та практичних проблем захисту персональних даних займалися такі науковці, як: І. О. Бут, І. Л. Білан, О. С. Брель, Л. В. Борисова, О. А. Дмитренко, С. С. Єсімов, Н. В. Камінська, О. О. Кулініч, М. М. Кравчук, Т. І. Обуховська, М. В. Різак, І. М. Сопілко, В. І. Теремецький та ін.

Мета дослідження. Метою роботи є встановлення особливостей правового регулювання відносин щодо захисту персональних даних.

Для досягнення поставленої мети потрібно виконати такі **завдання**:

- розкрити поняття та види персональних даних за законодавством України;
- визначити суб'єктів правовідносин у сфері персональних даних;
- виявити особливості захисту персональних даних в порядку цивільного судочинства;
- охарактеризувати альтернативні способи вирішення спорів у сфері захисту персональних даних;
- встановити особливості міжнародно-правового захисту персональних даних.

Об'єктом дослідження є суспільні відносини у сфері захисту персональних даних.

Предмет дослідження – цивільно-правовий захист персональних даних.

Методи дослідження. Методологічну основу випускної кваліфікаційної роботи складають як загальнонаукові, так і спеціальні методи пізнання. Для дослідження поняття «персональні дані» та їх видів було застосовано діалектичний метод. Формально-догматичний метод застосовувався при тлумаченні правових категорій, в результаті чого поглиблено та уточнено понятійно-категоріальний апарат персональних даних. Використання порівняльно-правового методу дало змогу виявити спільну для більшості зарубіжних країн тенденцію до закріплення в правових нормах, положень щодо права фізичної особи на захист персональних даних. На основі поєднання формально-логічного методу та методу моделювання сформульовано конкретні пропозиції щодо вдосконалення норм національного законодавства щодо захисту персональних даних.

Наукова цінність одержаних результатів полягає у подальшій розробці доктринальних положень цивільно- правового захисту персональних даних.

Зокрема, елементи наукової новизни містяться у пропозиції щодо: удосконалення визначення поняття «персональні дані», «володілець персональних даних», класифікації персональних даних на загальні та особливі персональні дані.

Практичне значення полягає у можливості використання сформульованих у випускній кваліфікаційній роботі висновків та пропозицій для підготовки науково-дослідної діяльності, у законотворчій діяльності, у правозастосовній діяльності, при підготовці лекційних занять та спецкурсів у вищих навчальних закладах з дисциплін «Цивільне право», «Інформаційне право» тощо.

Окремі положення випускної кваліфікаційної роботи викладено у статті Степанюк І. А. Поняття та види персональних даних за законодавством України. Правове забезпечення підприємницької діяльності : зб. наук. ст. студ. / відп. ред. О. О. Бакалінська, В. Д. Примак, Ю. В. Тищенко». Київ: Київ. нац. торг.-екон. ун-т, 2019. Ч. 2. С. 23-27.

Структура випускної кваліфікаційної роботи. Робота складається зі вступу, двох розділів, що поділені на п'ять підрозділів, висновків та пропозицій, списку використаних джерел. Загальний обсяг роботи становить 69 сторінок. Список використаних джерел складається з 77 найменувань.

РОЗДІЛ 1

ПРАВОВЕ РЕГУЛЮВАННЯ СФЕРИ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ

1.1. Поняття та види персональних даних за законодавством України

Головними цінностями України як демократичної країни є людина, її права, свободи та законні інтереси. Держава гарантує невтручання у приватне життя людини, що являє собою недоторканість житла, таємниця листування, нерозголошення відомостей про особу. Право на невтручання у приватне життя людини вимагає не лише забезпечення його недоторканості, а й забезпечує його таємницю.

Загальна декларація прав людини, проголошена Генеральною Асамблеєю Організації Об'єднаних Націй 10 грудня 1948 року [1], вперше закріпила право на невтручання в особисте та сімейне життя, яке є одним із основоположних прав кожної людини. У Європейській Конвенції про захист прав людини і основоположних свобод, прийнятій 1950 року [2], закріплено, що кожна людина має право на свободу дотримуватися своєї думки, отримувати й поширювати інформацію та ідеї без втручання з боку державних органів і незалежно від державних кордонів. Україна приєдналась до Конвенції у 1997 році, визнавши положення Конвенції частиною національного законодавства.

У справі «Ван Остервійк проти Бельгії», Європейський суд з прав людини прийшов до висновку, що приватне життя є правом на невтручання в особисте життя, правом жити так, як хочеться, без оголошення деталей особистого життя, але право на повагу особистого життя цим не вичерпується. Воно вимагає також, до певної міри, право на встановлення і підтримання стосунків з іншими людьми, особливо в емоційній сфері, для розвитку і реалізації особистості людини [29].

У період переходу від індустріального до інформаційного суспільства у багатьох країнах було прийнято чимало нормативно-правових актів, які стосуються захисту даних та інформації. І. Білан зазначає, що у 1970 році у Німеччині був прийнятий перший у світі закон про захист персональних даних. Цим законом було введено державну посаду Комісара по захисту персональних даних, який набув право незалежності від владних структур, а також право спостереження за діяльністю щодо персональних даних [44].

Пізніше, у 1978 році у Франції був прийнятий Закон про інформатику, картотеки та свободи, який регулює механізм обробки та захисту персональних даних лише фізичних осіб, контроль за дотриманням якого покладено на Національну комісію з інформатики та свобод [54]. У 1984 році у Великобританії був прийнятий «Акт про захист персональних даних», яким було введено інститут Уповноваженого з питань захисту персональних даних та Суд із захисту даних [53].

Першим міжнародним документом, який регулює сферу захисту персональних даних, стала Конвенція Ради Європи № 108 «Про захист прав осіб у зв'язку з автоматизованою обробкою персональних даних» (далі – Конвенція № 108), яка стала відкрита для підписання 28 січня 1981 року [5]. Вона визначає основоположні принципи обробки персональних даних та регулює застосування процесу обробки та механізм захисту персональних даних. Стороною Конвенції № 108 може стати не тільки держава-член Ради Європи, а й будь-яка країна, яка бажає забезпечити належний рівень захисту персональних даних на законодавчому рівні.

Вперше в українському законодавстві інститут захисту персональних даних було регламентовано в Конституції України, де в ст. 32 Основного Закону закріплено, що ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [8].

На сучасному етапі у процесі адаптації законодавства України до європейських стандартів національне законодавство поступово приводиться у відповідність до положень міжнародних конвенцій та положень, які регулюють сферу персональних даних. Станом на сьогодні серед міжнародних стандартів, які регулюють відносини щодо захисту персональних даних, основне місце посідає Конвенція № 108. Згідно зі ст. 2 даної Конвенції, персональні дані – це будь-яка інформація, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною [5].

У 2010 році Україна ратифікувала Конвенцію № 108 і Додатковий протокол до неї та водночас взяла на себе зобов'язання забезпечити дотримання основоположних прав і свобод людини, зокрема права на невтручання у особисте та сімейне життя. Для втілення поставленої мети та з метою конкретизації прав та свобод людини, закріплених у ратифікованих Україною міжнародних договорах та Конституції України, Верховною Радою України 01 червня 2010 року було прийнято Закон України № 2297-VI «Про захист персональних даних», який набув чинності 1 січня 2011 року та який став ключовим нормативно-правовим актом, що регулює сферу захисту персональних даних в Україні. Цей нормативно-правовий акт регулює відносини, які виникають у процесі обробки та захисту персональних даних. Законом покладено повноваження з контролю за дотриманням законодавства про захист персональних даних на Уповноваженого Верховної Ради України з прав людини.

Відповідно до ст. 2 Закону України «Про захист персональних даних», персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [18]. Ідентифікованою вважається особа, котру можна виокремити серед інших. Зазвичай для того, щоб ідентифікувати фізичну особу, необхідно володіти інформацією про її ім'я, прізвище та по батькові, а також реквізити документа, що посвідчують особу (паспорт громадянина України, реєстраційний номер облікової картки платника податків тощо).

Провідну роль у системі права Європейського Союзу у сфері захисту персональних даних відігравала Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року, метою якої є забезпечення однакового рівня захисту прав і свобод особи при обробці персональних даних в усіх державах-членах ЄС [6].

З 25 травня 2018 року Директива 95/46/ЄС «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» втратила чинність та вступили в силу нові правила захисту персональних даних для всіх держав-членів Європейського Союзу та країн Європейської економічної зони під назвою Загальний регламент захисту даних або General Data Protection Regulation (GDPR), прийнятий 27 квітня 2016 року [3]. Предметом регулювання Регламенту є правовідносини, пов'язані з вільним переміщенням персональних даних та захистом фізичних осіб у зв'язку з обробкою персональних даних. Норми Регламенту є нормами прямої дії, тому не передбачають імплементації у національне законодавство. Хоча Україна не є державою-членом Європейського Союзу, Загальний регламент захисту даних стосується також і українських компаній, які обробляють персональні дані осіб, які проживають у Європейському Союзі. Тому Регламент застосовується до всіх без винятку компаній, які зберігають та обробляють персональні дані громадян та резидентів Європейського Союзу, незалежно від місцезнаходження компанії.

Згідно з п. (1) ст. 4 Загального регламенту про захист даних від 27 квітня 2016 року, термін «персональні дані» означає будь-яку інформацію, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних») [3]. Тобто можна стверджувати, що норми національного законодавства, які поступово приводяться у відповідність до права Європейського Союзу, відповідають міжнародним стандартам.

На думку Н. В. Камінської, можна відзначити паралельне, іноді тотожне, використання термінів «персональні дані», «персоніфікована інформація», «інформація про особу», «інформація про фізичну особу» тощо [55, с. 107].

Інформація про фізичну особу – це інформація, за допомогою якої можливо ідентифікувати особу, виявити особливі, персоніфіковані, характерні елементи кожної особи.

О. А. Дмитренко зазначає, що поняття «персональні дані» – будь-яка інформація, що стосується ідентифікованої фізичної особи або фізичної особи, яку можна ідентифікувати, є тотожним поняттю «інформація про особу» [50, с.5].

Т. І. Обуховська вважає, що до персональних даних належать не тільки біографічні дані, такі як: прізвище, ім'я, по батькові, дата і місце народження особи, національність, релігійні, політичні чи філософські переконання, освіта, місце навчання і роботи, відомості про сімейний стан, наявність дітей, ставлення до військової служби. До персональної інформації також належать відомості про матеріально-фінансовий стан (банківські рахунки, платежі по них, нерухоме та рухоме майно, майнові права), стан здоров'я, особисті стосунки приватного характеру та багато інших відомостей у матеріальній формі в різних сферах суспільного життя, що створюються, збираються, зберігаються, поширюються та використовуються в інших спосіб як з відома особи – суб'єкта даних, так і без її відома [68, с. 19].

Відповідно до ст. 11 Закону України «Про інформацію» № 2657-ІІІ від 02.10.1992 року, інформація про фізичну особу (персональні дані) – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [20]. У цьому Законі, поняття «персональні дані» та «інформація про фізичну особу» також ототожнюються.

Л. В. Борисова, порівнюючи вищезазначені поняття, зазначає, що основними даними про особу (персональними даними) є: національність, освіта, сімейний стан, релігійність, стан здоров'я (факт звернення за медичною допомогою, діагноз, результат медичного обстеження), адреса, дата і місце народження, майнове становище, тощо [45, с. 99]. На нашу думку, інформація про особу та персональні дані є рівнозначними поняттями, обидва поняття є

сукупністю відомостей про фізичну особу, що дає змогу виокремити її серед інших учасників суспільних відносин.

О. С. Брель стверджує, що визначення персональних даних у Законі України «Про захист персональних даних», незважаючи на відповідність міжнародній практиці, не є вичерпним і не дає чітких критеріїв того, які саме дані про фізичну особу можна вважати персональними [46, с. 222].

У роз'ясненні Міністерства юстиції України від 21.12.2011 року «Деякі питання практичного застосування Закону України «Про захист персональних даних» зазначено, що законодавством України не встановлено і не може бути встановлено чіткого переліку відомостей про фізичну особу, які є персональними даними, в тому числі при обробці персональних даних в інформаційних (автоматизованих) базах та картотеках персональних даних, що можуть виникнути у майбутньому, у зв'язку зі зміною в технологічній, соціальній, економічній та інших сферах суспільного життя [27].

Відповідно до ч. 3.1 Рішення Конституційного Суду України від 20.01.2012 року №2-рп/2012, за Цивільним кодексом України зміст права на недоторканність особистого і сімейного життя як одного з видів особистого немайнового права полягає в тому, що фізична особа вільно, на власний розсуд визначає свою поведінку у сфері свого приватного життя і можливість ознайомлення з ним інших осіб та має право на збереження у таємниці обставин свого особистого життя (статті 270, 271, 301). Фізична особа не може відмовитися від особистих немайнових прав, а також не може бути позбавлена цих прав (частина третя статті 269 Цивільного кодексу України) [32].

Конституційний Суд України виходить з того, що неможливо визначити абсолютно всі види поведінки фізичної особи у сферах особистого та сімейного життя, оскільки особисті та сімейні права є частиною природних прав людини, які не є вичерпними, і реалізуються в різноманітних і динамічних відносинах майнового та немайнового характеру, стосунках, явищах, подіях тощо. Право на приватне та сімейне життя є засадничою цінністю, необхідною для повного розквіту людини в демократичному суспільстві, та розглядається як право

фізичної особи на автономне буття незалежно від держави, органів місцевого самоврядування, юридичних і фізичних осіб.

У рішенні Європейського суду з прав людини у справі «S. та Марпер проти Сполученого Королівства» зазначено, що «приватне життя» – широке поняття, якому неможливо дати вичерпне визначення. Воно включає фізичну та психологічну недоторканність особи, тому може охоплювати різні аспекти фізичної та соціальної самоідентифікації особи. Наприклад, такі елементи як прираховування себе до певної статі, ім'я, а також сексуальна орієнтація і статеве життя потрапляють у приватну сферу, яка охороняється ст. 8 Конвенції. Крім імені людини, її приватне та сімейне життя може включати й інші засоби самоідентифікації особистості та підтримки зв'язків із сім'єю. Важливим елементом приватного життя може бути інформація про стан здоров'я людини. Крім того, Суд вважає, що національна приналежність людини також повинна вважатися частиною її приватного життя. Крім того, ст. 8 Конвенції захищає право людини на особистісний розвиток, а також її право налагоджувати й розвивати стосунки з іншими людьми та зовнішнім світом. До того ж поняття приватного життя охоплює елементи, які стосуються права людини на своє зображення [30].

