**Київський національний торговельно-економічний університет**

**Кафедра міжнародного, цивільного та комерційного права**

**ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА**

на тему:

# ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В МЕРЕЖІ ІНТЕРНЕТ

студентки 2 курсу, 8 м групи,
спеціальності 081 «Право»,
спеціалізації
«Цивільне право і процес» _____ Ручки Катерини Юріївни

Науковий керівник
к.ю.н., доц. _____ Тищенко Юлія Вікторівна

Гарант освітньої програми
д.ю.н. _____ Примак Володимир Дмитрович

**Київ-2020**

# ЗМІСТ

# ВСТУП

**Актуальність теми.** У наш час, коли йдеться про інформацію та свободу інформації, перш за все, слід говорити про можливості, які надає щодо цього всесвітня мережа Інтернет. У контексті активного користування мережею як глобальним інформаційним середовищем перед Україною постають питання правового врегулювання нових відносин інформаційного характеру, що виникають у системі людина – Інтернет.

Персональні дані особи завжди були, є і будуть ключовим об'єктом особистих немайнових прав фізичної особи, а тому належне правове регулювання правовідносин щодо їх збереження, використання та розповсюдження має вирішальне значення для їх належного правового захисту.

Активність у формуванні баз персональних даних через використання соціальних мереж, факти шахрайства та кіберзлочинності особливо загострили питання правового захисту прав фізичних осіб. Невідкладним стає питання створення адекватної системи законодавства, що регулює захист персональних даних в сучасних соціально-правових реаліях.

Концепція захисту персональних даних, без сумніву, є відміткою загального права людини на приватність та конфіденційність. Вона не тільки була закріплена відповідно до статті 12 Загальної декларації прав людини, вона також була включена до більшості регіональних конвенцій, хартій та договорів з прав людини. Зокрема, слід згадати про Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) (далі – Регламент) [76]. Прийняття Регламенту кардинально вплинуло на захист персональних даних в Україні та на роботу веб-сайтів, які почали прописувати регламенти захисту з метою уникнення

порушень, що у свою чергу, було пов'язано з роботою таких підприємців на європейському ринку.

Слід відзначити наявність досить широкого кола наукових праць, у яких розглядаються різні аспекти проблематики захисту персональних даних в мережі Інтернет, міжнародних відносин у галузі обміну інформацією, здійснення державної та міжнародної інформаційної політики тощо. Безпосередньо науковим дослідженням питань захисту персональних даних займалися: О. А. Баранов [25], К. І. Бєляков [27], В. В. Головченко [31], І. Р. Березовська [**Ошибка! Источник ссылки не найден.**26], І. М. Забара [37], О. С. Каретник [39], А. В. Пазюк [47], М. Різак [56], Д. М. Русак [57], В. І. Теремецький [62], В. М. Фурашев [64], М. Я. Швець [67] та інші.

**Мета дослідження**: визначити особливості правового регулювання суспільних відносин, пов'язаних із захистом персональних даних в мережі Інтернет.

Залежно від мети та враховуючи логіку дослідження перед даною роботою поставлено **завдання**, які сформульовані таким чином:

- розглянути поняття прав суб'єкта персональних даних, їх зміст та види;

- дослідити співвідношення захисту та охорони персональних даних;

- визначити підстави виникнення прав на захист персональних даних в мережі Інтернет;

- проаналізувати правове регулювання захисту персональних даних в мережі Інтернет;

- вивчити форми та способи захисту персональних даних в мережі Інтернет.

**Об'єкт дослідження:** суспільні відносини, що виникають стосовно захисту персональних даних.

**Предмет дослідження:** захист персональних даних в мережі Інтернет.

**Методи дослідження.** У процесі дослідження даної теми були використані загальнонаукові та спеціальні методи, що дозволили всебічно вивчити теоретичні основи та практично розглянути захист персональних даних в мережі Інтернет. Зокрема, відповідно до формально-логічного методу в дослідженні застосовувався категоріально-понятійний апарат та закони логіки. Метод логічного аналізу використовувався для встановлення змісту та спрямованості норм законодавства, які регулюють відносини, що є предметом дослідження. Порівняльно-правовий метод застосовувався при вивченні та порівнянні положень національного та міжнародного законодавства, що стосується захисту персональних даних.

**Наукова новизна** дослідження визначена як комплексний аналіз основних питань захисту персональних даних в мережі Інтернет, порівнянні нормативно-правових актів, що стосуються володіння, використання та обробки персональних даних, виявленні недоліків законодавства, і наведенні пропозицій щодо його удосконалення та гармонізації з правом ЄС про захист персональних даних в мережі Інтернет.

Окремі положення випускної кваліфікаційної роботи викладено у статті «Правове регулювання захисту персональних даних в мережі Інтернет», що опублікована у збірнику наукових статей «Цивільне та комерційне право : виклики сьогодення». К.: Київ. нац. торг.-екон. ун-т, 2020. С. 36-43.

**Практична цінність дослідження** полягає у можливості застосування одержаних результатів: у науковій діяльності – для проведення подальших наукових досліджень, у навчальному процесі – під час проведення лекційних, семінарських і практичних занять, у законотворчій діяльності – з метою вдосконалення чинного законодавства України в частині правового регулювання захисту персональних даних.

**Структура роботи**. Дана випускна кваліфікаційна робота складається із вступу, двох розділів, що включають п’ять підрозділів, висновків та пропозицій, а також списку використаних джерел. Загальний обсяг роботи –

64 сторінки, основного тексту – 54 сторінки. Список використаних джерел налічує 75 найменувань.

# РОЗДІЛ 1
# ПРАВОВІ ЗАСАДИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В МЕРЕЖІ ІНТЕРНЕТ

## 1.1. Поняття прав суб'єкта персональних даних, їх зміст та види

Згідно зі ст. 2 Закону України «Про захист персональних даних» від 01.06.2010 № 2297 (далі – Закон № 2297) суб'єктом персональних даних є фізична особа, персональні дані якої обробляються [11]. Звідси випливає, що права суб'єкта персональних даних варто розуміти як права фізичної особи, персональні дані якої обробляються.

Дещо ширше дана дефініція визначається в науковій літературі. Так, зокрема, В. І. Теремецький під суб'єктом персональних даних пропонує розуміти фізичну особу, якій належать персональні дані, що обробляються, або її представників, які від імені цієї особи надають згоду на таку обробку та здійснюють інші права щодо захисту персональних даних [62, с.173]. Тобто, керуючись науковим підходом стосовно тлумачення поняття суб'єкта персональних даних під його правами маємо розуміти права фізичної особи, якій належать персональні дані, що обробляються, або її представників, які від імені цієї особи надають згоду на таку обробку та здійснюють інші права щодо захисту персональних даних. Вважаємо за доцільне закріпити запропоноване тлумачення у ст. 1 Закону № 2297

Перелік прав суб'єкта персональних даних наведений у ч. 2 ст. 8 Закону № 2297, де зазначається, що 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 [11].

При цьому, необхідно зазначити, що значно розширює права громадян Регламент (ЄС) 2016/679 від 27.04.16 р. «Про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЄС (Загальні Положення про захист даних)» [76]. Зокрема, відповідно до положень Регламенту суб'єкти даних мають право запрошувати підтвердження факту обробки їх даних, місце і мету обробки, категорії оброблюваних персональних даних, яким третім особам вони розкриваються, період, протягом якого дані оброблятимуться, а також уточнюватимуть джерело їх отримання і вимагатимуть їх виправлення. Більш того, суб'єкт даних має право вимагати припинення обробки своїх даних. Регламент встановлює високі вимоги до форми отримання згоди на обробку даних. Згода людини на обробку її персональних даних повинна бути визначена у формі однозначно чіткого твердження про відповідний дозвіл. Наприклад, повідомлення на сайті про те, що суб'єкт даних автоматично дав згоду на збір і обробку його персональних даних, не є згодою фізичної особи. Згода повинна бути надана в активній дії, наприклад, письмовою заявою, зокрема електронним способом. Суб'єкт даних має право на виправлення персональних даних, що стосуються його або її. Комісія ЄС відстоює право кожного користувача Інтернету в ЄС мати також «право бути забутим», тобто право на видалення його/її персональних даних та припинення обробки. Пошукові системи і соціальні мережі зобов'язані стирати фото і інші відомості про суб'єкта даних на його вимогу. Обробка фотографій не повинна розглядатися як обробка особливих категорій персональних даних. Суб'єкт даних має право заперечувати проти обробки його даних, яка здійснюється з метою прямого маркетингу, у тому числі профілювання, до ступеню, в якому це пов'язано з таким маркетингом, стосовно як початкової, так і подальшої обробки. Діти заслуговують на

особливий захист їх персональних даних. Не можна вимагати згоду на обробку в контексті надання профілактичних або консультаційних послуг безпосередньо у дитини. Згода повинна бути авторизована батьками (або законними представниками дитини). Віковий поріг авторизації встановлюється державами-членами ЄС окремо (від 13 до 16 років). Фізичні особи повинні бути обізнані про ризики, правила, гарантії та права стосовно обробки персональних даних та здійснення своїх прав стосовно такої обробки. Кожен суб'єкт даних має право подати скаргу до національного наглядового органу, зокрема у державі-члені, де він чи вона постійно проживає, та право на ефективні засоби правового захисту. У випадку проваджень проти контролера або обробника позивач повинен мати можливість подавати позов до судів держав-членів, де розташовані установи контролера або обробника або де проживає суб'єкт даних, за винятком випадків, коли контролер є державним органом держави-члена, що діє при здійсненні своїх публічних повноважень.

Зауважимо, що кожна людина з моменту народження отримує комплекс невід'ємних прав і свобод, основними з яких є захист приватного життя та особиста недоторканність, що включають право на захист персональних даних. Так, відповідно до ч. 1 ст. 270 Цивільного кодексу України (далі – ЦК України), фізична особа має право на життя, право на охорону здоров'я, право на безпечне для життя і здоров'я довкілля, право на свободу та особисту недоторканність, право на недоторканність особистого і сімейного життя, право на повагу до гідності та честі, право на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції, право на недоторканність житла, право на вільний вибір місця проживання та на свободу пересування, право на свободу літературної, художньої, наукової і технічної творчості [8].

Не можна також оминути увагою закон Європейського Союзу про конфіденційність даних, який гармонізує закони про конфіденційність в

усьому ЄС і оновлює директиву із захисту даних. Йдеться про Директиву 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 (далі – Директива про захист персональних даних, Директива) [3].

Серед основних прав, які були вдосконалені Регламентом, варто виділити такі:

1. Право бути поінформованим. Якщо інформація збирається безпосередньо від індивіда, необхідним є його оповіщення про це та отримання однозначної згоди. Згода повинна бути відкритою, явно вираженою та незавуальованою (наприклад, на практиці може виражатися як проставляння галочки біля кожного пункту персональних даних, що вводяться у мобільному додатку виклику таксі). Згода не може бути мовчазною та повинна бути відділена від інших умов договору (в тому числі приєднання як terms and conditions в соціальних мережах).

2. Право на видалення (право бути забутим). За запитом суб'єкта, вся інформація про нього повинна бути видалена. Цього правила можна не дотримуватися, якщо інформація необхідна для реалізації права на інформацію, виконання норм чинного законодавства, забезпечення громадського здоров'я, наукової, історичної чи статистичної мети, вирішення правових спорів. Компанії, які можуть розміщувати інформацію користувачів онлайн, повинні за запитом особи видаляти не лише інформацію, а й посилання на неї чи будь-які можливі копії.