Вважаємо, що все ж таки необхідно визначити у законодавчих нормах орієнтовний мінімальний перелік відомостей, що становлять персональні дані та який не буде вичерпним та буде залежати від мети обробки персональних даних.

Окрім того, варто зазначити, що в національному законодавстві відсутня класифікація персональних даних. Лише п. 1 ст. 7 Закону України «Про захист персональних даних» визначено особливі категорії персональних даних. До них належать: дані про расове або етнічне походження; політичні, релігійні переконання; засудження до кримінального покарання; дані, що стосуються здоров'я, статевого життя, біометричні або генетичні дані [18]. Дане положення Закону дублює положення Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ст. 7) та Загального

регламенту про захист даних (ст. 9). Опрацювання цих категорій персональних даних здійснюється в спеціальному порядку, визначеному у відповідному нормативно-правовому акті.

У цивілістичній науці немає єдиного підходу до класифікації персональних даних. М. В. Різак пропонує класифікувати персональні дані на такі види: 1) загальні персональні дані – прізвище, ім'я та по батькові, дата народження, а також інші персональні дані, які за згодою суб'єкта цих даних розміщені в загальнодоступних базах персональних даних та які на момент їх обігу та/або обробки не були вилучені або знищені з цих баз; 2) спеціальні персональні дані – відомості про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та політичних спілках, звинувачення у скоєнні злочину або засудження до кримінального покарання, а також дані, що стосуються здоров'я чи статевого життя; 3) вразливі персональні дані – персональні дані, які не входять до вразливих чи загальних персональних даних, межі обігу яких визначаються суб'єктом цих даних [70, с. 94].

Т. І. Обуховська розподіляє персональні дані наступним чином. Перша група персональних даних створюється та збирається органами державної влади і місцевого самоврядування відповідно до вимог закону. До таких даних належать: оперативно-розшукові дані, відомості про сплату податків та інших обов'язкових платежів, дані про доходи фізичних осіб, про проходження митного контролю, ідентифікаційні дані документів на ім'я особи (серія, номер, дата видачі документа і найменування органу, який здійснив цю видачу) та ін.

Друга група персональних даних створюється та збирається суб'єктами права власності і господарювання відповідно до вимог закону. До таких даних належать: витяги з наказів про працівників, характеристики на працівників, ідентифікаційні дані документів на ім'я особи та інше.

Третя група персональних даних самотійно надається фізичними особами органам державної влади і місцевого самоврядування та суб'єктам права власності і господарювання у визначені законом терміни та ситуації. До

таких персональних даних належать: податкова декларація, податковий звіт, митна декларація, анкета, суб'єктивні симптоми захворювання пацієнтів.

Четверта група персональних даних створюється суб'єктами права власності і господарювання згідно з угодами між ними та фізичними особами, що описуються цими даними [68, с. 101].

О. А. Дмитренко, поділяє персональні дані залежно від того, якими органами чуття сприймаються персональні дані, на звукові і зорові (включаючи символічні (зокрема текст) та образні (зокрема фото)); ті, що сприймаються безпосередньо органами чуття (містяться в документах, портретах), і ті, для обробки яких потрібна спеціальна апаратура (зчитувач скану сітківки ока, комп'ютер тощо) [50, с. 28].

С. С. Єсімов вважає доцільним розділити персональні дані на персональні дані ідентифікації та персональні дані, які характеризують особу. Персональні дані ідентифікації належать до даних, неправомірне володіння якими однозначно може завдати шкоди власнику цих ідентифікацій, використання яких потребує підвищеного захисту під час зберігання і обробки. Персональні дані, які характеризують особу, але не є даними ідентифікації, доцільно розділити на загальнодоступні, важливі та використання яких може завдати шкоди суб'єкту. Доцільно визначити режим персональних даних, використання яких може завдати шкоди суб'єкту, на самого суб'єкта при укладенні договорів про використання персональних даних між суб'єктом і оператором [51, с. 148].

На думку А. І. Мужик та Мужик І. М., можна виділити три групи персональних даних:

- дані, що дозволяють однозначно ідентифікувати громадянина;
- дані, що розкривають загальну інформацію, але не дозволяють однозначно ідентифікувати громадянина;
- дані, що розкривають особливо чутливу інформацію, але не дозволяють однозначно ідентифікувати громадянина [66, с. 105].

Як зазначає О. О. Кулініч, персональні дані охороняються в режимі конфіденційної інформації, що виключає їх випадкове або несанкціоноване

псування або випадкову їх втрату, а також несанкціонований доступ до них, їх зміну, блокування, передачу. Правовий режим інформації персонального характеру забезпечує права людини на самовизначення стосовно підстав, умов і обсягу операцій з обробки персональних даних, на контроль за здійсненням таких операцій, а також право на доступ, внесення змін, знищення і заперечення обробці персональних даних у випадках і в порядку, які повинні бути додатково визначені чинним законодавством. Режим конфіденційності персональних даних знімається у випадках знеособлювання персональних даних і за бажанням суб'єкта для його персональних даних (у тому числі може бути встановлений режим загальнодоступної інформації – бібліографічні довідники, телефонні книги, адресні книги, приватні оголошення тощо). У цих випадках у загальнодоступні бази даних можуть включатися такі персональні дані: прізвище, ім'я, по батькові, рік і місце народження, адреси місця проживання і роботи, номер контактного телефону, відомості про професії, інші відомості, надані суб'єктом і (або) отримані з відкритих джерел. В останньому разі власник повинний проінформувати суб'єкта про зміст його персональних даних, про джерела їх одержання і мету використання [60, с. 42].

Таким чином, проаналізувавши нормативно-правові акти та наукові праці українських вчених щодо класифікації персональних даних, вважаємо за доцільне поділити персональні дані за порядком надання доступу до них на загальні та особливі персональні дані та доповнити ст. 2 Закону України «Про захист персональних даних» наступними термінами :

«загальні персональні дані – прізвище, ім'я, по батькові, дата народження, номер телефону, електронна адреса, місце проживання/перебування, місце роботи, реєстраційний номер облікової картки платника податків та інші дані, за якими можна ідентифікувати фізичну особу, що розміщені в загальнодоступних базах даних»;

«особливі персональні дані – дані про расову або етнічну приналежність, політичні, релігійні або світоглядні переконання, відомості, що стосуються

здоров'я чи статевого життя, генетичні дані, біометричні дані, дані про судимість і кримінальні злочини».

Процес обробки особливих персональних даних повинен мати більший порівняно з загальними персональними даними режим захисту.

1.2. Суб'єкти правовідносин у сфері персональних даних

Учасниками правовідносин у сфері персональних даних, носіями суб'єктивних прав та юридичних обов'язків є суб'єкти відносин, пов'язаних з персональними даними, та інші особи. Варто звернути увагу на те, що питання правового статусу суб'єктів відносин, що пов'язані з персональними даними, та вивчення їх особливостей у працях вітчизняних науковців практично не розглядалося. Законодавством України хоч і визначено правовий статус кожного суб'єкта правовідносин у сфері персональних даних, проте воно містить певні недоліки та потребує доопрацювання та подальшого законодавчого врегулювання з урахуванням зарубіжного досвіду та міжнародних стандартів.

Відповідно до ст. 4 Закону України «Про захист персональних даних» суб'єктами відносин, пов'язаних із персональними даними є:

- суб'єкт персональних даних;
- володілець персональних даних;
- розпорядник персональних даних;
- третя особа;
- Уповноважений Верховної Ради України з прав людини [18].

К. С. Мельник пропонує до складу суб'єктів відносин, пов'язаних із персональними даними, долучити також органи виконавчої влади, що формують та реалізують державну політику у сфері захисту персональних даних [65, с. 36]. Адже, Кабінет Міністрів України спрямовує та координує роботу міністерств та інших органів центральної виконавчої влади, які у свою чергу забезпечують формування та реалізації державної політики у відповідних

сферах суспільного життя, виконання Конституції України та інших нормативно-правових актів, а також дотримання прав та свобод людини і громадянина.

Необхідно також враховувати, що міжнародне співробітництво та транскордонна передача персональних даних, відповідно до статті 29 Закону «Про захист персональних даних», здійснюються у тісному співробітництві з іноземними суб'єктами відносин, пов'язаних з персональними даними. Тому з метою органічного та системного викладення правових норм у Законі вбачається за доцільне долучити до суб'єктного складу, визначеному у статті 4 Закону «Про захист персональних даних», іноземних суб'єктів відносин, пов'язаних з персональними даними [65, с. 36].

Відповідно до ст. 2 вищезазначеного Закону, суб'єкт персональних даних – фізична особа, персональні дані якої обробляються [18]. Оскільки законодавством не встановлено певних виняткових ознак фізичної особи-суб'єкта персональних даних, то варто виходити з загальних положень цивільного законодавства. Згідно з ст. 24 Цивільного кодексу України, людина як учасник цивільних відносин вважається фізичною особою [11]. Фізична особа наділена цивільною правоздатністю, яка виникає з моменту народження, та дієздатністю, яка виникає з настанням певного віку.

Як слушно відмічає В. І. Теремецький, суб'єкт персональних даних є основним учасником правовідносин у сфері захисту персональних даних. Однак у вітчизняному законодавстві не визначеними залишилися деякі питання його правового становища, зокрема щодо віку та громадянства. Отже, суб'єктами персональних даних можуть бути громадяни України, іноземці та особи без громадянства, незалежно від віку, національності та релігійних уподобань. До вказаних суб'єктів персональних даних доцільно віднести також батьків та опікунів фізичних осіб, які за своїм віком або станом здоров'я не мають можливості самотійно реалізувати права у сфері захисту персональних даних [74, с. 173].

Кожен суб'єкт персональних даних володіє комплексом прав, які визначені у ст. 8 Закону України «Про захист персональних даних» та які є невід'ємними і непорушними. Так, відповідно до ч. 2 ст. 8 цього Закону, суб'єкт персональних даних має право:

1) знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом;

2) отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані;

3) на доступ до своїх персональних даних;

4) отримувати не пізніш як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи обробляються його персональні дані, а також отримувати зміст таких персональних даних;

5) пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних;

6) пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними;

7) 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;

8) звертатися із скаргами на обробку своїх персональних даних до Уповноваженого або до суду;

- 9) застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних;
- 10) вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди;
- 11) відкликати згоду на обробку персональних даних;
- 12) знати механізм автоматичної обробки персональних даних;
- 13) на захист від автоматизованого рішення, яке має для нього правові наслідки [18].

Зважаючи на наведені вище положення, суб'єкт персональних даних має право застосовувати такі засоби правового захисту своїх персональних даних: звернення із скаргою до володільця, Уповноваженого Верховної Ради України з прав людини або до суду.

У ч. 2 ст. 12 Закону України «Про захист персональних даних» зазначено, що суб'єкт персональних даних повідомляється про володільця персональних даних, склад та зміст зібраних персональних даних, свої права, визначені цим Законом, мету збору персональних даних та осіб, яким передаються його персональні дані:

- в момент збору персональних даних, якщо персональні дані збираються у суб'єкта персональних даних;
- в інших випадках протягом тридцяти робочих днів з дня збору персональних даних [18].

Із статті Закону випливає, що володілець повідомляє суб'єкта у кожному випадку обробки персональних даних. Проте, доцільно було б врахувати те, що повідомляти суб'єкта про обробку персональних даних немає необхідності, якщо суб'єкту вже відома ця інформація.

Відповідно до ст. 2 Закону України «Про захист персональних даних», володілець персональних даних – фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом [18]. Володільцем персональних даних можуть бути підприємства, установи, організації не залежно від форми

власності, фізичні особи-підприємці, органи державної влади, чи органи місцевого самоврядування, які здійснюють обробку персональних даних на законних підставах.

У міжнародних актах, зокрема у Конвенції Ради Європи № 108, володільця персональних даних називають контролером файлів, що означає фізичну або юридичну особу, державний орган, установу чи будь-який інший орган, що уповноважений відповідно до національного законодавства вирішувати, яким повинно бути призначення файлу даних для автоматизованої обробки, які категорії персональних даних повинні зберігатися та які операції повинні здійснюватися з ними [5].

П. 7 ст. 4 Загального регламенту захисту даних визначає контролера як фізичну чи юридичну особу, орган публічної влади, агентство чи інший орган, який самостійно чи спільно з іншими визначає цілі та засоби опрацювання персональних даних; якщо цілі та засоби такого опрацювання визначаються законодавством Союзу чи держави-члена, контролер або спеціальні критерії його призначення може бути передбачено законодавством Союзу чи держави-члена [3].

Проаналізувавши міжнародні нормативно-правові акти, варто зазначити, що визначення володільця є дещо неточним, адже у приватних цивільно-правових відносинах володільць самостійно приймає рішення про обробку персональних даних та встановлює мету обробки, а у відносинах, де персональні дані обробляються на підставі закону, у багатьох нормативно-правових актах не визначено хто саме є володільцем. У випадку обробки персональних даних органом державної влади чи органом місцевого самоврядування, що діють виключно в межах чинного законодавства, обсяг та мета обробки вже визначені нормативно-правовими актами, що регламентують діяльність даних органів. Тому, у даному випадку, визначення, що наведене у Конвенції № 108 є більш вдалим, де контролеру (володільцеві) надається право самостійно чи разом з іншими приймати рішення щодо обробки персональних даних.

Володілець обробляє персональні дані відповідно до Закону України «Про захист персональних даних» та Типового порядку обробки персональних даних від 08 січня 2014 року № 1/02-14, затвердженим Наказом Уповноваженого Верховної Ради України з прав людини. Згідно з п. 2.1 Типового порядку обробки персональних даних, володілець визначає:

- 1) мету та підстави обробки персональних даних;
- 2) категорії суб'єктів персональних даних;
- 3) склад персональних даних;
- 4) порядок обробки персональних даних, а саме:
 - спосіб збору, накопичення персональних даних;
 - строк та умови зберігання персональних даних;
 - умови та процедуру зміни, видалення або знищення персональних даних;
 - умови та процедуру передачі персональних даних та перелік третіх осіб, яким можуть передаватися персональні дані;
 - порядок доступу до персональних даних осіб, які здійснюють обробку, а також суб'єктів персональних даних;
 - заходи забезпечення захисту персональних даних;
 - процедуру збереження інформації про операції, пов'язані з обробкою персональних даних та доступом до них [26].