3. Право на заборону обробки. Компанія зобов'язана відмовитися від обробки персональних даних на вимогу суб'єкта. Методами, за допомогою яких компанія може це здійснити, є унеможливлення доступу третіх осіб до даних, видалення їх із веб-сайту тощо.

Директива встановлює низку принципів обробки персональних даних серед яких можна виділити наступні:

1. принцип законності обробки;

2. принцип конкретизації цілей та обмеження;

3. принципи якості персональних даних, що включає принцип відповідності даних, принцип точності даних, принцип збереження даних протягом обмеженого періоду,

4. принцип ретельності обробки, що включає прозорість, формування довіри;

5. принцип підзвітності.

Відповідно до права про захист персональних даних ЄС та РЄ принцип законності обробки є першим із перерахованих принципів. Зауважимо, що цей принцип майже однаково визначається у статті 5 Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року (далі – Конвенція 108) та у статті 6 Директиви про захист персональних даних. Жодне з цих положень не містить визначення того, що наповнює поняття «законна обробка». Щоб зрозуміти цей юридичний термін, необхідно звернутися до визначеного у Конвенції про захист прав людини і основоположних свобод (далі – ЄКПЛ) поняття виправданого втручання у тлумаченні судової практики Європейського суду з прав людини (далі – ЄСПЛ).

Обробка персональних даних може бути втручанням у право на повагу до приватного життя суб’єкта персональних даних. Проте право на повагу до приватного життя не є абсолютним, воно має бути збалансоване і узгоджене з іншими законними інтересами, незалежно від того, чи це інтереси інших осіб (приватні інтереси), чи інтереси суспільства в цілому (суспільні інтереси).

Принцип конкретизації і обмеження мети означає, що законність обробки персональних даних залежить від мети обробки. Мета обробки персональних даних має бути чітко визначена та оприлюднена володільцем до початку процесу обробки. Відповідно до права ЄС це здійснюється або в заявному порядку, інакше кажучи, шляхом надсилання повідомлення до

відповідного наглядового органу або, як мінімум, шляхом розробки внутрішньої документації, яку слід надати для здійснення інспекції наглядовим органам та надати до неї доступ суб'єкту персональних даних.

Тільки ті дані підлягають обробці, які є «адекватними, відповідними та ненадмірними стосовно мети, з якою вони збираються та/або обробляються». Категорії вибраних для обробки персональних даних мають бути необхідними для досягнення заявленої загальної мети здійснення операцій з обробки, а володілець повинен суворо обмежувати процес збирання персональних даних такою інформацією, що прямо відповідає конкретній меті, яку переслідує процедура обробки. У сучасному суспільстві принцип відповідності персональних даних має додаткове значення: використання персональних даних можна взагалі уникнути, якщо використовувати технології підвищеної конфіденційності або псевдоніми, результатом чого може рішення, сприятливе для забезпечення приватності. Це особливо доречно в системах з великим обсягом даних, які оброблюються.

Володілець персональних даних не повинен використовувати надану інформацію, не пересвідчившись у тому, що вона точна і актуалізована. Обов'язок щодо забезпечення точності даних слід розглядати в контексті мети обробки персональних даних.

У статті 6 (1) (e) Директиви про захист персональних даних, а також у статті 5 (e) Конвенції 108 від держав-членів вимагається забезпечити збереження персональних даних «у формі, що дозволяє встановлювати особу суб'єктів персональних даних не довше, ніж це необхідно з метою, заради якої дані були зібрані чи заради якої вони надалі обробляються». Тому персональні дані повинні бути видалені, якщо цієї мети вже немає. Так, у справі «С. і Марпер» ЄСПЛ дійшов висновку, що основні принципи відповідних документів Ради Європи, законодавство і практика інших Договірних Сторін вимагають, щоб збереження даних було пропорційним

меті збирання та обмежувалось у часі, особливо у секторі діяльності поліції [17, с.123].

Принцип ретельності обробки регулює, передусім, взаємовідносини між володільцем та суб'єктом персональних даних. Цей принцип зобов'язує володільця персональних даних постійно інформувати суб'єктів персональних даних про те, як використовуються їхні персональні дані.

Підзвітність вимагає від володільців активного здійснення заходів щодо підтримки та захисту персональних даних під час їхньої обробки. Володільці відповідають за відповідність операцій з обробки законодавству про захист персональних даних. Володільці мають бути готові у будь-який час продемонструвати відповідність нормам закону про захист персональних даних суб'єктам персональних даних, громадськості та наглядовим органам.

Необхідно зазначити, що всі розроблені пізніше правові документи РЄ або ЄС про захист персональних даних повинні відповідати цим принципам, і ці принципи слід враховувати під час тлумачення таких правових документів. Будь-які винятки і обмеження щодо цих ключових принципів мають бути передбачені на національному рівні [51, с.68].

Отже, права суб'єкта персональних даних слід розглядати як права фізичної особи, якій належать оброблювані персональні дані, або права представників, які від імені цієї особи надають згоду на таку обробку і відповідно здійснюють інші права щодо захисту персональних даних. Згідно з ч. 1 ст. 8 Закону № 2297 особисті немайнові права суб'єкта персональних даних на персональні дані є невід'ємними та непорушними. Вважаємо, що найбільш повний перелік прав суб'єкта персональних даних з погляду національного законодавства наведено в ч. 2 ст. 8 Закону № 2297. Принагідно зауважимо, що вказаний перелік прав у різних країнах може відрізнятися. Це пояснюється зокрема неоднорідністю правозастосовної практики, швидкістю розвитку інформаційних технологій, неможливістю охопити всі сфери

сучасного життя і, звичайно, передбачити всі ймовірні та малоймовірні ситуації.

## 1.2. Захист та охорона персональних даних: питання співвідношення

У контексті досліджуваної теми варто також розглянути питання співвідношення захисту та охорони персональних даних. Переходячи до безпосереднього вивчення цього питання, насамперед, слід звернути увагу на проблему, яка пов'язана з використанням понять «охорона» і «захист». Їх використовують досить широко, але чіткого розмежування цих понять не прослідковується. Одним із ключових питань у дослідженнях будь-якого правового явища є питання про його зміст. Ці дефініції дуже близькі за змістом, а тому іноді вживаються в юридичній літературі як тотожні слова, та не мають чітких відмінностей. Наприклад, в одному з тлумачних словників поняття «захист» визначається як те, що захищає, служить обороною, а слово «захищати» охороняти, огородити від посягань, від негативних дій, від небезпеки; попередити, убезпечити від чого-небудь. Так виникає ситуація, коли «охорона» визначається за допомогою слова «захист», а «захист» - слова «охорона».

У деяких дисертаційних дослідженнях робляться поодинокі спроби здійснити розмежування. На думку Ю. С. Довгаль, їх не можна визнати вдалими, за винятком роботи Р. Б. Шишки, який наголошує на необхідності розмежування захисту права та його охорони, аналізує право на захист, яке, на його думку, є самостійним суб'єктивним правом та включає в себе дві правомочності: право позитивної поведінки управленої особи і право вимагати відповідної поведінки від правозобов'язаної особи [69, с. 318; 326]. До того ж право на захист розуміється як самостійне суб'єктивне право і реальна правова можливість, що виникає лише за порушення або оскарження

останнього і реалізується в межах охоронних правовідносин [69, с. 134]. У найбільш загальному плані можна стверджувати, що захист здійснюється лише щодо порушених прав, тоді як охорона має перманентний характер, і її завданням, передусім, є створення умов для реалізації цих прав.

Я. М. Шевченко вважає, що «поняття охорони включає в себе поряд із заходами економічного, політичного, ідеологічного характеру, що забезпечують нормальне регулювання суспільних відносин, попередження правопорушень, усунення причин, що їх породжують (регулятивні норми), а також і заходи, спрямовані на поновлення чи визнання прав у разі порушення чи оспорювання їх, а саме: захист (охоронні норми)» [68, с. 139].

Основна мета захисту полягає в необхідності негайно відновити порушене право, сприяти запобіганню порушень прав у майбутньому [30, с.11].

Захистом, на думку Ю. С. Довгаль, ми можемо назвати державно примусову діяльність спеціальних органів державної влади, спрямовану на поновлення порушеного права, а охороною сукупність засобів, методів та способів, що спрямовані на забезпечення нормальної реалізації прав [35, с.84-85].

В. Темченко вважає, що «термін «захист» у єдності термінологічних конструкцій, що позначають певні суб'єктивні процесуальні можливості (право) особи щодо захисту порушених прав, стосується будь-якого конституційного права чи свободи, незалежно від буквального вживання цього терміну безпосередньо у тексті норм Конституції. Це право логічно виокремлюється відповідно до теоретичного поняття суб'єктивного права та його структури в якому структура складається із наступних загальновизнаних теоретичною наукою елементів: право особи на власні фактичні чи юридичні дії – право - поведінка; право вимагати від іншої сторони виконання обов'язків - право-вимога; можливість звертатися за захистом до компетентних державних органів - право-домагання; можливість

користуватися певним соціальним благом, цінністю - право-користування» [61, с.61].

Керуючись вищенаведеним, пропонуємо під охороною персональних даних розуміти сукупність засобів, методів та способів, що спрямовані на гарантування особистих немайнових прав на персональні дані, а під захистом – державно-примусову діяльність спеціальних органів державної влади, спрямовану на поновлення порушених особистих немайнових прав на персональні дані.

При цьому, маємо зазначити, що під персональними даними варто розуміти відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [11]. При цьому, відповідно до Закону України «Про інформацію» від 02.10.1992 № 2658 (далі – Закон № 2658) [12], будь-які персональні дані (інформація про фізичну особу) водночас вважаються конфіденційною інформацією, тобто інформацією з обмеженим доступом. Трохи вужчим до конфіденційної інформації є підхід, закладений в Законі України 13.01.2011 № 2939 «Про доступ до публічної інформації» [10] і в Законі України № 2297 [11]. Додаткову плутану створює той факт, що згідно з абз. 2 ч. 1 ст. 302 ЦК України [8] «збирання, зберігання, використання і поширення інформації про особисте життя фізичної особи без її згоди не допускаються, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини». Отже, мова йде ще про окремий законодавчий термін «інформація про особисте життя фізичної особи».

Зауважимо, що у Регламенті, Директиві, Конвенції 108 та Законі № 2297 поняття персональних даних визначено приблизно однаково, а саме як: «будь-яка інформація, яка стосується ідентифікованої особи або особи, яка може бути ідентифікованою». Ключовим у вищенаведеному визначенні також є поняття «ідентифікована особа». Таким чином, ідентифікованою є особа, яку за наявною в розпорядженні володільця інформацією можна

безпомилково виділити з-посеред інших осіб. Зазвичай для того, щоб вважати особу ідентифікованою, необхідні її ім'я, прізвище, по батькові та реквізити документа, що посвідчує особу/цифровий номер, що присвоюється особі (наприклад, ідентифікаційний номер фізичної особи). Однак, за певних умов наявність меншої кількості інформації чи певного об'єму іншої інформації є достатніми для того, щоб ідентифікувати особу (див. приклади нижче). Більше деталей у цьому відношенні передбачає Регламент.

У той же час, Регламент містить найбільш сучасне та практичне визначення «особи, що може бути ідентифікованою», згідно з яким це «особа, яку можна ідентифікувати прямо чи опосередковано, зокрема вказавши такі ідентифікатори, як ім'я, ідентифікаційний номер, дані щодо місцезнаходження, онлайн ідентифікатор чи інші особливості фізичної, фізіологічної, генетичної, духовної, економічної, культурної чи соціальної ідентичності такої фізичної особи».