Володілець самостійно визначає порядок обробки персональних даних та здійснює обробку лише за згодою суб'єкта персональних даних, крім випадків, передбачених законодавством України. На всіх етапах обробки персональних даних володілець повинен вживати заходи щодо забезпечення захисту персональних даних.

Відповідно до ст. 2 Закону України «Про захист персональних даних», розпорядник персональних даних - фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця [18]. Розпорядником, так само, як і володільцем, можуть бути підприємства, установи, організації незалежно від форми власності, фізичні особи-підприємці, органи державної влади чи органи місцевого

самоврядування. У п. 3 ст. 4 Закон України «Про захист персональних даних» зазначено, що розпорядником персональних даних, володільцем яких є орган державної влади чи орган місцевого самоврядування, крім цих органів, може бути лише підприємство державної або комунальної форми власності, що належить до сфери управління цього органу [18]. Розпорядник обробляє персональні дані на підставі договору, укладеного в письмовій формі з володільцем та лише з метою і в обсязі, визначених договором. Також, розпорядник самостійно визначає засоби обробки персональних даних.

Відповідно до ст. 2 Закону України «Про захист персональних даних» третьою особою вважається будь-яка особа, за винятком суб'єкта персональних даних, володільця чи розпорядника персональних даних та Уповноваженого Верховної Ради України з прав людини, якій володільцем чи розпорядником персональних даних здійснюється передача персональних даних [18].

Подібне визначення закріплене у ч. 10 ст. 4 Загального регламенту про захист даних, де третя особа називається третьою стороною та означає фізичну чи юридичну особу, орган публічної влади, агентство чи орган, який не є суб'єктом даних, контролером, оператором та особами, які, під безпосереднім керівництвом контролера або оператора, уповноважені опрацьовувати персональні дані.

Після прийняття Закону України «Про захист персональних даних» продовжився розвиток законодавства, яке регулює сферу захисту персональних даних та конфіденційної інформації фізичних осіб. 03 липня 2013 року було прийнято Закон України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» № 383-VII, яким на Уповноваженого Верховної Ради України з прав людини було покладено функції щодо здійснення контролю за додержанням законодавства про захист персональних даних [15].

Уповноважений Верховної Ради України з прав людини (далі – Уповноважений) здійснює парламентський контроль за додержанням конституційних прав і свобод людини і громадянина та захист прав кожного на

території України і в межах її юрисдикції на постійній основі, у тому числі здійснює контроль за дотриманням законодавства про захист персональних даних.

З метою забезпечення виконання Уповноваженим повноважень, передбачених Законом України «Про захист персональних даних», було створено Департамент з питань захисту персональних даних у Секретаріаті Уповноваженого Верховної Ради України.

Уповноважений також зобов'язаний включати до своєї щорічної доповіді про стан дотримання та захисту прав і свобод людини і громадянина в Україні звіт про стан дотримання законодавства у сфері захисту персональних даних.

Наказом Уповноваженого «Про затвердження документів у сфері захисту персональних даних» № 1/02-14 від 08.01.2014 року [25] було затверджено наступні документи:

- Типовий порядок обробки персональних даних;
- Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за дотриманням законодавства про захист персональних даних;
- Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації.

Відповідно до ст. 23 Закону України «Про захист персональних даних» до повноважень Уповноваженого належать:

- 1) отримувати пропозиції, скарги та інші звернення фізичних і юридичних осіб з питань захисту персональних даних та приймати рішення за результатами їх розгляду;
- 2) проводити на підставі звернень або за власною ініціативою виїзні та безвиїзні, планові, позапланові перевірки володільців або розпорядників персональних даних в порядку, визначеному Уповноваженим, із забезпеченням

відповідно до закону доступу до приміщень, де здійснюється обробка персональних даних;

3) отримувати на свою вимогу та мати доступ до будь-якої інформації (документів) володільців або розпорядників персональних даних, які необхідні для здійснення контролю за забезпеченням захисту персональних даних, у тому числі доступ до персональних даних, відповідних баз даних чи картотек, інформації з обмеженим доступом;

4) затверджувати нормативно-правові акти у сфері захисту персональних даних у випадках, передбачених цим Законом;

5) за підсумками перевірки, розгляду звернення видавати обов'язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних, у тому числі щодо зміни, видалення або знищення персональних даних, забезпечення доступу до них, надання чи заборони їх надання третій особі, зупинення або припинення обробки персональних даних;

6) надавати рекомендації щодо практичного застосування законодавства про захист персональних даних, роз'яснювати права і обов'язки відповідних осіб за зверненням суб'єктів персональних даних, володільців або розпорядників персональних даних, структурних підрозділів або відповідальних осіб з організації роботи із захисту персональних даних, інших осіб;

7) взаємодіяти із структурними підрозділами або відповідальними особами, які відповідно до цього Закону організовують роботу, пов'язану із захистом персональних даних при їх обробці; оприлюднювати інформацію про такі структурні підрозділи та відповідальних осіб;

8) звертатися з пропозиціями до Верховної Ради України, Президента України, Кабінету Міністрів України, інших державних органів, органів місцевого самоврядування, їх посадових осіб щодо прийняття або внесення змін до нормативно-правових актів з питань захисту персональних даних;

- 9) надавати за зверненням професійних, самоврядних та інших громадських об'єднань чи юридичних осіб висновки щодо проектів кодексів поведінки у сфері захисту персональних даних та змін до них;
- 10) складати протоколи про притягнення до адміністративної відповідальності та направляти їх до суду у випадках, передбачених законом;
- 11) інформувати про законодавство з питань захисту персональних даних, проблеми його практичного застосування, права і обов'язки суб'єктів відносин, пов'язаних із персональними даними;
- 12) здійснювати моніторинг нових практик, тенденцій та технологій захисту персональних даних;
- 13) організовувати та забезпечувати взаємодію з іноземними суб'єктами відносин, пов'язаних із персональними даними, у тому числі у зв'язку з виконанням Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до неї, інших міжнародних договорів України у сфері захисту персональних даних;
- 14) брати участь у роботі міжнародних організацій з питань захисту персональних даних [18].

Згідно зі п. 1.1. Порядку здійснення Уповноваженим Верховної Ради України з прав людини контролю за дотриманням законодавства про захист персональних даних, цей Порядок встановлює процедуру здійснення Уповноваженим Верховної Ради України з прав людини контролю за дотриманням вимог законодавства про захист персональних даних шляхом проведення перевірок фізичних осіб, фізичних осіб - підприємців, підприємств, установ і організацій усіх форм власності, органів державної влади та місцевого самоврядування, що є володільцями та/або розпорядниками персональних даних (далі - суб'єкт перевірки), а також оформлення і розгляд результатів перевірок [24].

Уповноважений чи уповноважені ним посадові особи, здійснюючи контроль за дотриманням законодавства про захист персональних даних, мають право здійснювати перевірки (планові, позапланові, виїзні та безвиїзні), які

проводяться відповідно до затвердженого Уповноваженим чи уповноваженими посадовими особами річного чи квартального плану.

С. Кикіш вказує, що окрім розгляду письмових звернень, Омбудсмен наділений прогресивним повноваженням на участь у судовому розгляді справи (зокрема, у ролі позивача, апелянта чи касатора). Також Уповноважений з прав людини може бути присутній на засіданнях судів усіх інстанцій. У таких випадках він повинен надати суду докази того, що особа не може самостійно звернутися до суду з позовом, відповідною апеляційною чи касаційною скаргою через вік, недієздатність або фізичний стан. При цьому чинне процесуальне законодавство дозволяє Уповноваженому з прав людини представляти інтереси осіб лише в межах адміністративного та цивільного судочинства [57, с. 27].

Погоджуємось із висновками К. С. Мельника, який проаналізував зміни до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних та зазначає, що покладена в основу Закону ідея включення інституту Уповноваженого Верховної Ради України з прав людини до механізму здійснення завдань та функцій центральних органів виконавчої влади, що забезпечують формування й реалізацію державної політики у сфері персональних даних, та наділення його невластивими повноваженнями у цій сфері є концептуально уразливою й такою, що не у повну міру узгоджується з відповідними положеннями Конституції та Закону України «Про Уповноваженого Верховної Ради України з прав людини».

У зазначених змінах пропонується переважну більшість повноважень із питань здійснення державного контролю за додержанням законодавства про захист персональних даних, які за своєю природою є повноваженнями саме органів виконавчої влади, покласти на Уповноваженого Верховної Ради України з прав людини. Запропоновані зміни не повною мірою узгоджуються з природою конституційно-правового статусу Уповноваженого Верховної Ради України з прав людини, який відповідно до статті 101 Конституції України здійснює парламентський контроль за додержанням конституційних прав і

свобод людини і громадянина. Найбільш оптимальним шляхом вирішення питання забезпечення «незалежності» уповноваженого органу з питань захисту персональних даних є утворення окремого органу зі статусом та повноваженнями, подібними до тих, що має Антимонопольний комітет України, Рахункова палата України тощо. Утім, реалізація окресленого «сценарію» потребуватиме внесення відповідних змін до Конституції України [64, с.101-102].

Проведений аналіз наукової доктрини та законодавства у сфері персональних даних у контексті розуміння понять «персональні дані», класифікації персональних даних, суб'єктів правовідносин у сфері персональних даних дозволив нам дійти до наступних висновків.

Національним законодавством забезпечено право особи на невтручання в особисте і сімейне життя та право на приватність як одні із основоположних прав людини. Україна як європейська держава, яка дотримується принципів поваги до прав людини, свободи, демократії та верховенства права, приділяла багато уваги охороні приватного життя та захисту інформації. Захист персональних даних в Україні регулюється Конституцією України, Законом України «Про захист персональних даних», Законом України «Про інформацію», Законом України «Про доступ до публічної інформації» міжнародними договорами та конвенціями, а також іншими нормативно-правовими актами.

Персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Персональні дані можна поділити на загальні та особливі. До загальних персональних даних належать: прізвище, ім'я, по батькові, дата народження, номер телефону, електронна адреса, місце проживання/перебування, місце роботи, реєстраційний номер облікової картки платника податків та інші дані, за якими можна ідентифікувати фізичну особу, що розміщені в загальнодоступних базах даних. До особливої категорії персональних даних відносяться: дані про расову або етнічну приналежність, політичні, релігійні

або світоглядні переконання, відомості, що стосуються здоров'я чи статевого життя, генетичні дані, біометричні дані, дані про судимість і кримінальні злочини.

Учасниками правовідносин у сфері персональних даних, носіями суб'єктивних прав та юридичних обов'язків є суб'єкти персональних даних та інші особи. Проведений аналіз свідчить про те, що комплексні наукові розробки, присвячені визначенню правового статусу суб'єктів правовідносин у сфері персональних даних та вивченню їх особливостей практично відсутні, тому вивчення даного питання потребує подальшої наукової розробки.

До суб'єктів відносин, пов'язаних із персональними даними відносяться: суб'єкт персональних даних, володілець персональних даних, розпорядник персональних даних, третя особа та Уповноважений Верховної Ради України з прав людини. Доцільно було б до визначеного у Законі України «Про захист персональних даних в Україні» переліку суб'єктів відносин, пов'язаних з персональними даними, додати таких суб'єктів як: органи виконавчої влади, що формують та реалізують державну політику у сфері захисту персональних даних та іноземні суб'єкти відносин, пов'язані з персональними даними.

Визначення правового статусу суб'єктів відносин, що пов'язані з персональними даними, зокрема таких як суб'єкт персональних даних та володілець персональних даних, має суттєві недоліки та потребує удосконалення. Також варто зазначити, що в Україні відсутній спеціальний регулюючий уповноважений орган, який відіграв би роль регулятора захисту персональних даних на національному рівні та здійснював контроль за дотриманням законодавства сфері захисту персональних даних.

РОЗДІЛ 2

ОСОБЛИВОСТІ ЦИВІЛЬНО-ПРАВОВОГО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

2.1. Захист персональних даних в порядку цивільного судочинства

В умовах побудови сучасної демократичної європейської держави важливу роль відграє механізм захисту прав, свобод та законних інтересів фізичних осіб, адже людина вважається найвищою соціальною цінністю в Україні, а держава є головним гарантом здійснення та захисту її прав, свобод та законних інтересів.

Механізм реалізації та захисту прав і свобод людини набув світового значення та є найважливішою проблемою багатьох держав. Саме забезпечення прав і свобод особи та їх практичної реалізації є критерієм для визначення рівня демократичного розвитку будь-якої держави. Захист персональних даних фізичних осіб займає особливе місце в системі прав людини та повинен нерозривно розглядатися із захистом основоположних прав та свобод.

В теорії цивільного права вже сформований усталений підхід класифікації форм захисту прав та законних інтересів людини на юрисдикційну та неюрисдикційну. Юрисдикційна форма – це комплекс дій, що здійснюються компетентними органами (органами державної влади, органами місцевого самоврядування, судом, нотаріусом тощо), які уповноважені вжити заходи для відновлення порушених прав та інтересів фізичних осіб та суб'єктів господарювання у визначеному законом порядку. За загальним правилом захист прав та інтересів здійснюється судом.

Погоджуємось з думкою В. М. Куруц, що судовий захист займає чільне місце серед юрисдикційних форм захисту прав людини та має універсальний характер, адже дозволяє захистити будь-яке порушене право або законний інтерес. Звідси слідує, що саме суд є тим органом, котрий здійснює захист прав, свобод та законних інтересів у сфері приватноправових та публічно-правових відносин [61, с. 26].

Із аналізу положень ст. 24 Закону України «Про захист персональних даних» випливає, що захист персональних даних фізичної особи забезпечують органи державної влади, органи місцевого самоврядування, володільці, розпорядники відповідних даних, а також фізичні особи-підприємці, адвокати, нотаріуси та лікарі, які мають відповідну ліцензію.

Кожна фізична особа має право на захист від неправомірного використання інформації про себе відповідно до Закону України «Про доступ до публічної інформації» [16]. Так, кожна особа має право: на те, щоб знати які відомості про неї збираються та з якою метою; доступу до інформації, яка збирається; виправлення неточної, неповної чи застарілої інформації про особу; відшкодування шкоди у разі розкриття інформації про особу, з порушенням законодавства тощо.

Обробка даних про фізичну особу, які є конфіденційною інформацією, не допускається без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Законом України «Про захист персональних даних», а саме ч. 1 ст. 11, визначено вичерпний перелік підстав обробки персональних даних, в тому числі їх збирання, накопичення та поширення. Особливі вимоги визначені ч. 2 ст. 7 цього Закону, де передбачено вичерпний перелік підстав для обробки особливої категорії персональних даних. Із аналізу вищезазначених положень можна дійти до висновку, що обробка персональних даних здійснюється як із наявністю згоди суб'єкта персональних даних, так і без згоди такого суб'єкта (укладення правочину, стороною якого є суб'єкт персональних даних, важливі життєві інтереси суб'єкта персональних даних, необхідна в цілях охорони здоров'я, надання медичних послуг, встановлення діагнозу тощо). Наприклад, адвокату у зв'язку з наданням правової допомоги для обґрунтування, задоволення або захисту правової вимоги може бути надано доступ до персональних даних особи про її расове або етнічне походження, політичні, релігійні переконання, членства в політичних партіях та професійних спілках,

засудження до кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних.

Водночас ч. 2 ст. 25 Закону України «Про захист персональних даних» визначено умови обробки персональних даних та обмеження щодо застосування даного Закону. Так, дозволяється обробка персональних даних без застосування положень Закону України «Про захист персональних даних», якщо така обробка здійснюється виключно для особистих чи побутових потреб або для журналістських та творчих цілей.

Законом України «Про захист персональних даних», не конкретизуються відповідальність за порушення законодавства про захист персональних даних, лише зазначено про відповідальність, встановлену законом. Норми, які передбачають відповідальність за порушення законодавства у сфері захисту персональних даних, містяться у Кримінальному кодексі України та Кодексі України про адміністративні правопорушення.

Відповідно до ч. 1 ст. 182 Кримінального кодексу України, незаконне збирання, зберігання, використання або поширення конфіденційної інформації про особу без її згоди або поширення цієї інформації у публічному виступі, творі, що публічно демонструється, чи в засобах масової інформації, - караються штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або арештом на строк до шести місяців, або обмеженням волі на строк до трьох років [10].

Статтею 188-39 Кодексу України про адміністративні правопорушення передбачено накладення штрафу за: 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; повторне протягом року вчинення порушення з числа передбачених частинами першою або другою цієї статті, за яке особу вже було піддано адміністративному стягненню; 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 [9].

Законом України «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних» 02 червня 2011 року № 3454-VI [13], який набув чинності 1 липня 2012 року, було доповнено лише статті Кримінального кодексу України та Кодексу України про адміністративні правопорушення.

Реалізація особистих немайнових прав фізичної особи має бути забезпечена належним захистом в порядку цивільного судочинства. У ЦК України, на відміну від Кримінального кодексу України та Кодексу України про адміністративні правопорушення, не передбачено окремої статті, яка б визначала відповідальність за незаконну обробку, зберігання, накопичення чи поширення персональних даних фізичної особи.

Ч. 1 ст. 15 ЦК України визначено, що кожна особа має право на захист свого цивільного права у разі його порушення, невизнання або оспорювання [11]. Відповідно до ч. 1 ст. 55 Конституції України, права та свободи людини і громадянина захищаються судом.

Рішенням Конституційного Суду України від 25.12.1997 року № 9-зп встановлено, що частина перша статті 55 Конституції України містить загальну норму, яка означає право кожного звернутися до суду, якщо його права чи свободи порушені або порушуються, створено або створюються перешкоди для їх реалізації або мають місце інші ущемлення прав та свобод. Зазначена норма зобов'язує суди приймати заяви до розгляду навіть у випадку відсутності в законі спеціального положення про судовий захист. Відмова суду у прийнятті позовних та інших заяв чи скарг, які відповідають встановленим законом вимогам, є порушенням права на судовий захист, яке відповідно до статті 64

Конституції України не може бути обмежене [31]. Тому будь-яка особа у зв'язку з незаконною обробкою, зберіганням, накопиченням чи поширенням її персональних даних має право звернутися до суду для захисту порушених прав та законних інтересів.

Відповідно до ч. 2 ст. 16 ЦК України способами захисту цивільних прав та інтересів можуть бути: визнання права; визнання правочину недійсним; припинення дії, яка порушує право; відновлення становища, яке існувало до порушення; примусове виконання обов'язку в натурі; зміна правовідношення; припинення правовідношення; відшкодування збитків та інші способи відшкодування майнової шкоди; відшкодування моральної (немайнової) шкоди [11].

Для захисту персональних даних можна застосувати такі способи захисту порушених прав, як: припинення дії, яка порушує право; відшкодування збитків та інші способи відшкодування майнової шкоди; відшкодування моральної (немайнової) шкоди. Проте варто зазначити, що проаналізувавши судову практику цивільно-правового захисту персональних даних, можна зазначити, що судових рішень щодо предметного розгляду справ щодо персональних даних критично мало (не враховуючи справи, що закінчилися ухваленням рішення про відмову в позові).

Проте для демонстрації окремих випадків цивільного-правового захисту персональних даних в суді, наведемо такі справи з судової практики:

1. Перший випадок стосується визнання дій з розголошення персональних даних неправомірними.

Рішенням Апеляційного суду Харківської області від 12 квітня 2018 року встановлено, що Харківська первинна профспілкова організація Всеукраїнської профспілки «Федерація профспілок авіапрацівників радіолокації, радіонавігації і зв'язку України» (далі – ХППО ВП «ФПАРРІЗУ») звернулась до Фрунзенського районного суду м. Харкова з позовом до Державного підприємства обслуговування повітряного руху України про визнання протиправними дії керівника підприємства (далі – Украерорух).

Позивач в особі Голови профкому ХППО ВП «ФПАРРІЗУ» звертався до директора Харківського РСП Украерорух з листами, в яких просив надати інформацію, а саме: копії наказів щодо виплати матеріальної допомоги працівникам за весь 2016 рік. Листом № 6.4-1-1409 від 12.10.2016 р. голові профкому ХППО ВП «ФПАРРІЗУ» було повідомлено, що відповідна інформація надається після надання працівниками згоди на поширення персональних даних. При цьому відповідачем, з посиланням на ст. ст. 14, 16 Закону України «Про захист персональних даних», було надано відповідну інформацію щодо 15 осіб, які надали згоду на доступ до персональних даних, їх поширення та передачу третім особам. Щодо решти працівників, тридцять чотири з яких згоду не надала, а один - перебував у відпустці, то в наданні відповідної інформації було відмовлено.

Позивач просив визнати незаконним та протиправним ненадання директором Харківського регіонального структурного підрозділу Державного підприємства обслуговування повітряного руху України на запити Голови профкому ХППО ВП «ФПАРРІЗУ» копій наказів про виплати.

Суд першої інстанції у задоволенні позову відмовив, мотивуючи це тим, що інформація, яку запитує позивач містить персональні дані працівників Харківського РСП Харківського РСП Украероруху, а тому без їх згоди її поширено бути не можна, а також позивач не є суб'єктом, який уповноважений здійснювати контроль за дотриманням колективного договору та відповідно отримувати вказану інформацію за запитом.

Колегія суддів апеляційної інстанції, не погоджуючись із висновками суду першої інстанції, встановила, Харківський РСП Украерорух в розумінні Закону «Про захист персональних даних» є розпорядником інформації щодо використання бюджетних коштів, в тому числі щодо використання коштів на виплати, передбачені п. 6.28. Колективного договору.

Суд постановив апеляційну скаргу ХППО ВП «ФПАРРІЗУ» задовольнити. Визнати незаконним та протиправним ненадання директором Харківського РСП Украерорух на запити Голови профкому ХППО ВП

«ФПАРРІЗУ» копії наказів про виплати згідно п. 6.28 Колективного договору між адміністрацією Державного підприємства обслуговування повітряного руху України та профспілки. Зобов'язати Украерорух надати копії всіх наказів Харківського РСП Украерорух за 2016 рік, на запити про виплати, згідно п. 6.28 Колективного договору, профкому ХППО ВП «ФПАРРІЗУ» у повному обсязі [36].

В даному випадку був порушений Закон України «Про захист персональних даних» в частині порядку доступу до персональних даних третіх осіб, який визначається умовами згоди суб'єкта персональних даних, наданої володільцю бази персональних даних на обробку цих даних, або відповідно до вимог закону (ч. 1 ст. 16 Закону України «Про захист персональних даних»).

Однак, судова практика з даної категорії справ неодноманітна, тому що існує велика кількість судових рішень щодо відмови в позові (наприклад, Рішення Червонозаводського районного суду міста Харкова від 27 квітня 2015 р. [39]).

2. Другий випадок з судової практики стосується зобов'язання вчинити певні дії. Так, Рішенням Вінницького міського суду Вінницької області від 03 червня 2014 року встановлено: позивач звернувся до суду з позовом до Вінницького національного технічного університету про видачу документа про освіту.

Позов мотивований тим, що позивач, в 2013 р. згідно з наказом Вінницького національного технічного університету присвоєно кваліфікацію бакалавр з інженерної механіки з подальшою видачею диплома бакалавра без відзнак, як такому, що навчався за освітньо-професійною програмою підготовки бакалавра за напрямком підготовки «Інженерна механіка», виконав всі вимоги навчального плану та захистив дипломну роботу.

Однак, відповідач, порушуючи рішення Державної екзаменаційної комісії не видав позивачу диплом бакалавра, через те, що він не надав письмової згоди на обробку своїх персональних даних. Копії наказів про зарахування та

відрахування позивача та копія рішення Державної екзаменаційної комісії не були надані відповідачем на численні звернення позивача.

Згідно із заявою від 20.05.2013 року позивач відмовився надавати згоду на збір та обробку даних у Єдиній електронній державній базі з питань освіти, у зв'язку з чим відповідач листом від 05.06.2013 року №11/42 повідомив йому про те, що він втрачає право на отримання документу про освіту встановленого зразка, тобто відповідач не матиме можливості замовити та видати позивачу диплом про освіту. На думку позивача, вказана відповідь свідчить про невизнання з боку відповідача права позивача на отримання ним диплома про освіту встановленого зразка без надання згоди на обробку персональних даних.

На думку суду, таке невизнання права є незаконним, тому суд вирішив позов задовольнити. Зобов'язати Вінницький національний технічний університет видати позивачеві диплом про освіту встановленого зразка без обов'язкового оформлення згоди на збір та обробку персональних даних [37].

При винесенні рішення Суд керувався статтею 11 Закону України «Про захист персональних даних» в якій передбачено, що особа, яка обробляє персональні дані може здійснювати таку обробку не лише на підставі згоди особи, але і на підставі закону - для здійснення наданих їй повноважень та виконання правочину, стороною якого є суб'єкт персональних даних.

3. Третій випадок стосується визнання дій незаконними та зобов'язання вчинити певні дії.

Рішенням Голосіївського районного суду м. Києва від 30 травня 2016 року встановлено, що позивачка звернулась до суду з позовом до ПАТ «Укрсоцбанк» про визнання бездіяльності протиправною та зобов'язання ПАТ «Укрсоцбанк» та зобов'язання вчинити певні дії.

Позовні вимоги обґрунтовані тим, що 27.10.2006 р. між АКБ «Укрсоцбанк» та позивачкою був укладений кредитний договір № 2006\686-Ф03.7\36, відповідно до якого Банк зобов'язався надати кредит в сумі 50810 доларів США з оплатою 12,45% річних. У Позичальника відсутній документ, який би підтверджував перехід права власності на зазначені грошові кошти від

Банку до позивача. Банк відмовив у наданні інформації, яку просила надати позивачка, посилаючись на ст. 60 Закону України «Про банки і банківську діяльність».

Позивач вважає бездіяльність відповідача щодо ненадання інформації незаконною, оскільки вона, яка сторона кредитного договору і власник інформації, що стосується його виконання, в силу положень Закону України «Про банки і банківську діяльність», має право на отримання інформації, що становить банківську таємницю на підставі письмового запиту, а також відповідно до Закону України «Про захист персональних даних», як суб'єкт персональних даних, має право отримати інформацію стосовно третіх осіб, яким ці дані були передані. Крім того, посилаючись на положення Закону України «Про доступ до публічної інформації» позивач зазначає, що підстав, визначених законом, для відмови у задоволенні її запиту від 28.12.2015 р. у відповідача не було.

Суд вирішив позов задовольнити, визнати бездіяльність Публічного акціонерного товариства «Укрсоцбанк» протиправною та зобов'язати відповідача надати інформацію на запит позивача [38].

Суд керувався тим, що з точки зору ст. 14 даного Закону поширення персональних даних передбачає дії щодо передачі відомостей про фізичну особу з баз персональних даних за згодою суб'єкта персональних даних. Поширення персональних даних без згоди суб'єкта персональних даних або уповноваженої ним особи дозволяється у випадках, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. На безперешкодний і безоплатний доступ до персональних даних мають органи державної влади та органи місцевого самоврядування відповідно до їх повноважень.

Проте розглянуті нами рішення досить нетипові для справ з захисту персональних даних. Здебільшого, застосовується такий спосіб захисту як відшкодування моральної шкоди. Показовим є наступне судове рішення.

Рішенням Запорізького районного суду у Запорізькій області від 29 березня 2019 року встановлено, що позивач звернувся до суду із позовом про визнання неправомірним використання персональних даних на сторінці облікового запису (акаунту) «Владислав Куценко» у соціальній мережі Facebook та стягнення моральної шкоди, посилаючись на те, що у травні 2018 року до нього звернулися знайомі і колеги, які повідомили про те, що у соціальній мережі Facebook розміщуються публікації від імені позивача, зокрема провокативного характеру, шляхом створення та використання облікового запису (акаунту), найменування якого було «Владислав Куценко», та у якому були розміщені персональні дані позивача: його прізвище та ім'я, дата його народження, фотографії з зображенням позивача, дані біографії (зокрема, дані про теперішнє та колишні місця роботи, освіти, місце проживання).