Простіше кажучи, приватні дані – це будь-яка інформація, яка в кінцевому підсумку може ідентифікувати суб'єкта даних, навіть якщо вона віддалена.

Необхідно зазначити, що у чинному законодавстві дуже часто «інформація про особу» і «персональні дані» ототожнюються. Схожа позиція і в теорії. Так, О.О. Серебряник так само вважає, що між термінами «персональні дані» та «інформація про особу» можна поставити знак рівності, український законодавець вживає терміни «інформація про фізичну особу» і «персональні дані» як синоніми [59, с. 38, 79].

На думку А. Туніка та О. Чуприни, аналіз дефініцій «персональні дані» та «інформація про особу» свідчить, що у вітчизняному законодавстві вони є ідентичними, а тому можуть вживатися як синонімічні та взаємозамінні [63, с. 51; **Ошибка! Источник ссылки не найден.**65, с. 105].

Так само можна вважати, що шляхом ототожнення інформації про особу, персональних даних, інформації про особисте і сімейне життя та

визнання цих явищ конфіденційною інформацією пішов і Конституційний Суд України (далі – КСУ). Так, у Рішенні від 20 січня 2012 р. № 2-рп/2012 КСУ зазначив: «інформацією про особисте та сімейне життя особи є будь-які відомості та/або дані про відносини немайнового та майнового характеру, обставини, події, стосунки тощо, пов'язані з особою та членами її сім'ї, за винятком передбаченої законами інформації, що стосується здійснення особою, яка займає посаду, пов'язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень. Така інформація про особу є конфіденційною". У мотивувальній частині цього ж Рішення КСУ надав визначення терміна "інформація про особисте та сімейне життя особи (персональні дані про неї)». На його думку, це будь-які відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована, а саме: національність, освіта, сімейний стан, релігійні переконання, стан здоров'я, матеріальний стан, адреса, дата й місце народження, місце проживання та перебування тощо, дані про особисті майнові та немайнові відносини цієї особи з іншими особами, зокрема із членами сім'ї, а також відомості про події та явища, що відбувалися або відбуваються у побутовому, інтимному, товариському, професійному, діловому й інших сферах життя особи, за винятком даних стосовно виконання повноважень особою, яка займає посаду, пов'язану із здійсненням функцій держави або органів місцевого самоврядування. Фактично КСУ визнав тотожними терміни «конфіденційна інформація про особу», «інформація про особисте і сімейне життя", "персональні дані". При цьому, за логікою КСУ, конфіденційною є вся інформація про особисте і сімейне життя (інформація про особу, персональні дані) без орієнтації на обмеження доступу до зазначеної інформації і встановлення такого режиму щодо конкретної інформації законом чи самою особою.

На переконання І.В. Михайленко, персональні дані – це конфіденційна інформація, закріплена на матеріальних носіях (у документах, комп'ютері

тощо), а інформація про приватне життя – це відомості особистого характеру, що не підлягають розголошенню [43, с. 12]. А О.О. Серебряник вважає, що до змісту інформації про фізичну особу входять: інформація про приватне життя людини, персональні дані, комунікаційні дані (метадані) [59, с. 97].

О.П. Радкевич стверджує, що інформація, яка дозволяє безпосередньо або за допомогою інших чинників ідентифікувати особу, є персональною інформацією, а інформація, надана в електронному вигляді, що складається із знаків і чисел, є персональними даними [54, с. 123].

Щодо чіткого переліку відомостей про фізичну особу, які є персональними даними, то в зв'язку з численними зверненнями громадян щодо практичного застосування деяких положень Закону № 2297 Міністерство юстиції України надало роз'яснення з найбільш актуальних та поширених питань у цій сфері, зокрема зауважило, що «законодавством України не встановлено і не може бути встановлено чіткого переліку відомостей про фізичну особу, які є персональними даними, задля можливості застосування положень Закону України «Про захист персональних даних» до різноманітних ситуацій, 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» [34].

Що ж стосується позиції науковців, то, для прикладу, на думку О. С. Каретник, персональні дані – це конкретні відомості про суб'єктивні цивільні права і юридичні обов'язки особи, які забезпечують її правосуб'єктну персоніфікацію [39, с.230]. Як зазначає О. В. Оніщенко, первинними джерелами відомостей про фізичну особу є видані на її ім'я документи, підписані нею документи, відомості, які особа надає про себе. Тобто відомості про працівників, відображені в кадрових документах, зокрема про вік, дату і місце народження, місце проживання,

ідентифікаційний номер, соціальний статус, пільги відповідно до закону, варто розглядати як персональні дані, які в сукупності становлять базу персональних даних або її частину [46, с. 173].

Показовим є рішення Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ у справі № 6-25324ск14 щодо внесення персональних даних до автоматизованої системи бази даних «Укрзалізниці». Зокрема, зазначено, що прізвище та ім'я особи не є персональними даними, оскільки за ними неможливо ідентифікувати особу. Для ідентифікації конкретної особи за прізвищем та іменем необхідні додаткові дані про неї. Відповідно до листа Міністерства юстиції України від 15 листопада 2013 року № 13232-0-26-13/61, у якому зазначено, що Рекомендацією СМ/Лес (2010) Комітету Міністрів Ради Європи державам-членам щодо захисту осіб у зв'язку з автоматизованою обробкою персональних даних у контексті їх профілювання визначено, що під персональними даними розуміється виключно інформація, за допомогою якої особа ідентифікується або може бути ідентифікована [22, с.69-70].

У національній правовій системі право на захист персональних даних є елементом структури права на недоторканність особистого життя, що сформувалося в умовах кардинальної зміни способу обробки інформації. Зміст права на захист персональних даних становить виключення можливості будь-яких дій з персональними даними без згоди суб'єкта таких даних, а також забезпечення можливості цих суб'єктів контролювати дії операторів обробки зі своїми персональними даними [36, с.202].

Право на захист є суб'єктивним правом особи, що складається із правомочностей уповноваженої особи: права на свої дії (застосовувати захист чи не застосовувати); права на чужі дії – (вимагати певної поведінки від зобов'язаної особи); звертатися до юрисдикційного органу або вдатися до самозахисту у випадку не виконання зобов'язаною особою свого обов'язку. Цей обов'язок може бути активним (як правило у відносних

правовідношеннях), проте в більшості випадків коли мова йдеться про абсолютні правовідносини є пасивним (не втручатися в особисте та сімейне життя особи, не розголошувати лікарську таємницю, не порушувати таємницю листування, телефонних розмов, тощо). Право на захист виникає у особи у разі порушення особистого немайнового права, його невизнання, оспорювання або реальної загрози порушення цього права [25, с.604].

Отже, незважаючи на те, що поняття «захист» і «охорона» мають схоже значення, у контексті тематики персональних даних можемо прослідкувати суттєву різницю. Під охороною персональних даних слід розуміти сукупність методів, засобів та способів, які спрямовані на гарантування особистих немайнових прав особи на персональні дані. У свою чергу захист персональних даних – державно-примусова діяльність спеціальних органів влади, спрямована на поновлення порушених особистих немайнових прав на персональні дані.

### 1.3. Правове регулювання захисту персональних даних в мережі Інтернет

Основна роль у формуванні національної моделі механізму правового захисту персональних даних людини й громадянина розкривається через конституційні засади, що містяться у ст. 3, 28, 30, 31, 32, 34, 35, 41, 54, 55, 64 Конституції України [**Ошибка! Источник ссылки не найден.**1]. Відсутність у тексті Основного закону спеціально визначеного права на захист персональних даних не є перешкодою для визнання цього права предметом конституційного захисту, оскільки такий захист передбачений комплексом положень конституційних норм розд. 2 Конституції України [31].

Цивільним кодексом України персональні дані віднесені до особистих немайнових прав, передбачений судовий порядок їх захисту від протиправних посягань. Стаття 301 ЦК України зокрема визначає, що особа,

яка має доступ до персональних даних (конфіденційної інформації), зобов'язана не передавати таку інформацію третім особам без згоди на це її власника [8]. Винятком може бути інформація стосовно вчинених конкретною особою діянь протиправного (кримінального) характеру.

Основним законом, що регулює механізм поводження з персональними даними в нашій державі, є вже згаданий вище Закон №2297 [11]. У ст. 2 Закону №2297 визначаються зміст та значення основних термінів, які вживаються. Зокрема, висвітлено що персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифіковано. Дане визначення є майже тотожним поданому в Конвенції № 108 [5] та Директиві про захист персональних даних [3].

Гадаємо, варто погодитись із В.В. Головченком у тому, що недоліком такого визначення персональних даних є те, що в ньому відсутні критерії, за якими можна відрізнити персональні дані від будь-якої іншої (наприклад, конфіденційної) інформації про особу. Тому, вважаємо, що Закон №2297 не охоплює різноманітність проблемних правовідносин у сфері захисту персональних даних, що є важливим питанням у наш час, з огляду на те, що громадяни через низький рівень правової обізнаності часто ігнорують проблеми, пов'язані із захистом власних персональних даних [58]

Пізніше було ухвалено Закон України «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних» від 02.06.2011 № 3454 (далі - Закон № 3454) [9], яким доповнено зміст ст. 188-39, 188-40, 182 Кодексу України «Про адміністративні правопорушення». У даному законі передбачено відповідальність за порушення недоторканності приватного життя у вигляді штрафу.

Вважаємо, що персональні дані – це не лише недоторканність приватного життя, тому ефективність вказаних нововведень доволі сумнівна. На нашу думку, право на захист персональних даних, серед всіх

фундаментальних прав людини, - одна з найбільш мінливих правових категорій, що пов'язано зі стрімким розвитком інформаційних технологій, способів накопичення та обробки інформації. З огляду на визначення персональних даних, наведене вище у Законі №2297, пропонуємо внести доповнення до Закону № 3454, зокрема щодо уніфікації формулювання та поширення відповідальності за порушення не лише недоторканності приватного життя, але й інших пов'язаних аспектів персональних даних. [58]

У реаліях сучасного світу гостро постає питання захисту персональних даних в мережі Інтернет. Загальновідомим є те, що при користуванні Інтернетом значні обсяги персональних даних обробляються і передаються, без чіткої згоди і навіть інформування про їх обробку.

Існує необхідність доопрацювання процедур обробки персональних даних з використанням веб-ресурсів, зокрема встановлення процедури повідомлення відвідувачів сайтів про їх права, про склад та зміст персональних даних, що збираються, про мету збору персональних даних та про осіб, яким передаються їхні персональні дані.

Також потрібно усунути й інші порушення, зокрема такі, як надання безвідкличної чи безстрокової згоди на обробку персональних даних, передача персональних даних невстановленим третім особам тощо. Варто наголосити на праві суб'єкта персональних даних на знищення своїх даних, в разі відсутності підстав для їх обробки [**Ошибка! Источник ссылки не найден.**26, с.79]. У зв'язку з цим та з огляду на вищевказане гадаємо, що доречним буде внести відповідні доповнення в зазначений вище Закон №2297.

Гадаємо, далі слід зазначити, що актуальним з огляду на захист персональних даних в мережі Інтернет є розуміння понять «кібербезпека» і «кіберзахист».

Регулювання питань кіберзахисту на національному рівні почалося зі створенням Закону України «Про основні засади забезпечення кібербезпеки

України» від 21.06.2018 № 2469 [13] (далі - Закон № 2469). У пункті 7 ст. 1 даного закону визначено, що кіберзахист – це сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості й надійності функціонування комунікаційних, технологічних систем[13].