Позивач стверджував, що не створював даний обліковий запис (акаунт) у соціальній мережі Facebook, ніколи не мав доступу до нього та не здійснював його адміністрування та модерацію. Дозволу нікому на створення зазначеного облікового запису (акаунту), його адміністрування та модерацію позивач також не надавав. Будь-які інші облікові записи (акаунти) у соціальній мережі Facebook він також не створював. Таким чином, позивач вважав, що створення і функціонування даного облікового запису (акаунту), на якому розміщені його персональні дані, порушують його немайнові права.

Суд вирішив позов про визнання неправомірним використання персональних даних на сторінці облікового запису (акаунту) «Владислав Куценко» у соціальній мережі Facebook і стягнення моральної шкоди задовольнити. Визнати неправомірним використання відповідачем в обліковому записі (акаунті) «Владислав Куценко» у соціальній мережі Facebook персональних даних позивача: прізвища, ім'я, фотографій, даних про місця роботи, освіти, місце проживання. Стягнути з відповідача на користь позивача моральну шкоду в розмірі 2000 грн. 00 коп. (дві тисячі гривень 00 коп.) [39].

Тому розглянемо детальніше такий спосіб захисту як відшкодування моральної шкоди, адже при порушенні захисту персональних даних він є найбільш затребуваним та виконує компенсаторну функцію (оскільки матеріальні збитки зазвичай в таких категоріях справ відсутні).

Н. І. Логінова, Р. Р. Дробожур зазначають, що згідно з Цивільним кодексом України (статтями 22, 23, 277, 1166, 1167) фізична особа може звернутися до суду за захистом своїх прав, порушених у зв'язку з розголошенням персональних даних, має право на спростування недостовірної інформації та на відшкодування майнової та моральної шкоди [62, с. 95].

Ч. 2 ст. 200 ЦК України визначено, що суб'єкт відносин у сфері інформації може вимагати усунення порушень його права та відшкодування майнової і моральної шкоди, завданої такими правопорушеннями [11]. Фізична особа, особисті немайнові права якої порушено, може вибрати один або декілька способів захисту порушеного права, визначених ч. 2 ст. 16 Цивільного кодексу України, або обрати будь-який із спеціальних способів захисту особистого немайнового права, таких як: спростування недостовірної інформації (ст. 277 ЦК України), заборона поширення інформації, якою порушуються особисті немайнові права (ст. 278 ЦК України).

Згідно з ч. 1 ст. 277 ЦК України, фізична особа, особисті немайнові права якої порушено внаслідок поширення про неї та (або) членів її сім'ї недостовірної інформації, має право на відповідь, а також на спростування цієї інформації [11].

Пленум Верховного Суду України висловив правову позицію, що з огляду на положення статті 32 Конституції України, судам належить розрізняти справи про захист гідності, честі чи ділової репутації шляхом спростування недостовірної інформації (права на відповідь) від справ про захист інших особистих немайнових прав, зокрема, перелічених у статті 270 ЦК, порушених у зв'язку з поширенням про особу інформації, недоторканість якої спеціально охороняється Конституцією та законами України і поширення якої може завдати моральну шкоду навіть у випадку, якщо ця інформація відповідає

дійсності і не порочить гідність, честь чи ділову репутацію. Тобто, якщо інформація, яка порушує особисті немайнові права особи, є достовірною, вимоги про її спростування не можуть бути задоволені. Встановивши при вирішенні таких спорів факт поширення інформації про приватне життя позивача, що відповідає дійсності та не порочить його гідність, честь чи ділову репутацію, а також факт відсутності згоди позивача на поширення цієї інформації, суд повинен захистити його право на таємницю приватного життя та може зобов'язати відповідача відшкодувати моральну шкоду [34].

Тому можна стверджувати, що у разі порушення права фізичної особи на приватне життя та у разі відсутності згоди особи на розголошення її персональних даних найчастіше застосовується такий спосіб захисту як відшкодування моральної шкоди.

До 2014 року України діяла презумпція добропорядності (ч. 3 ст. 277 ЦК України), що означає, що будь-яка негативна інформація, яка поширена про особу, вважається неправдивою, якщо тільки той, хто її поширив, не доведе протилежного. Законом України «Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Закону України «Про інформацію» та Закону України «Про доступ до публічної інформації»» від 27.03.2014 року № 1170-VII [13] було виключено ч. 3 ст. 277 із Цивільного кодексу України. Тому обов'язок доведення того, що інформація, яка була поширена про особу, є неправдивою, покладається на позивача.

Показовим у даному випадку є наступна постанова Судової палати у цивільних справах Верховного Суду України від 27.09.2017 року.

Позивач звернувся до суду з позовом до Товариства з обмеженою відповідальністю з іноземними інвестиціями ТОВ «Віннер Імпортс Україна, Лтд» про захист прав споживача та відшкодування моральної шкоди.

У грудні 2014 року йому зателефонували з ТОВ «Віннер Імпортс Україна Лтд», у якому позивач був споживачем послуг, та запропонували надати коментарі щодо роботи сервісного центру. При цьому йому було повідомлено

про те, що розмова буде записана з метою покращення обслуговування клієнтів у подальшому.

Проте через деякий час після розмови з компанією відповідача у мережі Інтернет з'явилося відео з назвою «Уроки хамства от быдла по фамилии позивача», на якому в якості аудіофону використана його розмова з представником ТОВ «Віннер Імпортс Україна Лтд» та в якості картинки відображено належний позивачу автомобіль, хоча згоди на поширення зазначеної інформації позивач не давав.

Посилаючись на порушення відповідачем норм Законів України «Про захист прав споживачів» та «Про захист персональних даних», а також на спричинення йому протиправними діями ТОВ «Віннер Імпортс Україна Лтд» моральної шкоди, просив суд стягнути з останнього на його користь 12 млн. 627 тис. 400 грн.

Суди першої, апеляційної, касаційної інстанцій відмовили у задоволенні позову, мотивуючи своє рішення тим, що у деліктних зобов'язаннях саме на відповідача покладено обов'язок спростування презумпції вини шляхом доведення відсутності його вини у завданні шкоди позивачу (якщо зазначена презумпція в суді не спростована це є підставою для висновку про наявність вини відповідача – заподіювача шкоди). Між тим, будь-яких доказів на підтвердження поновлення права позивача щодо таємниці телефонної розмови, зокрема, вжиття заходів з видалення її запису з вільного доступу в мережі Інтернет, позивач не надав. У даному випадку суди мали б виходити з презумпції спричинення позивачу моральної шкоди відповідачем та обов'язку саме відповідача спростувати таку презумпцію [35].

Станом на сьогодні в межах національного законодавства існує чимало нормативно-правових актів, якими врегульовано питання відшкодування моральної шкоди. До них належать: Конституція України, ЦК України, Кодекс законів про працю України, Закон України «Про інформацію», Постанова Пленуму Верховного Суду України «Про судову практику в справах про

відшкодування моральної (немайнової) шкоди» від 31 березня 1995 року № 4 та інші.

Відповідно до ч. 2 ст. 23 ЦК України, моральна шкода полягає:

- 1) у фізичному болю та стражданнях, яких фізична особа зазнала у зв'язку з каліцтвом або іншим ушкодженням здоров'я;
- 2) у душевних стражданнях, яких фізична особа зазнала у зв'язку з протиправною поведінкою щодо неї самої, членів її сім'ї чи близьких родичів;
- 3) у душевних стражданнях, яких фізична особа зазнала у зв'язку із знищенням чи пошкодженням її майна;
- 4) у приниженні честі та гідності фізичної особи, а також ділової репутації фізичної або юридичної особи [11].

Під час вирішення питання про відшкодування моральної шкоди суд повинен врахувати, що компенсація завданої шкоди повинна здійснюватись з урахуванням наступних елементів: наявність моральної шкоди; протиправна поведінка; наявність причинного зв'язку між шкодою і протиправним діянням заподіювача; наявність вини особи, яка заподіяла шкоду.

Розмір відшкодування моральної шкоди, а також чіткі межі такого розміру не закріплені в чинному законодавстві. Не визначено і методик розрахунку моральної шкоди. Тому, право визначення розміру відшкодування моральної шкоди залишено за судом.

Суд, вирішуючи питання щодо розміру моральної шкоди, повинен встановити, чим підтверджується факт заподіяння позивачеві душевних страждань або втрат немайнового характеру, за яких обставин чи якими діями (бездіяльністю) була заподіяна шкода, ступінь вини заподіювача моральної шкоди, враховується стан здоров'я потерпілого, зміни його життєвих обставин та ділової репутації, а також інші обставини, що мають значення для вирішення спору. Моральна шкода може відшкодовуватися як у грошовій, так і в будь-якій іншій формі.

Постановою Пленуму Верховного суду України від 25 травня 2001 року [33] було закріплено певні критерії оцінки розміру відшкодування моральної

(немайнової) шкоди. Однак, коли межі відшкодування моральної шкоди визначаються у кратному співвідношенні з мінімальним розміром заробітної плати чи неоподатковуваним мінімумом доходів громадян, суд при вирішенні цього питання має виходити з такого розміру мінімальної заробітної плати чи неоподаткованого мінімуму доходів громадян, що діють на час розгляду справи. Тому вважаємо за доцільне розробити принципи мінімальної та максимальної межі визначення розміру оцінки моральної шкоди та закріпити їх на законодавчому рівні.

Відповідно до ст. 19 Цивільного процесуального кодексу України, суди розглядають у порядку цивільного судочинства справи, що виникають з цивільних, земельних, трудових, сімейних, житлових та інших правовідносин, крім справ, розгляд яких здійснюється в порядку іншого судочинства [12]. Справи щодо захисту персональних даних розглядаються місцевими загальними судами, як судами першої інстанції у порядку позовного провадження.

Відповідно до п.1 ч.1 ст. 268 ЦК України, позовна давність не поширюється на вимогу, що впливає із порушення особистих немайнових прав, крім випадків, встановлених законом [11].

Варто звернути увагу на те, що процес захисту персональних даних, порушення яких відбулось в мережі Інтернет на різноманітних сайтах чи у соціальних мережах має певні складнощі. Адже, враховуючи особливості роботи всесвітньої мережі, порушувати права на законну обробку чи збирання персональних даних може будь-яка особа, залишаючись при цьому невідомою, чим унеможливорює для особи, чиї права було порушено, подати позов відповідно до вимог цивільно-процесуального законодавства.

Дослідження загальних положень щодо захисту персональних даних в порядку цивільного судочинства дало змогу дійти до таких висновків. Під захистом персональних даних в порядку цивільного судочинства слід розуміти діяльність суду, що спрямована на відновлення та визнання порушених, невизнаних чи оспорюваних прав суб'єктів правовідносин у сфері

персональних даних у спосіб, встановлений законом. Захист персональних даних в порядку цивільного судочинства є юрисдикційною формою захисту прав та законних інтересів людини. Захист права у разі його порушення, невизнання чи оспорювання здійснюється судами загальної юрисдикції. У разі порушення особистих немайнових прав, а саме незаконне збирання, зберігання, використання та поширення персональних даних застосовуються такі загальні способи захисту прав та законних інтересів, визначених у ст. 16 ЦК України: визнання права; визнання правочину недійсним; припинення дії, яка порушує право; відновлення становища, яке існувало до порушення; примусове виконання обов'язку в натурі; зміна правовідношення; припинення правовідношення; відшкодування збитків та інші способи відшкодування майнової шкоди; відшкодування моральної (немайнової) шкоди. Найбільш доцільними способами захисту персональних даних у судовому порядку є: припинення дії, яка порушує право; відшкодування майнової та моральної (немайнової) шкоди.

Отже, способи захисту, передбачені ст. 16 ЦК України, не є вичерпними, але разом з тим не завжди можуть ефективно захистити і поновити порушені права, особливо якщо мова йде про захист персональних даних. Відсутність теоретичних розробок щодо режиму охорони персональних даних як об'єкта цивільних прав зумовлює необхідність подальших розробок в цьому напрямі.

Проблема захисту персональних даних потребує вдосконалення, адже прогалини в законодавстві або взагалі відсутність законодавчої та нормативної бази у сфері захисту інформації є перешкодою для надійного та дієвого захисту інтересів фізичних осіб.

2.2. Альтернативні способи вирішення спорів у сфері захисту персональних даних

На думку С. Ярошенко, судова форма захисту порушених, невизнаних і оспорюваних прав, свобод та інтересів традиційно вважається універсальною і найбільш ефективною. Проте наявність негативних тенденцій у судовій

системі, наприклад, судова тяганина, надмірна вартість судових витрат, ускладнений доступ до суду тощо, підривають авторитет судової влади, знижуючи ефективність цивільного судочинства і змушуючи осіб шукати більш дієві форми захисту своїх прав. Під впливом таких тенденцій починає формуватися окрема сфера юридичної практики з вирішення правових спорів, що отримує назву «альтернативне вирішення спорів» [76, с. 25].

І. О. Бут зазначає, що практика альтернативного вирішення цивільно-правових спорів (Alternative Dispute Resolution, скорочено – ADR), яка вперше була впроваджена у США у 60-х роках XX століття у якості «приватного правосуддя» (private justice) набула широкого застосування у багатьох країнах світу, серед яких Канада, Німеччина, Франція тощо [47, с. 57].

Як міжнародним, так і українським законодавством передбачено досить великий вибір альтернативних способів вирішення спорів, які забезпечують врегулювання спору без традиційного судового способу. До альтернативних способів вирішення спорів належать: переговори, медіація, комерційний арбітраж, третейський суд, міні-суд, незалежна експертиза та ін. Однак, при виборі способу захисту персональних даних має враховуватися специфіка відносин у сфері захисту таких даних.

С. В. Васильєв до основних альтернативних способів вирішення спорів в теорії цивільного права відносить такі способи:

- самозахист, що означає самостійне врегулювання спору;
- переговори (negotiation), що представляють собою врегулювання спору безпосередньо сторонами без участі інших осіб;
- посередництво (mediation), що означає врегулювання спору за допомогою незалежного, нейтрального посередника, який сприяє сторонам в досягненні угоди [48, с. 36].