Метою Закону № 2469 є створення національної системи кібербезпеки, що сприятиме захисту важливих інтересів суспільства та держави в цілому. Закон висвітлює основні поняття, визначає об'єкти кіберзахисту та виділяє ключових осіб, які мають слідкувати за реалізацією такого захисту.

Вважаємо, що важливим є питання, чи захищатиме Закон № 2469 інтереси окремої особи як індивіда, адже основна увага в нормативно-правовому акті зосереджується на захисті прав суспільства та держави в кіберпросторі. На нашу думку, саме людина як індивід зазнає найбільш негативних впливів у сучасному інформаційному просторі. Важливою складовою цього питання є недостатність розуміння того, що саме повинно захищатися в контексті інформаційної безпеки особи. У зв'язку з цим, гадаємо, що доречним було б внести зміни та доповнення до Закону № 2469. Зокрема, слід врегулювати питання захисту людини як індивіда в кіберпросторі, як одного з найбільш вразливих суб'єктів інформаційного середовища, а також визначити основні аспекти захисту персональних даних особи в мережі Інтернет.

Підкреслимо, що загалом національне законодавство щодо захисту персональних даних складається з більше ніж 20 нормативно-правових актів. Крім зазначених вище, слід згадати Типовий порядок обробки персональних даних, затверджений наказом Уповноваженого Верховної Ради України від 08.01.2014 № 1/02-14 [16] – підзаконний нормативно-правовий акт, затверджений наказом Уповноваженого Верховної Ради України з прав

людини, як уповноваженого органу у сфері захисту персональних даних. У даному порядку визначено загальні вимоги до обробки та захисту персональних даних суб'єктів персональних даних, що обробляються повністю чи частково із застосуванням автоматизованих засобів, а також персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів.

Повертаючись до уповноваженого органу у сфері захисту персональних даних, Уповноваженого Верховної Ради України з прав людини (далі – Уповноважений), підкреслимо, що його основною функцією у даному полі є контроль за додержанням законодавства про захист персональних даних, здійснюваний 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. Процедура проведення перевірок встановлена Порядком здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних, затвердженим наказом Уповноваженого Верховної Ради України з прав людини 08.01.2014 №1/02-14 [15].

Принагідно зауважимо, що існування єдиного незалежного уповноваженого органу у сфері захисту персональних даних, як того вимагає Конвенція 108 [5] є кроком вперед у відповідності регулювання вказаного питання Європейським нормам, оскільки Україна є асоційованим членом Європейського союзу.

Слід згадати, що національну конструкцію права на забезпечення конфіденційності персональних даних складають зокрема й рішення Конституційного Суду України. Зокрема, відповідно до правової позиції КСУ у справі Устименка К.Г., «...забороняється не лише збирання, але й зберігання, використання та поширення конфіденційної інформації про особу

без її попередньої згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту, прав та свобод людини» (Рішення КС України від 30.10.1997 №5-зп у справі щодо офіційного тлумачення ст. 3, 23, 31, 47, 48 Закону № 2658 та статті 12 Закону України «Про прокуратуру» (справа К.Г.Устименка) [21] та Рішення КС України від 20.01.2012 № 2-рп/2012 за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України) [20]. Цими ж рішеннями КС України визначено, щодо конфіденційної інформації про особу належать такі свідчення про особу як освіта, сімейний стан, релігійність, стан здоров'я, дата і місце народження, майновий стан, інші персональні дані [31].

Варто звернути увагу і на практику Верховного суду (далі – ВС) у даному правовому полі. Відповідно до Постанови ВС від 08.02.2019 №855/17/19 [19] було відмовлено у задоволенні апеляційної скарги кандидата на пост Президента України Гриценка А. С. до Центральної виборчої комісії про визнання протиправними дій стосовно надання електронної копії бази даних Реєстру з можливістю доступу лише в приміщенні та з обладнанням Центральної виборчої комісії. Суд дійшов висновку, що надання позивачу електронної копії бази даних Реєстру разом із програмним забезпеченням для перегляду цієї копії у неконтрольованому і незахищеному просторі, поза межами приміщення Центральної виборчої комісії, унеможливлюють забезпечення нею як розпорядником Реєстру законності і пріоритетності прав людини, а також захищеності її відомостей, а отже призведе до порушення Конституції України, законів та міжнародних нормативних актів у цій сфері.

Розглядаючи міжнародний досвід у даній сфері, слід зазначити, що відносини, пов'язані з використання інформації в мережі Інтернет, регулюються багатьма міжнародно-правовими актами, що досі не є ратифікованими Україною. Вважаємо, що серед них важливими є зокрема:

Окінавська хартія глобального інформаційного суспільства від 22.07.2000 (далі – Окінавська хартія) [7], Конвенція ООН про використання електронних повідомлень у міжнародних договорах від 23.11.2005 [4], Декларація принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті» від 12.12.2003 [2] та інші.

Вважаємо, бажаним і корисним для вітчизняного нормативного регулювання досліджуваного питання є ратифікація зазначених міжнародно-правових актів Україною.

Варто також підкреслити, що серед вказаних вище нормативно-правових актів важливу роль відіграє Окінавська хартія. Вона містить положення про те, що всі люди всюди, без винятку, повинні мати можливість користуватися перевагами глобального інформаційного суспільства. Саме ж інформаційне суспільство ґрунтується на стимулюючих розвиток людини демократичних цінностях, таких як вільний обмін інформацією та знаннями, взаємна терпимість і повага до особливостей інших людей. Хартія покликана ліквідувати прогалини у правовій, технологічній та інформаційній галузях знань [7, с. 26].

Як відомо, Україна є асоційованим членом Європейського Союзу, тож цікавим видається аналіз правового регулювання предмету дослідження в цьому інтеграційному об’єднанні.

Інститут захисту персональних даних в праві ЄС ґрунтується на принципах законності, цільової визначеності, мінімальності, конкретності та об’єктивності інформації, участі суб’єкта персональних даних у здійсненні контролю, обмеження розкриття персональних даних, інформаційної безпеки. Ці принципи мають нормативну силу та є підґрунтям для створення нових правових норм у даній сфері правовідносин, вони обов’язкові для уповноважених органів у процесі правозастосовної практики. Законодавство ЄС про захист персональних даних охоплює весь спектр правових норм, у тому числі норми-дефініції, уповноважуючі та забороняючі норми.

Слід згадати, що 28 січня 1981 року Радою Європи була прийнята Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (далі – Конвенція), згадувана вище Конвенція 108 [5]. Цей документ спрямований на об'єднання країн світу для визначення основних вимог до передачі індивідуальної інформації про людину у всесвітньому електронному просторі, тобто створення низки правил, які стають обов'язковими при обробці персональних даних.

Першими країнами, які приєдналися до Конвенції 108, були Франція, Швеція, Німеччина, Іспанія та Норвегія. Вже у 2000 році рішення про приєднання прийняли більше двадцяти країн [**Ошибка! Источник ссылки не найден.**26, с.81]. Україна ратифікувала Конвенцію у 2010 році з прийняттям Закону України «Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних» від 06.07.2010 № 2438 [14]. Гадаємо, імплементація норм вказаної конвенції позитивно вплинула на розвиток національного законодавства з досліджуваного питання. Зокрема, наприклад, це виражено у відповідності ряду обов'язкових при обробці персональних даних правил із стандартами ЄС, визначеними в згаданій конвенції, ратифікованій Україною.

Також, вважаємо позитивним впливом те, що наслідком ратифікації вказаної конвенції і з метою забезпечення незалежності уповноваженого органу з питань захисту персональних даних повноваження щодо контролю за додержанням законодавства про захист персональних даних покладено на Уповноваженого Верховної Ради України з прав людини, як того і вимагає конвенція [58].

Отже, національне законодавство щодо захисту персональних даних складається з більше ніж 20 нормативно-правових актів, які, з огляду на практику їх використання, потребують вдосконалення.

На нашу думку, у першу чергу слід внести зміни до визначення персональних даних, зазначеного у Законі №2297, яке у сучасних реаліях не охоплює різноманітність проблемних правовідносин у сфері захисту персональних даних.

У свою чергу недосконаліть визначення поняття «персональні дані» тягне за собою неможливість в повній мірі врегулювати проблеми визначення відповідальності за порушення в даній сфері. З огляду на вищевказані питання пропонуємо внести доповнення до Закону № 3454 зокрема щодо уніфікації формулювання та поширення відповідальності за порушення не лише недоторканності приватного життя, але й інших пов'язаних аспектів використання персональних даних.

З іншого боку, гадаємо, що важливим для врегулювання є питання захисту людини як індивіда в кіберпросторі, як одного з найбільш вразливих суб'єктів інформаційного середовища, а також визначення основних аспектів захисту персональних даних особи в мережі Інтернет. У зв'язку з цим, вважаємо, що доречним було б внести відповідні зміни та доповнення до Закону № 2469.

Вдосконалюючи вітчизняне законодавство, слід опиратися на міжнародно-правовий досвід, зокрема на нормативно-правову базу актів ЄС. На жаль, в деяких аспектах національне законодавство з досліджуваного питання не корелюється з європейським та міжнародно-правовим досягненнями в цій сфері.

Актуальним завданням для України є приведення національного законодавства у відповідність з міжнародними стандартами, а також ратифікувати нові міжнародні нормативно-правові акти, що регулюють вказане питання. Зокрема, на нашу думку, серед них варто виділити Окінавську хартію глобального інформаційного суспільства від 22.07.2000, що покликана ліквідувати прогалини у правовій, технологічній та інформаційній галузях знань.

Окрім вдосконалення національного правового регулювання захисту персональних даних в мережі Інтернет, враховуючи досвід Європейського Союзу та інші міжнародно-правові акти, існує необхідність доопрацювання процедур обробки персональних даних з використанням веб-ресурсів. Актуальними для вдосконалення даного питання, на нашу думку, є проблема надання безвідкличної чи безстрокової згоди на обробку персональних даних. Слід також звернути особливу увагу на забезпечення безпеки передачі персональних даних невстановленим третім особам та механізм їх модернізації.

Гадаємо, що зміни вітчизняного законодавства із врахуванням міжнародного досвіду (зокрема ЄС), позитивно вплинуть на захист персональних даних в мережі Інтернет у нашій державі.

# РОЗДІЛ 2
# МЕХАНІЗМ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В МЕРЕЖІ ІНТЕРНЕТ

## 2.1. Підстави виникнення прав на захист персональних даних в мережі Інтернет

Стрімкий розвиток інформаційно-комунікаційних технологій потребує розроблення та впровадження адекватних захисних механізмів, спроможних реально захистити персональні права та свободи власників особистих даних. Незважаючи на значну увагу з боку суспільства та держави до питання захищеності персональних даних від втручання та потенційного оприлюднення сторонніми особами, в сучасних умовах воно й досі залишається відкритим.

Підставою виникнення права на захист персональних даних, є порушення особистих немайнових прав суб'єкта персональних даних. До діянь, які становлять зміст відповідного правопорушення, переважно належать вчинки у процесі обробки володільцем чи розпорядником персональних даних, всупереч приписам законодавства [32, с.92]. Такі діяння проявляються в незаконному зборі, використанні й поширенні інформації персонального характеру.

Збирання персональних даних є складовою процесу їх обробки, що передбачає дії з підбору чи впорядкування відомостей про фізичну особу.

Суб'єкт персональних даних повідомляється про володільця персональних даних, склад та зміст зібраних персональних даних, свої права, визначені Законом № 2297, мету збору персональних даних та осіб, яким передаються його персональні дані:

1) в момент збору персональних даних, якщо персональні дані збираються у суб'єкта персональних даних;

2) в інших випадках протягом тридцяти робочих днів з дня збору персональних даних.

Використання персональних даних передбачає будь-які дії володільця щодо обробки цих даних, дії щодо їх захисту, а також дії щодо надання часткового або повного права обробки персональних даних іншим суб'єктам відносин, пов'язаних із персональними даними, що здійснюються за згодою суб'єкта персональних даних чи відповідно до закону. Використання персональних даних володільцем здійснюється у разі створення ним умов для захисту цих даних. Володільцю забороняється розголошувати відомості стосовно суб'єктів персональних даних, доступ до персональних даних яких надається іншим суб'єктам відносин, пов'язаних з такими даними. Використання персональних даних працівниками суб'єктів відносин, пов'язаних з персональними даними, повинно здійснюватися лише відповідно до їхніх професійних чи службових або трудових обов'язків. Ці працівники зобов'язані не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, крім випадків, передбачених законом. Таке зобов'язання чинне після припинення ними діяльності, пов'язаної з персональними даними, крім випадків, установлених законом.

Поширення персональних даних передбачає дії щодо передачі відомостей про фізичну особу 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 (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини. Виконання вимог встановленого режиму захисту персональних даних забезпечує сторона, що поширює ці дані. Сторона, якій

передаються персональні дані, повинна попередньо вжити заходів щодо забезпечення вимог закону.

Існує багато служб у мережі Інтернет, які відстежують та використовують персональні дані користувача. Наприклад, Google Maps відстежує місце розташування користувача в режимі реально часу та хронологію його пересування. Інший сервіс під назвою Glancee від Facebook може відстежувати місцеперебування конкретного користувача у пасивному режимі. Тобто, цей сервіс може показувати користувачу, де знаходяться його «друзі», а також показує користувачів мережі зі схожими інтересами поблизу користувача. На відміну від Google Maps, Glancee не вимагає реєстрації і працює у «тіні», проводячи моніторинг даних геолокації. Маркетологи рекламують цей сервіс, як «спосіб виявити навколо себе приховані зв'язки», але насправді це сервіс, який збирає персональні дані користувачів і використовує у своїх комерційних цілях.

Веб-сайти та Інтернет служби, які не мають нової та надійної системи безпеки, можуть залишити інформацію, яка містить персональні дані користувача, і дані, що передаються між комп'ютером користувача і веб-сервером на ризик від хакерів. Наприклад, веб-сайти, які використовують застарілий стандарт HTTP для веб-комунікації, а не більш надійний HTTPS, позбавлені зашифрованого з'єднання між комп'ютером або смартфоном та веб-сайтом, до якого він підключений. Це означає, що дані, що існують між двома точками, можуть контролюватися іншими компаніями або потенційно підхоплені та викрадені хакерами для більш небезпечних цілей. Сучасні Smart телевізори, холодильники із системою оновлення через мережу Інтернет, навушники з підтримкою Wi-Fi також можуть становити загрозу витоку персональних даних. Відсутність стандартів безпеки в Інтернеті, речі, колективне ім'я, пов'язане із підключеними та інтелектуальними пристроями означає, що деякі пристрої можуть не мати зашифрованих з'єднань із серверами, які керують їхніми розумними функціями, або можуть бути

вразливими до простих методів злому, що перетворює їх на мішені для кіберзлочинців. Використання громадських точок доступу до мережі Інтернет через Wi-Fi також може бути загрозою викрадення персональних даних користувача. Проблема полягає в тому, що вони часто мають слабку систему захисту або взагалі може бути відсутня система безпеки чи шифрування, а це означає, що хакери можуть перехоплювати персональні дані, що передаються між пристроєм користувача і точкою доступу до мережі Інтернет. Деякі точки доступу мають веб-портал, який вимагає надати електронну пошту або ввійти через Facebook або Twitter, тобто користувач повинен надати певні персональні дані.

Дослідження 45-ти соціальних мереж, проведене організацією Physorg у 2009 р., виявило «значну тривогу» самих учасників, так і з боку захисту персональних даних. Близько 90% сайтів, наприклад, для надання дозволу приєднатися до них необґрунтовано вимагають вказувати прізвище, ім'я або дату. 85% веб-сайтів не можуть використовувати стандартні протоколи шифрування для захисту даних користувачів від атак кіберзлочинців. 72% сайтів у своїй політиці залишають за собою право на передачу даних про користувачів стороннім особам [74].

У соціальних мереж є технічні можливості відслідковувати інформацію про своїх користувачів, їх активність у мережі Інтернет незалежно від того, чи перебувають вони в соціальній мережі, тобто після виходу зі сторінок соціальної мережі, а також про користувачів мережі Інтернет, які взагалі не мають аккаунта в соціальній мережі, шляхом створення профілів незареєстрованих користувачів [25].

Усе ж таки значну частину персональних даних користувачі соціальних мереж повідомляють добровільно. Соціальні сервіси передбачають розміщення в Інтернеті відомостей, які так чи інакше (через реєстраційні дані, особливості поведінки у віртуальному просторі) дозволяють ідентифікувати особу користувача. Зокрема, більшість соціальних мереж

передбачає розміщення на персональній сторінці прізвища та ім'я, дати народження, статі, місця народження (проживання), місця навчання/роботи, посади, інформації про сімейне становище, відомостей про батьків, братів/сестер, дітей тощо [41]. Після введення загальних відомостей у ході змістового наповнення відповідної сторінки можуть додаватися дані про факти зі свого особистого життя, рід занять, захоплення, національність, віросповідання, світлини, номер ICQ, Skype-ідентифікатор, партійну належність, коло друзів, колег, ділових партнерів тощо. Здебільшого акаунт користувача містить різні статистичні характеристики його перебування в системі: дату, час і тривалість останнього входу та перебування в системі, адреси, використані при підключенні комп'ютера тощо. Світлини, завантажені через смартфон із вбудованим GPS-модулем, містять точний час і GPS-координати місця, в якому було зроблено фото, а спеціальні сервіси дозволять визначити, яким саме пристроєм ви фотографували та чи було відредаговано зображення у редакторі Photoshop [65, с.207].

Поширення персональних даних через соціальну мережу відбувається значно швидше, ніж у реальному житті. Шкідливими для користувача є ті випадки, коли персональні дані потрапляють до людей, яким це зовсім не призначено. Часто користувачам соціальних мереж взагалі не відомо, що вони можуть змінити персональні параметри конфіденційності, і якщо цього не зроблять, то їхні персональні дані будуть відкриті іншим користувачам. На сьогодні, вже існує багато випадків негативних наслідків зайвої відвертості у соціальних мережах, як-от : звільнення з роботи, розголошення інтимних подробиць життя, крадіжка фінансів та інше [44, с.328].

Найчастіше виявляються такі типові порушення законодавства з питань захисту персональних даних при їх обробці з використанням веб-ресурсів:

1) у момент збору персональних даних суб'єкт персональних даних не повідомляється про володільця персональних даних (найменування юридичної особи-володільця та її адресу), склад та зміст зібраних

персональних даних, свої права, мету збору персональних даних та осіб, яким передаються його персональні дані;

2) зміст персональних даних є явно надмірним відповідно до визначеної мети обробки персональних даних;

3) процедури обробки персональних даних є визначені на сайті, але не є визначені розпорядчими документами володільця, як це передбачено законодавством [57, с.79].

Отже, аналізуючи підстави виникнення права на захист персональних даних, слід перш за все вказати на порушення особистих немайнових прав суб'єкта персональних даних. Зміст відповідного правопорушення становлять переважно діяння, вчинені у процесі обробки володільцем чи розпорядником персональних даних, всупереч приписам законодавства. Вони переважно проявляються в незаконному зборі, використанні й поширенні інформації персонального характеру.

## 2.2. Форми та способи захисту персональних даних в мережі Інтернет

Як зазначається у п. 8 ч. 2 ст. 8 Закону № 2297, суб'єкт персональних даних має право звертатися із скаргами на обробку своїх персональних даних до Уповноваженого Верховної Ради України з прав людини (далі – Уповноважений) або до суду [11].

Правовий статус Уповноваженого визначено Законом України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» № 383 від 03.07.2013 (далі Закон № 383), який набув чинності 1 січня 2014 року. Законом № 383 Уповноважений визначений як орган контролю за додержанням законодавства про захист персональних даних, створений з метою забезпечення незалежності в

регулюванні питань захисту персональних даних, як того вимагає Конвенція 108 [5].

Уповноважений має такі повноваження у сфері захисту персональних даних:

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 невиїзні, 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 [11].

Одним із пріоритетних напрямів діяльності Уповноваженого у сфері захисту персональних даних залишається просвітницька та роз'яснювальна

діяльність. Фахівцями з питань захисту персональних даних Секретаріату Уповноваженого регулярно проводяться навчальні заходи (семінари, лекції, тренінги) для професійних і цільових груп, надаються рекомендації та роз'яснення з питань практичного застосування положень законодавства у сфері захисту персональних даних. Зокрема, протягом 2019 року за зверненнями суб'єктів персональних даних, а також володільців і розпорядників персональних даних надавались рекомендації щодо практичного застосування законодавства про захист персональних даних стосовно об'єктів захисту, загальних та особливих вимог до обробки персональних даних, прав суб'єктів персональних даних, обов'язків володільців та розпорядників персональних даних, повідомлень про обробку персональних даних, підстав для обробки персональних даних, порядку доступу до персональних даних тощо [**Ошибка! Источник ссылки не найден.**69].

Зазначимо, що практично в усіх державах-членах Ради Європи та Євросоюзу створені національні органи: Уповноважені з питань приватності (права на недоторканність приватного життя) або спеціальні комісії (агентства) із захисту персональних даних, які здійснюють моніторинг застосування та забезпечення дотримання законодавства про захист персональних даних у межах своїх територій. Кілька держав-членів (наприклад, Австрія, Нідерланди) створили орган із захисту даних із загальною компетенцією і кілька наглядових органів в інших галузях (наприклад, у галузі охорони здоров'я або телекомунікацій). У країнах, що мають федеративний устрій або суттєві повноваження на регіональному рівні (наприклад, Німеччина, Іспанія), існують поряд із національним наглядовим органом субрегіональні органи, на які покладено ті самі функції, що й на регіональному або федеральному рівнях. Нагадаємо, що в деяких країнах, наприклад, Румунії, до створення національних органів із захисту персональних даних обов'язок контролювати дотримання права на

недоторканність приватного життя було покладено на інститут омбудсмена, а в деяких державах-членах, наприклад, Фінляндія, омбудсмен, як і раніше, підтримує відповідну функцію щодо захисту персональних даних. Цим органам і омбудсмену у відповідних країнах надано суттєві повноваження: уряд має консультуватися з ними при розробці законодавства, пов'язаного з обробкою інформації персонального характеру, вони також мають право проводити розслідування і отримувати доступ до інформації, що стосується їхнього розслідування, вимагати знищення інформації або забороняти її обробку, звертатися до суду з позовами, розглядати скарги і вимагати звіти від посадових осіб. На них покладено функції щодо правової освіти населення та підтримання міжнародних зв'язків у галузі захисту і передачі даних. Органи влади, що є операторами баз даних, отримують відповідні ліцензії у уповноважених з питань прайвесі та захисту даних [60, с. 282].