Відповідно до ст. 19 ЦК України, самозахистом є застосування особою засобів протидії, які не заборонені законом та не суперечать моральним засадам суспільства [11].

О. Антонюк, досліджуючи заходи самозахисту цивільних прав та інтересів, виділяє такі ознаки самозахисту:

- надає особі можливість самостійно здійснювати захист, не звертаючись до юрисдикційного органу (що не виключає можливість товариської допомоги та сприяння органів, які не вирішують справу по суті);
- це право виникає в разі порушення чи створення реальної загрози порушення прав або інтересів;
- це право може реалізуватися за допомогою заходів, які відповідають загальним або спеціальним критеріям правомірності, що відрізняє самозахист від самоуправства, дії під час якого вчиняються з порушенням встановленого порядку;
- воно є цільовим правом і здійснюється з метою попередження, припинення порушення права або ліквідації наслідків порушення, що відрізняє самозахист від самосуду, спрямованого на покарання [43, с. 26].

Таким чином, можна вважати, що самозахист є одним із альтернативних способів захисту суб'єктивних цивільних прав та законних інтересів громадян, який здійснюється без звернення до компетентних органів та полягає у здійсненні особою дій, спрямованих на охорону її прав та законних інтересів.

Найпоширенішим способом вирішення спорів є переговори. Процес переговорів відбувається безпосередньо між сторонами або між представниками сторін для прийняття взаємовигідного рішення. На відміну від медіації, переговори відбуваються без участі третіх осіб чи посередника.

О. О. Маркова вказує, що процедура медіації є різновидом процедури примирення сторін, в основі якої лежить врегулювання спору або конфлікту шляхом досягнення сторонами взаємовигідного компромісного рішення, яке буде задовольняти обидві сторони за участю третьої нейтральної особи – медіатора, який, здійснюючи загальне керівництво процедурою, допомагає сторонам досягти максимально ефективного рішення самостійно [63, с. 208].

Досліджуючи західний досвід вирішення спорів шляхом медіації, С. Ярошенко зазначає, що на наднаціональному рівні основним інструментом є

директива Європейського парламенту та Ради ЄС від 21.05.2008 р. №2008/52/ЕС про певні аспекти медіації в цивільних та комерційних справах. Директива застосовується до транскордонних спорів у цивільних і комерційних справах. Вона охоплює спори, в яких принаймні одна зі сторін проживає або зареєстрована в державі ЄС, відмінній від місця проживання або місця реєстрації будь-якої іншої сторони на дату домовленості про використання процедури медіації або на дату судового наказу, що зобов'язує сторони до вирішення спору в порядку медіації [76].

Підписавши Угоду про асоціацію з Європейським Союзом, Україна взяла на себе зобов'язання забезпечувати верховенство права та кращий доступ до правосуддя, яке повинно включати доступ як до судових, так і до позасудових методів врегулювання спорів.

Указом Президента України від 20.05.2015 року №276 було затверджено Стратегію реформування судоустрою, судочинства та суміжних правових інститутів на 2015-2020 рр., де в ч. 10 п. 5.4 якої передбачено розширення способів альтернативного (позасудового) врегулювання спорів, зокрема, шляхом практичного впровадження інституту медіації і посередництва, розширення переліку категорій справ, які можуть вирішуватися третейськими суддями або розглядатися судами у спрощеному провадженні; запровадження ефективних процесуальних механізмів для попередження розгляду справ за відсутності спору між сторонами; вивчення доцільності введення мирових суддів [23].

У зв'язку з великою завантаженістю судів та тривалістю судового процесу, виникла необхідність забезпечити реалізацію медіації в Україні та закріпити інститут медіації на законодавчому рівні. У Верховній Раді України було зареєстровано кілька законопроектів, що регулюють питання врегулювання спорів за допомогою медіації. 3 листопада 2016 року Верховною Радою України було прийнято за основу проект Закону України «Про медіацію». Відповідно до ст. 2 проекту Закону України «Про медіацію» № 3665 від 27.03.2015 року, медіація – альтернативний (позасудовий) метод вирішення

спорів, за допомогою якого дві або більше сторони спору намагаються в рамках структурованого процесу за участі медіатора досягти згоди для вирішення їх спору [21]. Хоч і даний проект закону так і не було прийнято, однак медіацію намагаються частіше застосовувати в суспільному житті як альтернативу судовій формі вирішення спорів.

Сьогодні медіація поступово набирає поширення в Україні при врегулюванні спору між сторонами. Адже такий неюрисдикційний спосіб захисту прав та законних інтересів має переваги порівняно з судовим розглядом спорів. Економія часу, економія коштів на витрати адвоката та самостійне вирішення конфлікту шляхом напрацювання спільних рішень за допомогою медіатора сприяє більш ефективному врегулюванню спору, зокрема, у цивільних та комерційних справах.

Отже, альтернативні способи захисту персональних даних полягають у здійсненні певних дій для захисту порушених прав без звернення до юрисдикційних органів. У науці цивільного права такі дії вважаються самозахистом. Альтернативні способи практикуються в багатьох державах та поступово набирають поширення і в Україні. До основних альтернативних способів вирішення спорів належать: переговори, медіація (посередництво), третейський суд. До переваг альтернативних способів врегулювання спору можна віднести: швидкість розгляду спору, економія коштів та часу, збереження ділової репутації та позитивних відносин між сторонами, можливість самостійного вибору сторонами нейтральної особи (медіатора, третейського судді) для вирішення спору, конфіденційність інформації. Проте для забезпечення ефективного механізму захисту прав, свобод та законних інтересів необхідно закріпити способи альтернативного вирішення спорів щодо персональних даних на законодавчому рівні, удосконалити законодавство, яке б забезпечило належне правове регулювання процедур вирішення спору одним із альтернативних способів, вдосконалити процес організації та діяльності медіатора чи третейського суду.

2.3. Міжнародно-правовий захист персональних даних

На думку І. М. Сопілко, починаючи з другої половини ХХ сторіччя, правовий захист приватного життя в умовах побудови інформаційного суспільства стає одним із пріоритетних напрямів дослідження національних та зарубіжних вчених. Так, формування нової структури міжнародних відносин під впливом глобалізації та швидкоплинного розвитку високих технологій зумовлює потребу нових підходів та окреслення нових параметрів сучасної системи захисту персональних даних в умовах зростання нових загроз від міжнародної системи кібертероризму. Особливо гостро постає потреба міжнародного співробітництва у боротьбі із міжнародною кіберзлочинністю.

Так, 17 листопада 2014 року було заявлено, що спеціалісти ремонтують систему електронної пошти Держдепартаменту США після можливої шкоди завданої ймовірною хакерською атакою. Не так давно, ми спостерігали під час виборів в Україні в 2014 році цілу систему хакерських атак на сервери ЦВК України.

Інший аспект проблеми – це втручання через мережу Інтернет по усьому світу як в приватне життя людей, так і в діяльність державних органів і організацій через систему несанкціонованого доступу до приватної інформації про особу. Так, наприклад, політики в США намагаються отримати від найбільшого пошукача Google додаткові гарантії того, що компанія робить максимально можливо для захисту особистої інформації її користувачів та інших людей. Вісім членів американського конгресу звернулися до Google з листом з проханням уточнити деякі питання, пов'язані із захистом персональних даних під час використання нової технології розумних окулярів Google Glass, так як використання останніх ускладнює і не дає гарантій захисту персональних даних.

Інший приклад, ще в 2011 році через безліч скарг на порушення конфіденційності керівництво соціальної мережі Facebook ввело посаду директора із захисту персональних даних. Усі ці факти свідчать про зростання наукового інтересу до питання вдосконалення системи захисту персональних

даних та поглиблення міжнародного співробітництва в зазначеній сфері [71, с.71].

У більшості європейських країн вже прийняті базові нормативно-правові акти у сфері захисту персональних даних, які поступово приводяться у відповідність із законодавством Європейського Союзу. Незважаючи на деякі відмінності у правових системах, в основу всіх законів про захист персональних даних покладені однакові основоположні принципи, які повинні забезпечити ефективний захист таких даних.

О. О. Шарабурина зазначає, що до міжнародно-правових керівних принципів захисту персональних даних належать, зокрема, законність отримання, обробки і використання інформації; конкретна мета збору; обмеженість строку зберігання, точність; захист від випадкового чи несанкціонованого знищення чи випадкової втрати, від несанкціонованого доступу до інформації; гласність; право доступу особи до персональної інформації; право перевірки і внесення змін у свої дані та ін. [77, с. 75].

В. І. Теремецький та Д. В. Цвірюк, досліджуючи зарубіжний досвід правового захисту персональних даних, дійшли до висновку, що, без сумніву, країною з найрозвинутішою системою захисту інформаційного простору можна вважати США, оскільки її інформаційне законодавство – це найкращий приклад та орієнтир у сфері захисту персональних даних, на якому необхідно будувати вітчизняне законодавство у цій сфері [73, с. 74].

Захисту персональних даних в США приділяється особлива увага. За неналежне зберігання та обробку персональних даних передбачені суворі санкції та штрафи. Однак, механізм захисту персональної інформації переважно спрямований на приватно-правову сферу.

Основою нормативно-правового регулювання захисту персональних даних у США є Закон «Про свободу інформації» (The Freedom of Information Act) 1966 р. та Закон «Про надання кредитної інформації про покупця» (The Fair Credit Reporting Act) 1970 р. Окрему увагу привертає Закон США «Про конфіденційність» (The Privacy Act) 1974 р., головною метою якого є створення

умов для запобігання випадків протиправних дій з боку органів влади та державних інституцій у сфері використання інформації персонального характеру [73, с. 74].

М. М. Кравчук, вивчаючи міжнародний досвід правового регулювання захисту персональних даних в мережі інтернет, зазначила, що за новим законодавством США заборонена інсталяція програмного забезпечення для збору індивідуальної інформації, ідентифікації користувача, без його відома та згоди. Передбачена також відповідальність за підтасування результатів пошукової видачі з метою заманювання на комерційні сайти, подробиці сторінки і рекламу, і при цьому «чорні оптимізатори», які займаються подібною діяльністю, отримують винагороду в грошових та інших еквівалентах [58, с. 125]. У США діє Агентство національної безпеки (англ. National Security Agency (NSA)), яке займається збором, аналізом іноземної розвідувальної інформації та захистом персональних даних [41].

Варто зазначити, що досить розвинутим у сфері захисту персональних даних є європейське законодавство, яке постійно удосконалюється. Ключовим етапом стало прийняття Директиви 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» [6], прийнята 24.10.1995 року, та Директиви 97/66/ЄС Європейського Парламенту і Ради «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі» [7], прийнята 15.12.1997 року.

Парламентська Асамблея Ради Європи 26 червня 1998 року прийняла Резолюцію 1165 (1998) «Право на приватність» [4] після нещасного випадку, що стався з Принцесою Уельською Діаною, в якій закликала уряди країн-членів Ради Європи прийняти закон, який гарантував би право на приватність, в тому числі захист персональних даних фізичних осіб, або привести у відповідність вже прийнятий закон до принципів, визначених ч. 14 цієї Резолюції. Зокрема, передбачено, що суб'єкт персональних даних має право подати цивільний позов про відшкодування шкоди, заподіяної у результаті втручання у його особисте

життя, або позов проти фотографа, коли він проникає у приватне володіння або порушує приватність іншим способом.

Досліджуючи законодавство Європейського союзу у сфері захисту персональних даних, В. О. Волосецький зазначає, що захисту персональних даних в Інтернеті присвячено Рекомендації Ради Європи «Основні напрямки захисту прав фізичних осіб у зв'язку з обробкою персональних даних у інформаційних супермагістралях» від 09.12.1997 р. У відповідності до цих Рекомендацій користувачі та провайдери послуг Інтернету мають ураховувати особливість захисту персональних даних у цій мережі у зв'язку із можливістю несанкціонованого їх використання та нанесення шкоди людині, суспільству або державі [49, с. 472].

З 25 травня 2018 року набув чинності Загальний регламент про захист даних, який має декілька нововведень:

- збір та обробка персональних даних лише за згодою фізичної особи. Допускається обробка даних без згоди особи тільки у випадках, передбачених законодавством відповідної країни;
- дозвіл на обробку персональних даних може надавати особа, якій виповнилося 16 років;
- «право на переносимість даних» (right to data portability) означає, що на вимогу суб'єкта персональних даних компанія зобов'язана надавати електронну копію персональних даних іншій компанії безоплатно;
- будь-яка особа, захист персональних даних якої порушено, може звернутися зі скаргою до однієї із держав-членів Європейського Союзу;
- створити посади службовців із захисту персональних даних (обов'язково у компаніях, де кількість персоналу перевищує 250 осіб, а також у державних установах).

У Загальному регламенті захисту даних дублюється із Директиви 95/46/ЕС «право на забуття» (right to be erased), яке означає, що за запитом суб'єкта персональних даних компанія зобов'язана видалити будь-яку інформацію про персональні дані особи (в тому числі акаунти (облікові записи)

в соціальних мережах, повідомлення, інформацію з результатів пошуку тощо). Право на забуття було визнане Європейським Судом у 2014 році після справи Маріо Костехи Гонсалеса. Сама справа стосувалася звернення іспанського громадянина до корпорації Google з приводу видалення посилань оголошення у газеті (електронна версія видання містилася на сайті) щодо продажу його будинку на аукціоні за борги. Заявник обґрунтовував необхідність стирання даних тим, що інформація не є актуальною – оголошення вийшло близько 12 років перед тим, борг давно погашений і, незважаючи на це, пошукова система у відповідь на введення його, імені видавала посилання на цю інформацію, яка завдавала шкоди його репутації. У рішенні Суд встановив, що з метою забезпечення прав, передбачених у згаданих положеннях Директиви, «оператор пошукової системи зобов'язаний видаляти зі списку результатів, виданих у відповідь на пошуковий запит на основі імені особи, посилання на веб-сторінки, розміщені третіми особами, що містять інформацію про таку особу, також і у випадку, коли ім'я або інформація не видалена перед тим або у той самий час з самих веб-сторінок, і навіть тоді, коли публікація на цих сторінках розміщена на законних підставах» [72, с. 100].