У Великій Британії діє інститут Уповноваженого з питань захисту персональних даних, який функціонує відповідно до Закону «Про захист даних» від 12 липня 1984 р. Цей Закон визначив посади Міністра із захисту даних, Реєстратора із захисту даних і створив Суд із захисту даних. Будь-яка особа вправі звернутися з апеляцією до Суду із захисту даних у разі відмови Реєстратора розглянути скаргу про порушення законодавства [42, с. 61].

Канадський Уповноважений із захисту даних (Комісар з конфіденційності (PIPEDA) несе відповідальність за дотримання інформаційних прав людини, закріплених у законодавстві, а також за дотримання своїх обов'язків операторами даних. До його повноважень належить: розслідування скарг, проведення перевірок та подача судових позовів у рамках двох федеральних законів; інформування громадськості про практику поводження державних і приватних організацій з персональними даними; підтримка, проведення та публікація результатів досліджень з питань прайвесі; підвищення обізнаності громадськості та розуміння існуючих проблем щодо інформаційного прайвесі; проведення освітніх

семінарів та практикумів [60, с. 283-286]. На рівні канадських провінцій є незалежні Комісаріати з питань конфіденційності, які відповідають в першу чергу за дотримання законів про захист персональних даних.

Також у багатьох державах-членах Ради Європи та ЄС створені колегіальні органи нагляду (контролю) за діяльністю Уповноваженого органу, що мають назву – комісія, колегія чи рада із захисту даних [49, с. 16]. Це спеціальний орган для розгляду певних категорії справ у сфері персональних даних. За Законом Швейцарії, на Федерального Уповноваженого із захисту даних покладаються функції з ведення реєстру баз даних, нагляду за дотриманням правил поводження з даними, захисту прав суб'єктів даних. У разі встановлення порушень він ухвалює відповідні рекомендації. Однак у разі їх невиконання, Уповноважений може звернутися до Федеральної комісії з захисту персональних даних, яка виносить рішення, що має силу судового [48, с. 24].

Відповідно до правил нового порядку захисту персональних даних у державах – членах ЄС (Глава VI Регламенту (ЄС) 2016/679 від 27 квітня 2016 р.), кожна держава-член повинна мати незалежний контролюючий орган (SA) для розслідування скарг, застосування санкцій з правопорушень, співробітництва з іншими SA, забезпечення взаємної допомоги та організації спільних операцій щодо захисту персональних даних [28, с. 55].

Окрім національних органів, у самій Раді Європи діють Уповноважений з прав людини, який призначається та звітує перед Європейською Комісією з прав людини, та Комісар із захисту персональних даних (Уповноважений з питань захисту персональних даних), який призначається та звітує перед Парламентською Асамблеєю Ради Європи. Комісар із захисту персональних даних, з відповідною організаційною структурою (органом контролю), має вирішувати всі питання щодо захисту персональних даних. Керівники вказаних інститутів РЄ підпорядковуються Генеральному секретарю Ради Європи [49, с. 43].

Звертаючись до українських реалій, зазначимо, що вітчизняний досвід створення спеціальної інституційної структури, на яку покладено обов'язок контролю над законністю операцій з персональними даними та здійснення захисту прав їх суб'єктів, багато в чому схожий з європейським. Одразу ж після набрання чинності Законом № 2297 було створено Державну службу України з питань захисту персональних даних (далі – ДСПЗПД). Проте основною критичною характеристикою статусу Уповноваженого органу, що виділялася, є його «залежність» від інших владних структур у силу його входження в систему виконавчої влади України [56, с. 624]. Водночас цей механізм був вкрай неефективним, та й взагалі невиправданим. Так, за час існування процедури реєстрації баз персональних даних до ДСЗПД з кінця 2011 року надійшло близько 1 412 000 заяв про реєстрацію баз персональних даних. З них службою з кінця 2011 до середини 2013 року було зареєстровано близько 70 000. Відтак, процедура реєстрації не виправдала свого існування[42, с. 82].

Враховуючи досвід функціонування системи захисту персональних даних в Україні, 3 липня 2013 р. Верховна Рада України прийняла Закон України № 383 «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних», який набув чинності 1 січня 2014 року. Цим Законом скасовувалася процедура реєстрації баз даних, замість неї вводилася процедура повідомлення про такі бази, і лише в якщо вони охоплюють чутливі персональні дані, а функції із контролю за дотримання законодавства у цій сфері покладено на Уповноваженого Верховної Ради України з прав людини. З метою забезпечення виконання функцій контролю за виконанням законодавства в сфері захисту персональних даних у Секретаріаті Уповноваженого Верхової Ради України з прав людини створено Департамент з питань захисту персональних даних [38, с.180-181].

Під час проходження практики в ТОВ «Спанта» консультувалася з одним з керівників цієї компанії, адвокатом з 15-річним досвідом, щодо того який з способів захисту даних він вважає найбільш дієвим. Цікавою видавалась відповідь, по-перше тому, що на практиці мало хто з пересічних громадян здатен розпізнати порушення у використанні власних персональних даних. Можливо, через це звернень до адвокатів з цього приводу, принаймні у практиці ТОВ «Спанта» було дуже мало. Усе ж, грунтуючись на знаннях та власному досвіді, пан адвокат вважає, що більш дієвим механізмом захисту порушених прав у цьому випадку буде звернення до суду. Як показує практика, більш багатий досвід вирішення подібних справ має ЄСПЛ, ніж національні суди, можливо, з огляду на наявність розвинутої нормативно-правової бази (право ЄС)

Що ж стосується судового захисту персональних даних в Україні, то згадка про Закон № 2297 міститься у судових рішеннях з цивільних, кримінальних, господарських, адміністративних справ та справ про адміністративні правопорушення.

Зокрема, з метою захисту порушених прав персональних даних суб'єкт персональних даних може звернутися до суду в порядку позовного провадження у рамках цивільного судочинства. Так, у справі № 753/18972/16ц в жовтні 2016 р. позивач звернувся до суду з позовом до Громадської організації «Наші гроші» (далі - ГО «Наші гроші», відповідач 1) про заборону розповсюджувати відомості щодо позивача, зобов'язання видалити зі статті, розміщеної на офіційному сайті Громадської організації «Наші гроші», інформацію, яка дає можливість ідентифікувати позивача та відшкодування моральної шкоди в розмірі 77 140 грн.

Позов обґрунтований тим, що публікуючи відомості, які дають можливість ідентифікувати особу позивача, відповідач порушив особисті немайнові права позивача, зокрема право на використання імені, та незаконно розголосив відомості досудового розслідування. Публікацією

вищевказаної статті, яка була процитована усіма відомими інформаційними ресурсами і має понад 2 млн. переглядів, було завдано непоправної шкоди професійній та діловій репутації позивача, з подачі журналістів громадської організації вона зазнала суспільної ізоляції, утисків також зазнають члени її родини.

На стадії підготовчого провадження сторона позивача доповнила позов вимогами до власника веб-сайта (далі – відповідач про заборону розповсюджувати відомості щодо позивача), зобов'язання видалити з вищевказаної статті інформацію, яка дає можливість ідентифікувати позивача, та відшкодування моральної шкоди. Одночасно позивач відмовився від вимог до ГО «Наші гроші» про відшкодування моральної шкоди.

Суд у цій справі вирішив позов задовольнити частково. Зокрема, судом було прийнято рішення зобов'язати Громадську організацію «Наші гроші» протягом п'ятнадцяти календарних днів з дня набрання рішенням суду законної сили видалити зі статті, розміщеної на офіційному сайті Громадської організації «Наші гроші», інформацію, яка дає можливість ідентифікувати позивача, а також стягнути з відповідача на користь позивача 77 140 грн. на відшкодування моральної шкоди та 11 075,20 грн. судових витрат, а усього 88 215 гривень 20 копійок [24].

Уваги заслуговує також справа № 753/15830/18 у якій позивач, звернувся до суду з позовом до відповідача про зобов'язання вчинити дії, в якому просить зобов'язати головного редактора Інтернет-порталу видалити з веб-сайту персональні дані, у томі числі фотографії його та його дружини.

Позовні вимоги обґрунтовані тим, що на веб-порталі, головним редактором якого є відповідач було розміщено ряд публікацій, які містять персональні дані та фотографії із зображенням позивача та його дружини, які не давали згоди на їх публікацію.

06.08.2018 р. представник позивача надіслав відповідачу вимоги про видалення персональних даних позивача та його дружини, а також зазначено про ненадання дозволу на опрацювання персональних даних позивача та його дружини.

Як зазначає позивач, станом на день написання позовної заяви такі публікації та фотографії не видалені та залишаються розміщеними на веб-сайті. Таким чином, позивач вважає, що відповідач порушує особисті немайнові права Позивача.

Так як у вимогах про видалення персональних даних позивача, отриманих відповідачем не надано згоди на опрацювання персональних даних позивача та його дружини, а відповідач в порушення діючого законодавства продовжує розміщувати зазначені публікації та фотографії, для захисту порушеного права позивач звернувся до суду з цим позовом.

Всебічно проаналізувавши обставини справи в їх сукупності, оцінивши за своїм внутрішнім переконанням, що ґрунтується на повному і об'єктивному розгляді справи, зібрані по справі докази, керуючись законом, суд дійшов до висновку, що позов підлягає задоволенню [23].

Відповідно до права РЄ порушення прав на захист персональних даних, які, як стверджується, були допущені на національному рівні Договірних Сторін ЄКПЛ та водночас становлять порушення статті 8 ЄКПЛ, можуть також бути оскаржені в ЄСПЛ після вичерпання усіх доступних національних засобів пра-вового захисту. Заява до ЄСПЛ про порушення статті 8 ЄКПЛ також повинна відповідати іншим критеріям прийнятності (статті 34–37 ЄКПЛ). Хоча заяви до ЄСПЛ подаються лише проти Договірних Сторін, вони можуть також опосередковано стосуватися дій чи бездіяльності сторін-приватних осіб, з огляду на те, що Договірна Сторона не виконала свої позитивні зобов'язання за ЄКПЛ та не забезпечила у своєму національному законодавстві достатній рівень захисту від порушень прав на захист персональних даних. Наприклад, у справі «К.Ю. проти Фінляндії»

неповнолітній заявник скаржився, що на Інтернет-сайті знайомств про нього було розміщено оголошення сексуального характеру. Постачальник послуг не розкрив йому відомості про особу, яка розмістила цю інформацію, через свої зобов'язання дотримуватися конфіденційності, накладені на нього законодавством Фінляндії. Заявник стверджував, що законодавство Фінляндії не надавало достатній рівень захисту від таких дій приватної особи, яка розмістила в Інтернеті компромат про заявника. ЄСПЛ постановив, що держави не тільки мають утримуватися від довільного втручання в персональне життя осіб, але й можуть бути суб'єктами позитивних зобов'язань, які включають в себе «вжиття заходів, призначених гарантувати повагу до приватного життя навіть у сфері міжособистісних відносин». У справі заявника, його практичний й ефективний захист потребував здійснення ефективних кроків для виявлення порушника і притягнення його до відповідальності. Проте держава не надала такого захисту, і Суд дійшов висновку, що мало місце порушення статті 8 ЄКПЛ.

Класичним питанням для ЄСПЛ є питання співвідношення права на свободу слова та права на приватність, а саме – що має переважати у кожному конкретному випадку: можливість для медіа публікувати свої матеріали чи право особи вимагати нерозповсюдження інформації про себе. В останніх справах цієї тематики, які стосувались діяльності вже не друкованих, а онлайн медіа, ЄСПЛ підтвердив свої попередні висновки, відповідно до яких при вирішенні цього питання необхідно враховувати такі критерії:

- внесок матеріалу у публічну (суспільну) дискусію (наприклад, якщо публікація стосується політичних питань або злочинів);

- статус особи (ким вона є – приватним індивідом, чи публічною фігурою (особою);

- метод отримання інформації (добросовісність, авторитетність джерел інформації);

- попередня поведінка особи, про яку йшлося (наприклад, надання нею коментарів);

- наслідки публікації.

Так, у 2017 році у справі Fuchsmann проти Німеччини [71] суд встановив відсутність порушення права на приватність німецького бізнесмена, про якого Нью-Йорк Таймс опублікувало статтю зі звинуваченнями у можливих зв'язках з кримінальним світом. Стаття було поширена в друкованій та онлайн версії видання, а також доступна у результатах пошукових систем. Суд встановив, що можлива причетність до кримінального світу німецького бізнесмена становить суспільний інтерес, а він сам в силу наявності бізнесу в медіа секторі і його міжнародної активності може вважатись публічною особою. Крім того, журналісти до нього звертались, і він мав змогу прокоментувати матеріал, що готувався до публікації.

У 2018 році Суд застосував ці ж критерії, розглядаючи питання про можливість видалення із веб-сайту радіоорганізації персональної інформації з матеріалів про скоєне багато років тому вбивство та подальше ув'язнення особи (справа M.L. та W.W проти Німеччини [72]). Суд зазначив, що в інтересах суспільства бути проінформованим не лише про поточні події, але й мати можливість шукати інформацію про минулі. Включення персональної інформації в новинні матеріали сприяло публічній дискусії, і з часом не втратило своєї актуальності. Суд відзначив, що заявники не були приватними особами, вони стали відомими в результаті судового розгляду і сприяли своїй пізнаваності, подаючи запити про перегляд справи, звертаючись до преси та закликаючи журналістів інформувати громадськість. Таким чином, сподівання заявників забезпечити анонімність звітів або навіть реалізувати право бути забутим в Інтернеті були дуже обмеженими. Крім того, суд врахував, що спірні матеріали не були доступні на сторінках новин на веб-сайтах, і на них застосовувались обмеження, такі як платний доступ або

підписка, як наслідок, публікації не були відомі користувачам Інтернету, якщо вони спеціально не шукали прізвища заявників, а також заявники не робили спроб зв'язатися з операторами пошукових систем з метою ускладнення відстеження інформації про них.

З кожним днем збільшується кількість справ, пов'язаних з втручанням держави у приватність своїх громадян. Не оспорюючи можливість такого втручання, ЄСПЛ неодноразово розглядав питання дотримання державами умов ст. 8 Конвенції 108, а саме: здійснення такого втручання у відповідності до закону, його необхідність у демократичному суспільстві та законна ціль: інтереси національної та громадської безпеки чи економічного добробуту країни, запобігання заворушенням чи злочинам, захист здоров'я чи моралі або для захисту прав і свобод інших осіб. Так, у справі Бенедік проти Словаччини [73] у 2018 році Суд вкотре наголосив, що закон, який є підставою втручання у приватність, має бути чітким і пропонувати достатні гарантії від зловживань посадовими особами під час процедури доступу та передачі персональних даних. Суть справи полягала у тому, що правоохоронні органи, розслідуючи справу про розповсюдження дитячої порнографії, без судового ордеру отримали від провайдера інформацію, яка ідентифікувала власника динамічної IP-адреси. Одним з ключових питань для Суду у цій справі стало питання чи міг заявник, користуючись всесвітньої мережею, обґрунтовано розраховувати на анонімність та чи в достатній мірі національне законодавство захищало його приватність від втручання. Суд наголосив, що заявник не міг обґрунтовано очікувати збереження його динамічної IP-адреси в таємниці, але він міг обґрунтовано очікувати конфіденційності стосовно його особистості. Зокрема тому, що присвоєну динамічну IP-адресу, навіть якщо її могли бачити інші користувачі мережі, неможливо було простежити до певного комп'ютера без перевірки даних провайдерів на підставі запиту поліції. Встановивши порушення, суд зазначив, що у відповідний час не існувало жодних правил, які б визначали

умови для збереження отриманих у ході розслідування даних, а також жодних гарантій від зловживань посадових осіб під час процедури доступу та передачі таких даних, а отже – законодавство було, принаймні, не когерентним щодо рівня захисту інтересів заявника в конфіденційності.

У 2014 р. Суд Європейського Союзу виніс рішення, яким право бути забутим було затверджене. Це викликало неабиякі зміни у юридичній практиці держав-членів ЄС та дискусії щодо відповідного права по всьому світу. Відправною точкою справи було звернення іспанського громадянина Маріо Костехи Гонсалеса, який поскаржився на оголошення у газеті (електронна версія видання містилася на сайті), що були опубліковані в 1998 році, але все ще були доступні в Інтернеті. Вони стосувалися банкрутства та аукціону нерухомості, щодо продажу його будинку за борги. Пошуки Google за його іменем приводили до посилань на ці сторінки. Маріо Костеха хотів, щоб їх було видалено, оскільки його борги давно були погашені, і ця інформація була неактуальною і не відображала той стан справ, яким він є сьогодні, що шкодило його репутації [75].

Пан Костеха вимагав від газети видалити або змінити відповідні сторінки таким чином, щоб його персональні дані більше не відображалися. Він також допускав можливість використання газетами певних інструментів для запобігання відображенню його даних у результатах пошукових систем. «La Vanguardia» відмовила в задоволенні його вимог. Після цього пан Костеха направив компанії Google вимогу видалити статті з результатів пошуку. Оскільки компанія Google також не задовольнила його вимоги, адвокати Костехи подали скаргу до Іспанського агентства захисту персональних даних (AEPD). 30 липня 2012 року Агентство AEPD наказало Google Spain та Google Inc задовольнити вимоги пана Костехи. Компанія Google подала апеляцію на адміністративне рішення до іспанського суду - Audiencia Nacional, який у свою чергу припинив провадження й направив

його до Суду Європейського Союзу для отримання попереднього рішення [76].

Європейський суд постановив, що з метою забезпечення прав, передбачених у згаданих положеннях Директиви 108, «оператор пошукової системи зобов'язаний видалити зі списку результатів, виданих у відповідь на пошуковий запит на основі імені особи, посилання на веб-сторінки, розміщені третіми особами, що містять інформацію про цю 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» [75]

Як бачимо, наразі Уповноважений та суди є єдиними інституціями, які здійснюють контроль за додержанням законодавства про захист персональних даних. Проте цього недостатньо. З огляду на це, на нашу думку, цілком слушним є створення не лише спеціального незалежного наглядового органу із захисту персональних даних, а навіть цілої системи таких органів, що могли б охопити різні аспекти проблемних питань.

З огляду на вказане, доцільно було б удосконалити законодавство про захист персональних даних з метою приведення його у відповідність з Регламентом (ЄС) 2016/679. Зокрема: створити систему незалежних наглядових органів із захисту персональних даних; зобов'язати компанії отримувати чітку згоду користувачів на обробку даних; зобов'язати компанії призначити особу відповідальну за захист персональних даних, а також забезпечувати безпеку персональних даних (шифрування, псевдонімізація тощо); надати користувачу право «стирання» даних, якщо у них немає необхідності, користувач відкликає згоду на їх обробку, відсутній легітимний інтерес, або їх обробку здійснено незаконно; надати регулятору повноваження штрафувати компанії за порушення [52].

Отже, суб'єкт персональних даних має право звертатися із скаргами на обробку своїх персональних даних до Уповноваженого Верховної Ради

України з прав людини або до суду. Уповноважений діє як орган контролю за додержанням законодавства про захист персональних даних, створений з метою забезпечення незалежності в регулюванні питань захисту персональних даних.

## ВИСНОВКИ ТА ПРОПОЗИЦІЇ

Отже, здійснене магістерське дослідження дало можливість на основі чинного законодавства України, узагальнення практики його реалізації, а також міжнародного досвіду визначити особливості захисту персональних даних в мережі Інтернет.

Найважливіші наукові та практичні результати одержані в магістерській роботі полягають у наступному:

1. Права суб'єкта персональних даних варто розуміти як права фізичної особи, якій належать персональні дані, що обробляються, або її представників, які від імені цієї особи надають згоду на таку обробку та здійснюють інші права щодо захисту персональних даних.
2. Суб'єкт персональних даних має право: 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;

отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані; на доступ до своїх персональних даних; 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; пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних; 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; 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; звертатися із скаргами на обробку своїх персональних даних до Уповноваженого або до суду; застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних; вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди; відкликати згоду на обробку персональних даних; знати механізм автоматичної обробки персональних даних; на захист від автоматизованого рішення, яке має для нього правові наслідки.

3. До принципів обробки персональних даних відносяться: принцип законності обробки; принцип конкретизації цілей та обмеження; принципи якості персональних даних, що включає принцип відповідності даних, принцип точності даних, принцип збереження

даних протягом обмеженого періоду, принцип ретельності обробки, що включає прозорість, формування довіри; принцип підзвітності.

4. Під охороною персональних даних розуміти сукупність засобів, методів та способів, що спрямовані на гарантування особистих немайнових прав на персональні дані, а під захистом державно-примусову діяльність спеціальних органів державної влади, спрямовану на поновлення порушених особистих немайнових прав на персональні дані.
5. Підставою виникнення права на захист персональних даних, є порушення особистих немайнових прав суб'єкта персональних даних. До діянь, які становлять зміст відповідного правопорушення, переважно належать вчинки у процесі обробки володільцем чи розпорядником персональних даних, всупереч приписам законодавства. Такі діяння проявляються в незаконному зборі, використанні й поширенні інформації персонального характеру.
6. Національне законодавство щодо захисту персональних даних складається з більше ніж 20 нормативно-правових актів, які, з огляду на практику їх використання, потребують вдосконалення.
7. Суб'єкт персональних даних має право звертатися із скаргами на обробку своїх персональних даних до Уповноваженого Верховної Ради України з прав людини або до суду.

За підсумками дослідження розроблено такі пропозиції щодо вдасконалення законодавства України щодо захисту персональних даних в мережі Інтернет:

- доповнити статтю 2 Закону України «Про захист персональних даних» новою частиною щодо визначення поняття прав суб'єкта персональних даних, виклавши її в такий редакції: «права суб'єкта персональних даних – права фізичної особи, якій належать персональні дані, що обробляються, або її представників, які від імені цієї особи надають згоду

на таку обробку та здійснюють інші права щодо захисту персональних даних»;

- внести зміни до частини першої статті 182 Кримінального кодексу України, виклавши її в такій редакції: «1. Незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації та/або персональних даних про особу або незаконна зміна такої інформації та/або даних, крім випадків, передбачених іншими статтями цього Кодексу»;

- актуальним завданням для України є приведення національного законодавства у відповідність з міжнародними стандартами, тому Україні слід ратифікувати Окінавську хартію глобального інформаційного суспільства від 22.07.2000, що покликана ліквідувати прогалини у правовій, технологічній та інформаційній галузях знань;

- внести зміни до визначення персональних даних, зазначеного у Законі №2297, яке у сучасних реаліях не охоплює різноманітність проблемних правовідносин у сфері захисту персональних даних. Недосконаліть визначення поняття «персональні дані» тягне за собою неможливість в повній мірі врегулювати проблеми визначення відповідальності за порушення в даній сфері.