Європейська рада з питань захисту даних була утворена замість «Робочої групи 29-ої статті», що діяла відповідно до норм Директиви 97/66/ЄС. Європейська рада з питань захисту даних є органом Європейського союзу, який здійснює контроль за дотриманням та застосуванням Загального регламенту захисту даних. Відповідно до ч. 3 ст. 68 Загального регламенту про захист даних, Рада складається з голови одного наглядового органу кожної держави-члена та Європейського інспектора із захисту даних або їхніх відповідних представників [3].

Як зазначає З. О. Кукіна, при розробці реформи Європейська комісія визначила три основні проблеми європейського законодавства в сфері захисту персональних даних. Першою проблемою є труднощі, які виникають у фізичних осіб щодо контролю обігу особистої інформації. З огляду на недостатній рівень гармонізації національних законів про захист персональних

даних, особам складніше користуватися своїм правом на захист в одних країнах порівняно з іншими, особливо в мережевому просторі. Особи втратили контроль над обігом персональної інформації через великий обсяг даних, які розповсюджуються в мережі без їхнього відома. Крім того, розповсюдженою є думка, що поширення персональних даних є частиною сучасного життя і 72% європейських користувачів Інтернету вважають, що від них вимагають забагато особистої інформації. Часто вони навіть не знають, яким чином використовувати свої права в Інтернеті.

Другою проблемою є прогалини та невідповідність в правовому регулюванні захисту персональних даних в сфері судового співробітництва в кримінальних справах.

Третьою проблемою є бар'єри для бізнесу та органів державної влади в результаті фрагментації, правової невизначеності і непослідовним застосування законодавства про захист персональних даних [59, с. 102].

Вважаємо, що всі ці проблеми притаманні і Україні також. Останнім часом уряди держав і міжнародні організації все більше уваги приділяють захисту персональних даних. Основним приводом для підвищення уваги став швидкий розвиток технологій та відсутність достатньо ефективної регламентації інформаційних відносин в мережі Інтернет. Реформа Європейського союзу, гармонізація законодавства держав-членів, зміни в законі «Про захист персональних даних» в нашій країні свідчать про проведення активних дій в напрямку вдосконалення відповідного нормативного регулювання захисту права особи на приватне життя, як фундаментального права людини.

У ФРН у 1977 році були прийняті Закон «Про захист даних», Закон «Про порядок опублікування інформації», у 1978 р. Закон «Про порядок ведення інформаційних реєстрів». У 1990 році був прийнятий новий закон «Про удосконалення обробки даних і захист інформації», який поклав основу у процесі обробки, збирання, накопичення та поширення інформації. З прийняттям цього закону скасовані попередні нормативно-правові акти у сфері

інформаційного законодавства. У 1997 році в ФРН було прийнято Акт захисту інформації в телекомунікаціях (Teleservices Data Protection Act).

Контроль за захистом персональних даних у ФРН здійснює Федеральний уповноважений із захисту персональних даних, якого обирає Бундестаг Німеччини, існує посада уповноваженого із захисту персональних даних на підприємствах, в організаціях. Використання персональних даних у Німеччині здійснюється лише у випадках, передбачених законом, у іншому випадку – заборонене. У громадян є можливість оскарження положень законодавства, що регулюють захист персональних даних. Значна увага приділяється безпеці держави та захисту секретної інформації, що охороняється на належному рівні.

У Франції регулювання захисту персональних даних здійснюється на загальному рівні відповідно до Закону «Про інформатику, картотеки та свободи», прийнятого у 1978 році. Особи, які винні у порушенні даного закону можуть бути притягнуті до адміністративної та кримінальної відповідальності. Також діє Інститут Уповноваженого із питань захисту персональних даних.

О. О. Кукіна вказує, що у Великій Британії питання захисту персональних даних регламентується «Актом про захист персональних даних» від 1984 року, який був прийнятий пізніше, ніж у ФРН, Франції та інших країнах. Закон «Про свободу інформації» був прийнятий у 2000 році [59, с. 101]. Цим законом було введено Інститут Уповноваженого з питань захисту персональних даних. У Британії функціонує Офіс уповноваженого з питань інформації - Information Commissioner's Office (ICO) [42], який є незалежним державним органом, створений для забезпечення підтримання права на інформацію в інтересах суспільства, сприяючи відкритості державних органів та конфіденційності даних для осіб.

В Естонії Закон «Про захист персональних даних» вперше було прийнято у 1996 році, новий закон – у 2007 році [19]. У 2000 році був прийнятий Закон «Про публічну інформацію» [22], у 2004 році Закон «Про електронні комунікації» [17]. Особливу роль відіграє Інспекція захисту даних [52], яка була створена у 1999 році. Інспекція проводить консультації, розглядає скарги,

приймає зобов'язуючі рішення розпорядження, надає доступ до делікатних особистих даних, проводить аудити на місцях, може призначити грошовий платіж за недотримання відповідного законодавства або клопотатись про порушення кримінальної справи.

Підсумовуючи дослідження міжнародно-правового регулювання захисту персональних даних, слід зазначити, що у багатьох державах світу існує розвинене нормативно-правове забезпечення захисту інформації та багаторічний досвід. Міжнародна практика свідчить про те, що захист персональних даних є невід'ємним елементом захисту права людини на приватність та права на невтручання в особисте життя.

Отже, нами узагальнено міжнародний досвід в застосуванні організаційних та правових механізмів регулювання обробки інформації та захисту персональних даних, який пропонуємо імплементувати в законодавство України, а саме при вдосконаленні Законів України «Про захист персональних даних», «Про інформацію», «Про доступ до публічної інформації», «Про звернення громадян».

Варто зазначити, що у подальшому на розроблення національного законодавства має впливати інформатизація та стрімкий розвиток технологій, адже в сучасному інформаційному просторі існує чимало загроз. Багато людей залишає свої персональні дані, не задумуючись над цим. А це призводить до того, що ці дані залишаються незахищеними, тому що використання їх в мережі Інтернет нічим не обмежене і не врегульоване. Тому, пропонуємо за доцільне внести зміни в чинне законодавство України і визначитись із статусом персональних даних, отриманих із загальнодоступних джерел та їх захистом.

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

Здійснивши дослідження цивільно-правового регулювання захисту персональних даних на підставі викладеного в випускній кваліфікаційній роботі матеріалу можна зробити наступні висновки:

1. Персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. До персональних даних фізичної особи відносяться відомості про прізвище, ім'я, по батькові, дата народження, домашня та/або робоча адреса, поштова адреса, електронна адреса, номер телефону, місце роботи, реєстраційний номер облікової картки платника податків, дані про расову або етнічну приналежність, політичні, релігійні або світоглядні переконання, відомості, що стосуються здоров'я чи статевого життя, генетичні дані, біометричні дані, дані про судимість і кримінальні злочини.

Вважаємо за доцільне поділити персональні дані за порядком надання доступу до них на загальні та особливі персональні дані. До загальних персональних даних відносяться прізвище, ім'я, по батькові, дата народження, номер телефону, електронна адреса, місце проживання/перебування, місце роботи, реєстраційний номер облікової картки платника податків та інші дані, за якими можна ідентифікувати фізичну особу, що розміщені в загальнодоступних базах даних. До особливих персональних даних належать: дані про расову або етнічну приналежність, політичні, релігійні або світоглядні переконання, відомості, що стосуються здоров'я чи статевого життя, генетичні дані, біометричні дані, дані про судимість і кримінальні злочини.

2. Учасниками правовідносин у сфері персональних даних, носіями суб'єктивних прав та юридичних обов'язків є суб'єкти відносин, пов'язаних з персональними даними, та інші особи. Проведений аналіз свідчить про те, що комплексні наукові розробки, присвячені визначенню правового статусу суб'єктів правовідносин у сфері персональних даних та вивченню їх особливостей майже відсутні.

До суб'єктів відносин, пов'язаних із персональними відносяться: суб'єкт персональних даних, володілець персональних даних, розпорядник персональних даних, третя особа, Уповноважений Верховної Ради України з прав людини, органи виконавчої влади, що формують та реалізують державну політику у сфері захисту персональних даних та іноземні суб'єкти відносин, пов'язані з персональними даними. Визначення правового статусу таких суб'єктів, зокрема суб'єкта персональних даних та володільця персональних даних, має суттєві недоліки та потребує удосконалення. Також варто зазначити, що в Україні відсутній спеціальний регулюючий уповноважений орган, який відіграв би роль регулятора захисту персональних даних на національному рівні та здійснював контроль за дотриманням законодавства сфері захисту персональних даних. Тому доцільно було б утворити орган з питань захисту персональних даних, який буде забезпечувати реалізацію державної політики у сфері захисту персональних даних та дотримання як національного, так і міжнародного законодавства у цій сфері.

3. Під захистом персональних даних в порядку цивільного судочинства слід розуміти діяльність суду, що спрямована на відновлення та визнання порушених, невизнаних чи оспорюваних прав суб'єктів правовідносин у сфері персональних даних у спосіб, встановлений законом. Захист персональних даних може здійснюватися у юрисдикційній та неюрисдикційній формі. Юрисдикційна форма – це комплекс дій, що здійснюються компетентними органами, які уповноважені вжити заходи для відновлення порушених прав та інтересів фізичних осіб та суб'єктів господарювання у визначеному законом порядку. За загальним правилом захист прав та інтересів здійснюється судом. Найбільш доцільними способами захисту персональних даних у судовому порядку є: припинення дії, яка порушує право; відшкодування майнової та моральної (немайнової) шкоди.

4. Широкого поширення серед зарубіжних країн та України набули альтернативні способи вирішення спорів щодо захисту порушених прав фізичних осіб, такі як: переговори, медіація (посередництво). Однак, в Україні

ці способи захисту персональних даних ще не стали популярними через законодавчу неврегульованість. До того ж, при виборі способу захисту персональних даних має враховуватися специфіка відносин у сфері захисту таких даних.

5. Досліджуючи міжнародно-правовий захист персональних даних, зроблено висновок, що країни, які мають розвинену економіку та високий рівень інформаційної безпеки, характеризуються підвищеним інтересом до забезпечення захисту інформації та персональних даних про особу, а також дієвим механізмом правового регулювання даної сфери. В Україні закладені лише основи законодавства у сфері захисту персональних даних. Враховуючи міжнародний досвід, нашій державі необхідно розробити механізм, який буде забезпечувати ефективний захист персональних даних та контроль за дотриманням законодавства в сучасних умовах.

Аналіз національного законодавства у сфері захисту персональних даних свідчить про те, що станом на сьогодні нормативно-правове забезпечення відносин у сфері персональних даних в частині їх захисту є недостатнім та має суттєві недоліки. Чинне національне законодавство, враховуючи прогресивний розвиток технологій, потребує вдосконалення у даній сфері, основними напрямками якого мають бути: приведення у відповідність до міжнародних стандартів, систематизація та уніфікація.

З метою удосконалення чинного законодавства України з питань регулювання цивільно-правового захисту персональних даних пропонується внести наступні зміни та доповнення до деяких законодавчих актів України, а саме:

1) додати до ч. 1 ст. 5 Закону України «Про захист персональних даних» наступний абзац: «До переліку інформації, що належить до персональних даних слід віднести наступні відомості про особу: відомості про прізвище, ім'я, по батькові, дата народження, номер телефону, електронна адреса, місце проживання/перебування, місце роботи, реєстраційний номер облікової картки платника податків, дані про расову або етнічну приналежність, політичні,

релігійні або світоглядні переконання, відомості, що стосуються здоров'я чи статевого життя, генетичні дані, біометричні дані, дані про судимість і кримінальні злочини».

2) доповнити ст. 2 Закону України «Про захист персональних даних» наступними термінами:

«загальні персональні дані – «загальні персональні дані – прізвище, ім'я, по батькові, дата народження, номер телефону, електронна адреса, місце проживання/перебування, місце роботи, реєстраційний номер облікової картки платника податків та інші дані, за якими можна ідентифікувати фізичну особу, що розміщені в загальнодоступних базах даних»;

«особливі персональні дані – дані про расову або етнічну приналежність, політичні, релігійні або світоглядні переконання, відомості, що стосуються здоров'я чи статевого життя, генетичні дані, біометричні дані, дані про судимість і кримінальні злочини»;

3) внести зміни до ст. 2 Закону України «Про захист персональних даних» та викласти поняття «володілець персональних даних» в такій редакції: «володілець персональних даних – фізична або юридична особа, орган державної влади чи орган місцевого самоврядування, підприємство, установа, організація, незалежно від форми власності, яка самостійно чи разом з іншими визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом».

4) запровадити в Україні спеціальний орган – Інспекцію з питань захисту персональних даних – для забезпечення реалізації державної політики у сфері захисту персональних даних та дотримання як національного, так і міжнародного законодавства у цій сфері.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Загальна Декларація прав людини ООН від 10.12.1948 р. URL: https://zakon.rada.gov.ua/laws/show/995_015 (дата звернення 15.04.2019).
2. Конвенція про захист прав людини і основоположних свобод від 04.11.1950 р. URL: https://zakon.rada.gov.ua/laws/show/995_004 (дата звернення 01.05.2019).
3. EU General Data Protection Regulation (GDPR). URL: <https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf> (дата звернення 01.05.2019).
4. Право на приватність: Резолюція Ради Європи 1165 від 26 червня 1998 р.
5. Про захист осіб у зв'язку з автоматизованою обробкою персональних даних : Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; Amendment to Convention ETS No. 108 allowing the European Communities to accede) : Конвенція Ради Європи від 28.01.81 р. № 108. URL: <http://www.convention.coe.int/treaty/en/Treaties/Html/108.html> (дата звернення 17.04.2019).
6. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних : Директива Європейського Парламенту і Ради від 24.10.1995 р. № 95/46/ЄС. URL: https://zakon.rada.gov.ua/laws/show/994_242 (дата звернення 17.04.2019).
7. Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі : Директива Європейського Парламенту і Ради від 15.12.1997 р. № 97/66/ЄС. URL: https://zakon.rada.gov.ua/laws/show/994_243 (дата звернення 20.08.2019).
8. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80> (дата звернення 10.05.2019).
9. Кодекс України про адміністративні правопорушення від 07.12.1984 р. № 8073-X. URL: <https://zakon.rada.gov.ua/laws/show/80731-10> (дата звернення 23.08.2019).

10. Кримінальний кодекс України від 05.04.2001 р. № 2341-III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#n1190> (дата звернення 23.08.2019).
11. Цивільний кодекс України від 16.01.2003 р. № 435-IV. URL: <http://zakon5.rada.gov.ua/laws/show/435-15> (дата звернення 14.09.2019).
12. Цивільний процесуальний кодекс України від 18.03.2004 р. № 1618-IV. URL: <https://zakon.rada.gov.ua/laws/show/1618-15> (дата звернення 23.08.2019).
13. Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Закону України «Про інформацію» та Закону України «Про доступ до публічної інформації» : Закон України від 27.03.2014 р. № 1170-VII. URL: <https://zakon.rada.gov.ua/laws/show/1170-18> (дата звернення 23.08.2019).
14. Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних : Закон України від 04.02.2012 р. № 4343-VI. URL: <https://zakon.rada.gov.ua/laws/show/3454-17> (дата звернення 20.08.2019).
15. Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних : Закон України від 03 липня 2013 р. № 383-VII. URL: <https://zakon.rada.gov.ua/laws/show/383-18> (дата звернення 01.05.2019).
16. Про доступ до публічної інформації : Закон України від 13.01.2011 р. № 2939-VI. URL: <https://zakon.rada.gov.ua/laws/show/2939-17> (дата звернення 20.08.2019).
17. Про електронні комунікації : Закон Естонії від 08.12.2004 р. URL: <https://www.riigiteataja.ee/akt/105072013003?leiaKehtiv> (дата звернення 01.09.2019).
18. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення 17.09.2019).
19. Про захист персональних даних : Закон Естонії від 15.02.2007 р. URL: <https://www.riigiteataja.ee/akt/130122010011?leiaKehtiv> (дата звернення 01.09.2019).

20. Про інформацію : Закон України від 01.06.2010 р. № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення 01.09.2019).

21. Про медіацію : Проект Закону України від 17.12.2015 р. № 3665. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=57463 (дата звернення 01.09.2019).

22. Про публічну інформацію : Закон Естонії від 15.11.2000 р. URL: <https://www.riigiteataja.ee/akt/119122012005?leiaKehtiv> (дата звернення 01.09.2019).

23. Про Стратегію реформування судоустрою, судочинства та суміжних правових інститутів на 2015-2020 роки : Указ Президента України від 20.05.2015 р. № 276/2015. URL : <http://zakon3.rada.gov.ua/laws/show/276/2015>. (дата звернення 25.08.2019).

24. Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних : Наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 р. № 1/02-14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#n92 (дата звернення 01.05.2019).

25. Про затвердження документів у сфері захисту персональних даних : Наказ Уповноваженого від 08 січня 2014 р. № № 1/02-14 (дата звернення 01.05.2019).

26. Типовий порядок обробки персональних даних : Наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 р. № 1/02-14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14 (дата звернення 01.05.2019).

27. Деякі питання практичного застосування Закону України «Про захист персональних даних» : Роз'яснення Міністерства юстиції України від 21.12.2011р. URL: <http://zakon3.rada.gov.ua/laws/show/n0076323-11> (дата звернення 20.04.2019).

28. Google Spain SL Google Inc. V Agencia Española de Protección de Datos (AEPD) Mario Costeja Gonzalez Judgment of the Court (Grand Chamber) in Case C-131/12, 13 May 2014. URL:

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131> (дата звернення 15.05.2019).

29. Van Oosterwijk v Belgium judgment of 6 November 1980, Series A, No. 40. 22 P. URL: <http://www.pfc.org.uk/caselaw/The%20Van%20Oosterwijk%20case.pdf> (дата звернення 15.05.2019).

30. С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom) за заявами №№ 30562/04 і 30566/04, Рішення ЄСПЛ від 04 грудня 2008 р. URL: http://europeancourt.eu/uploads/ECHR_S_and_Marper_v_The_United_Kingdom_04_12_2008.pdf (дата звернення 15.05.2019).

31. Рішення Конституційного Суду України від 25.12.1997 р. № 9-зп. URL: <http://zakon5.rada.gov.ua/laws/show/v009p710-97/paran54#n54> (дата звернення 23.08.2019).

32. 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. № 2-рп/2012. URL: <https://zakon.rada.gov.ua/laws/main/v002p710-12> (дата звернення 23.08.2019).

33. Про внесення змін та доповнень до постанови Пленуму Верховного Суду України від 31 березня 1995 р. № 4 «Про судову практику в справах про відшкодування моральної (немайнової) шкоди» : Постанова Верховного суду України від 25.05.2001 р. № 5. URL: <https://zakon.rada.gov.ua/laws/show/v0005700-01> (дата звернення 23.08.2019).

34. Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи : Постанова Пленуму Верховного Суду України від 27.02.2009 р. № 1. URL: https://zakon.rada.gov.ua/laws/show/v_001700-09 (дата звернення 23.08.2019).

35. Постанова Судової палати у цивільних справах Верховного суду України від 27.09.2017 р. у справі № 369/5585/15-ц. Єдиний державний реєстр судових рішень: [сайт]. URL: <http://reyestr.court.gov.ua/Review/70427210> (дата звернення 23.08.2019).

36. Рішення Апеляційного суду Харківської області від 12 квітня 2018 р. у справі № 645/545/17. Єдиний державний реєстр судових рішень: [сайт]. URL: <http://reyestr.court.gov.ua/Review/73528431> (дата звернення 23.10.2019).

37. Рішення Вінницького міського суду Вінницької області від 03 червня 2014 р. у справі № 127/7229/14-ц. Єдиний державний реєстр судових рішень: [сайт]. URL: <http://reyestr.court.gov.ua/Review/39125979> (дата звернення 23.08.2019).

38. Рішення Голосіївського районного суду м. Києва від 30 травня 2016 р. Єдиний державний реєстр судових рішень: [сайт]. URL: <http://reyestr.court.gov.ua/Review/58136830> (дата звернення 23.08.2019).

39. Рішення Запорізького районного суду у Запорізькій області від 29 березня 2019 р. у справі № 752/5161/16-ц. Єдиний державний реєстр судових рішень: [сайт]. URL: <http://reyestr.court.gov.ua/Review/80910846> (дата звернення 23.08.2019).

40. Рішення Червонозаводського районного суду міста Харкова від 27 квітня 2015 р. у справі № 646/901/15-ц. Єдиний державний реєстр судових рішень: [сайт]. URL: <http://reyestr.court.gov.ua/Review/44141588> (дата звернення 23.08.2019).

41. National Security Agency. Офіційний сайт. URL: <https://www.nsa.gov/> (дата звернення 17.09.2019).

42. Information Commissioner's Office (ICO). Офіційний сайт. URL: <https://ico.org.uk/> (дата звернення 17.09.2019).

43. Антонюк О. Заходи самозахисту цивільних прав та інтересів. *Підприємництво, господарство і право: науково-практичний господарсько-правовий журнал*. Київ. 2003. № 6. С. 26.

44. Білан І. Огляд міжнародного законодавства в сфері регулювання захисту персональних даних. URL: <http://www.ucipr.kiev.ua/modules.php?op=modload&name=News&file=article&sid=6032695> (дата звернення 15.04.2019).

45. Борисова Л. В., Тулупов В. В. Захист прав суб'єктів персональних даних. *Форум права*. 2013. № 1. С. 96-100.

46. Брель О. С. Персональні дані як об'єкт інформаційних правовідносин за участю суб'єктів господарювання. *Право України*. 2011. № 4. С. 220-224.
47. Бут І. О. Розгляд цивільно-правових спорів третейськими судами в Україні: дис. ... канд. юрид. наук : 12.00.03. Нац. ун-т «Одес. юрид. Акад». Одеса, 2016. 229 с. URL: <http://dspace.onua.edu.ua/bitstream/handle/11300/5686/%d0%91%d1%83%d1%82%20%d0%86.%d0%9e..pdf?sequence=2&isAllowed=y>.
48. Васильев С. В. Порівняльний цивільний процес: підручник. Київ, 2015. 352 с.
49. Волосецький В. О. Законодавство ЄС у сфері захисту персональних даних. *Гілея: науковий вісник*. 2016. № 115. С. 471-474.
50. Дмитренко О. А. Право фізичної особи на власні персональні дані в цивільному праві України : автореф. дис. ... канд. юрид. наук :12.00.03. Київ, 2010. 210 с.
51. Єсімов С. С. Особливості правового режиму інформаційних систем з обробки персональних даних. *Науковий вісник Львівського державного університету внутрішніх справ*. 2018. №1. С. 145-156.
52. Інспекція захисту даних Естонії. URL: <https://www.aki.ee/et> (дата звернення 15.09.2019).
53. Законодательство Великобритании в сфере защиты персональных данных и информационной безопасности. URL:<http://www.uipdp.com/solutions/services/consulting/legislation/eu/england.html> (дата звернення 15.09.2019).
54. Законодательство Франции в сфере защиты персональных данных и информационной безопасности. URL:<http://uipdp.com/solutions/services/consulting/legislation/eu/france.html> (дата звернення 15.09.2019).
55. Камінська Н. В. Захист персональних даних: проблеми внутрішньодержавного, наднаціонального і міжнародно-правового регулювання. *Науковий вісник Національної академії внутрішніх справ*, 2015. № 3. С. 106-114.

56. Касперський І. П. Правові режими захисту персональних даних в Україні. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2011. № 1-2. С. 102-105.
57. Кикіш С. Омбудсмен як альтернативний спосіб захисту прав людини: міф чи реальність? *Юридична газета*. 2018. № 49. С. 26-27.
58. Кравчук М. М. Міжнародний досвід правового регулювання захисту персональних даних в мережі Інтернет. *Наукові записки Інституту законодавства Верховної Ради України*. 2013. № 3. С. 123-126. URL: http://nbuv.gov.ua/UJRN/Nzizvru_2013_3_24 (дата звернення 10.09.2019).
59. Кукіна З. О. Основні аспекти міжнародно-правового регулювання захисту персональних даних. *Актуальні проблеми міжнародних відносин*. 2013. № 115(2). С. 98-104.
60. Кулініч О.О. Цивільно-правовий захист персональних даних фізичних осіб. *Актуальні проблеми держави і права: зб. наук. пр.*, 2007. С. 41-45. URL: <http://www.apdp.in.ua/v33/08.pdf> (дата звернення 25.08.2019).
61. Куруц М. В. Деякі особливості судового захисту інформаційних прав людини. *Судова апеляція*. 2014. № 2. С. 25-32. URL: http://nbuv.gov.ua/UJRN/Suar_2014_2_5/ (дата звернення 02.10.2019).
62. Логінова Н. І., Дробожур Р. Р. Правовий захист інформації : навч. посібн. Одеса, 2015. 264 с.
63. Маркова О. О. Щодо можливості використовувати договір у процедурі примирення сторін для врегулювання конфліктів та спорів: порівняльний аналіз із законодавством країн Європейського Союзу. *Форум права*. 2014. № 3. С. 208-209.
64. Мельник К. С. Іноземний та вітчизняний досвід становлення інституту захисту персональних даних. *Інформаційна безпека людини, суспільства, держави*. 2013. № 2. С. 97-103. URL: http://nbuv.gov.ua/UJRN/iblsd_2013_2_18 (дата звернення 10.09.2019).

65. Мельник К. С. Удосконалення нормативно-правового регулювання захисту персональних даних в Україні. *Правова інформатика*. 2014. № 1. С. 30-43.
66. Мужик А. І., Мужик І. М. Підходи до обробки персональних даних. *Вісник Інженерної академії України*. 2013. № 3-4. С. 103-106. URL: http://nbuv.gov.ua/UJRN/Viau_2013_3-4_23 (дата звернення 02.10.2019).
67. Обуховська Т. І. Захист персональних даних в умовах розвитку інформаційного суспільства: передумови, принципи та міжнародне законодавство. *Вісник Національної академії державного управління при Президентові України*. 2014. № 1. С. 95-103.
68. Обуховська Т. І. Класифікація персональних даних та режиму доступу до них. *Вісник Національної академії державного управління при Президентові України*. 2013. № 1. С. 97-104.
69. Петрицький А. Л. Актуальні проблеми правового забезпечення захисту персональних даних в Україні. *Вісник Маріупольського державного університету*. 2013. № 6. С. 111-119.
70. Різак М. В. Класифікація персональних даних як необхідний елемент введення ефективної комунікації в суспільстві. *Науковий вісник Міжнародного гуманітарного університету*. 2013. № 6-3(1). С. 91-95.
71. Сопілко І. М. Міжнародно-правовий досвід захисту персональних даних: напрямки вдосконалення для України. *Юридичний вісник. Повітряне і космічне право*. 2014. № 4. С. 70-75.
72. Сухорольський П. Право бути забутим у правовій системі Європейського союзу: реалії, проблеми та перспективи. *Наука міжнародного права на рубежі століть. Тенденції розвитку та трансформації : спеціальне видання наукових статей*. Львів : ЛНУ імені Івана Франка, 2016. С.90-101.
73. Теремецький В. І., Д. В. Цвірюк. Застосування зарубіжного досвіду правового захисту персональних даних в Україні. *Часопис Академії адвокатури України*. 2014, № 2. С. 73-82. URL: http://nbuv.gov.ua/UJRN/Chaa_u_2014_7_2_11 (дата звернення 20.08.2019).

74. Теремецький, В. І. Суб'єкти відносин, пов'язаних з персональними даними. *Право і безпека*. 2015. № 2 (57). С. 171–176.
75. Ткачук О. С. Альтернативне вирішення спорів як форма захисту цивільних прав, свобод та інтересів. *Проблеми законності*. 2016. № 133. С. 20–31.
76. Ярошенко С. Медіація: конфіденційна та швидка нейтралізація конфлікту при мінімумі витрат. *Закон і Бізнес*. 2019. № 15 (1417). URL: https://zib.com.ua/ua/137328mediaciya_konfidenciyna_ta_shvidka_neytralizaciya_konfliktu_.html (дата звернення 20.09.2019).
77. Шарабурина О. О. Проблеми правового захисту персональних даних як відомостей з обмеженим доступом. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право*. 2012. № 4 (16). С. 74–78.