Здобуті результати можуть бути використані науково та практично у:

- науковій діяльності – для проведення подальших цілеспрямованих досліджень за темою роботи, а також при підготовці та написанні підручників, навчальних посібників;

- законотворчій діяльності з метою вдосконалення чинного законодавства України.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України: Закон України від 28.06.1996 року № 254к/96. *Відомості Верховної Ради України.* 1996. № 30. Ст. 141.
2. Декларація принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті» від 12.12.2003 // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/995_c57 (дата звернення: 09.10.2020).
3. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24.10.1995 // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/994_242 (дата звернення: 09.10.2020).
4. Конвенція ООН про використання електронних повідомлень у міжнародних договорах від 23.11.2005 // База даних «Законодавство

України». URL: https://zakon.rada.gov.ua/laws/show/995_e71 (дата звернення: 09.10.2020).

5. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних 28.01.1981 // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/994_326 (дата звернення: 09.10.2020).
6. Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/994_326 (дата звернення: 09.10.2020).
7. Окінавська хартія глобального інформаційного суспільства від 22.07.2000 // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/ laws/show/998_163 (дата звернення: 09.10.2020).
8. Цивільний кодекс України : Закон України від 16.01.2003 № 435-IV. URL: https://zakon.rada.gov.ua/laws/card/435-15 (дата звернення: 09.10.2020).
9. Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних: Закон України від 02.06.2011 № 3454. *Відомості Верховної Ради України*. 2011. № 50. Ст. 549.
10. Про доступ до публічної інформації: Закон України від 13.01.2011 року № 2939-VI. URL: https://zakon.rada.gov.ua/laws/card/2939-17 (дата звернення: 09.10.2020).
11. Про захист персональних даних: Закон України від 01.06.2010 року № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 09.10.2020).

12. Про інформацію: Закон України від 02.10.1992 року № 2657-XII. URL: https://zakon.rada.gov.ua/laws/card/2657-12 (дата звернення: 09.10.2020).
13. Про основні засади забезпечення кібербезпеки України: Закон України від 21.06.2018 № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.
14. Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних: Закон України від 06.07.2010 № 2438. *Відомості Верховної Ради України*. 2010. № 46. Ст. 542.
15. Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних, затверджений наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 №1/02-14 // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14 (дата звернення: 09.10.2020).
16. Типовий порядок обробки персональних даних, затверджений наказом Уповноваженого Верховної Ради України від 08.01.2014 № 1/02-14. URL: http://www.ombudsman.gov.ua/ua/page/secretariat/docs/legislation/tipovij-poryadok-obrobki-personalnix-danix.html (дата звернення: 09.10.2020).
17. Рішення ЄСПЛ у справі «С. та Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom), №№ 30562/04 та 30566/04 від 4 грудня 2008 р.; див. також, наприклад: рішення ЄСПЛ у справі «М.М. проти Сполученого Королівства» (M.M. v. the United Kingdom), № 24029/07 від 13.11.2012. URL: https://rm.coe.int/168059920d (дата звернення: 09.10.2020).

18. Рішення ЄСПЛ у справі «К.У. проти Фінляндії». № 2872/02 від 02.12.2008 р. URL: https://protocol.ua/ua/k_u_proti_finlyandii/ (дата звернення: 09.10.2020).
19. Постанова Верховного суду України від 08.02.2019 №855/17/19 // База даних «Єдиний державний реєстр судових рішень». URL: http://www.reyestr.court.gov.ua/Review/79699192(дата звернення: 09.10.2020).
20. Рішення Конституційного суду України від 20.01.2012 № 2-рп/2012 за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/v002p710-12 (дата звернення: 09.10.2020).
21. Рішення Конституційного суду України від 30.10.1997 №5-зп у справі щодо офіційного тлумачення ст. 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К.Г.Устименка). *База даних «Законодавство України»*. URL: https://zakon.rada.gov.ua/ laws/show/v005p710-97 (дата звернення: 09.10.2020).
22. Рішення Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ по справі №6-25324ск14 від 18.07.2014. URL: http://www.reyestr.court. gov.ua/Review/39797551 (дата звернення: 09.10.2020).
23. Категорія справи № 753/15830/18: Цивільні справи (до 01.01.2019); Позовне провадження; Спори про недоговірні зобов'язання. URL: http://reyestr.court.gov.ua/Review/89694900 (дата звернення: 09.10.2020).
24. Категорія справи № 753/18972/16-ц: Цивільні справи (до 01.01.2019); Позовне провадження; Спори про недоговірні зобов'язання; Спори про

відшкодування шкоди. URL: http://reyestr.court.gov.ua/Review/91614000 (дата звернення: 09.10.2020).

25. Баранов О. А. Віртуальність і правове регулювання. *Публічне право*. 2017. № 1. С. 210-218.
26. Березовська І. Р., Русак Д. М. Вдосконалення правового регулювання захисту персональних даних в мережі Інтернет в контексті інтеграції України в світовий інформаційний простір. *Актуальні проблеми міжнародних відносин*. 2017. №124. С. 74-84.
27. Бєляков К. І. Понятійні та методологічні основи регулювання нових типів інформаційних відносин: «віртуальні правовідносини». *Lex Portus*. 2016. № 2. С. 47-63.
28. Брижко В.М. Сучасні основи захисту персональних даних в європейських правових актах. *Інформація і право*. 2016. № 3(18). С. 45-57.
29. Гавловський В. Д. До питання захисту персональних даних у соціальних мережах. URL: http://pravoznavec.com.ua/period/ article/26876/%C3. (дата звернення: 09.10.2020).
30. Головатий С. Передмова до проекту Цивільного кодексу України. *Українське право*. 1996. № 2 (Спецвипуск). С. 11.
31. Головченко В. В. Правові основи захисту персональних даних. *Юридична газета*. 2018. №36. С. 16-24.
32. Гуйван П. Д. Правові оцінки ЄСПЛ щодо захисту персональних даних та їхнє значення для України. *Вісник НТУУ «КПІ» Політологія. Соціологія. Право.* 2019. №1. С. 91-96.
33. Данильченко О. В. Цивільно-правовий захист немайнових прав фізичної особи за законодавством України. *Молодий вчений*. 2018. №5. С. 603-607.
34. Деякі питання практичного застосування Закону України «Про захист персональних даних»: роз'яснення Міністерства юстиції України від

21.12.2011 р. URL: http://zakon2.rada.gov.ua/laws/show /n0076323-11/conv (дата звернення: 09.10.2020)

35. Довгаль Ю. С. Поняття захисту інформаційних систем. *Науковий вісник Херсонського державного ун-ту*. 2015. №2 3. Том 2. С.83 86
36. Єсимов С. С. Захист персональних даних у контексті розвитку динамічних інформаційних систем. *Науковий вісник ЛДУВС*. 2013. №3. С. 198-208.
37. Забара І. М. Міжнародна інформаційна безпека: сучасні концепції в міжнародному праві. *Теорія і практика правознавства*. 2013. № 2. С. 21-28.
38. Кардаш А. В. Конституційно-правовий захист інформації про особу (порівняльно-правовий аспект): дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.02. Харків, 2019. 244 с.
39. Каретник О. С. Поняття інформації про фізичну особу (персональні дані) в цивільному праві України. *Часопис Київського університету права*. 2013. № 2. С.228-231.
40. Коренюк О.О. Адміністративно-правовий режим інформації з обмеженим доступом : автореф. дис. ... канд. юрид. наук : 12.00.07. Київ, 2019. 18 с.
41. Марущак А. І. Проблеми правового захисту персональних даних в умовах соціалізації Інтернет-сервісів. URL: http://ippi.org.ua/sites/default/files/ 12maisis.pdf. (дата звернення: 09.10.2020).
42. Мельник К. С. Теоретичні та організаційно-правові засади захисту персональних даних в контексті євроінтеграції України. Київ: ТОВ «ПанТот», 2016. 126 с.

43. Михайленко І. В. Право людини на недоторканість приватного життя: поняття, аспекти, механізм реалізації : автореф. дис. ... канд. юрид. наук. Харків, 2014. 20 с.
44. Муха А. В. Загрози використання персональних даних у мережі Інтернет. *Наукові записки студентів та аспірантів*. 2020. №5. С. 323-330.
45. Нестеренко О. Інформація в Україні: право на доступ. Харків. : Акта, 2012. 306 с.
46. Оніщенко О. В. Персональні дані працівників: деякі особливості використання. *Вісник Академії адвокатури*. 2012. №3. С. 173–175.
47. Пазюк А. В. Міжнародно-правовий захист права людини на приватність персоніфікованої інформації: дис… канд. юрид. наук: 12.00.11. Київ, 2004. 205 с.
48. Пазюк А. Захист персональних даних: європейський досвід та перспективи впровадження в Україні. *Економіка. Фінанси. Право*. 2000. № 10. С. 22-25.
49. Пилипчук В. Г., Брижко В. М. Реформування і розвиток системи захисту персональних даних в Україні. *Інформація і право* 2017. № 3(22). С. 5-21.
50. Пилипчук В. Г., Брижко В. М. Трансформація системи захисту персональних даних та приватності в контексті євроінтеграції України. *Вісник Національної академії правових наук України.* 2017 № 3 (90) С. 36-50.
51. Посібник з європейського права у сфері захисту персональних даних. Київ: К.І.С., 2015. 216 с.
52. Пріоритети співпраці З ЄС у сфері правоохоронного співробітництва, боротьби з організованою злочинністю, кібербезпеки та захисту персональних даних. Експертна підтримка впровадження порядку денного у сфері юстиції, свободи та безпеки Україна – ЄС.URL:

https://www.civic-synergy.org.ua/wp-content/uploads/2020/02/Priorytety-spivpratsi-z-YES-u-sferi-pravoohoronnogo-spivrobitnytstva-borotby-z-organizovanoyu-zlochynnistyu-kiberbezpeky-ta-zahystu-personalnyh-danyh.pdf (дата звернення: 09.10.2020)

53. Радкевич О. П. Законодавче забезпечення охорони й захисту персональної інформації в мережі Інтернет // *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: науково-технічний збірник*. 2012. №1 (23). С. 26-29.
54. Радкевич О.П. До розуміння персональної інформації та персональних даних Інформаційні технології в глобальному управлінні: Матеріали наук.-практ. конф. м. Київ, 29 жовтня 2011 р. Київ, 2011. С. 122- 124
55. Різак М. Практика країн ЄС та України у сфері судочинства щодо гарантування безпеки обігу та обробки персональних даних. *Підприємництво, господарство і право*. 2017. №7. С. 68-72.
56. Різак М.В. Правовий статус Уповноваженого органу з питань захисту персональних даних: досвід зарубіжних країн. *Форум права.* 2012. № 3. С. 619-625
57. Русак Д. М., Березоваська І. Р. Вдосконалення правового регулювання захисту персональних даних в мережі Інтернет в контексті інтеграції України в світовий інформаційний простір. *Actual problems of international relations*. Release 124 (part II). 2015. С. 74-84
58. Ручка К. Ю. Правове регулювання захисту персональних даних в мережі Інтернет. *Цивільне та комерційне право : виклики сьогодення.* КНТЕУ, 2020. С. 36-43.
59. Серебряник О. О. Інформація про особу як об’єкт цивільних справ : дис. ... канд. юрид. наук : 12.00.03. Івано-Франківськ, 2016.
60. Серьогін В. О. Конституційне право особи на недоторканість приватного життя (прайвесі): проблеми теорії та практики: дис. ... д-ра юрид. наук. Харків, 2011. 415 с.

61. Темченко В. Особливості юридичного змісту термінів «захист» та «охорона» у механізмі забезпечення прав людини. *Вісник Академії управління* МВС. 2007. № 2-3. С. 58-65
62. Теремецький В. І. Суб'єкти відносин, пов'язаних з персональними даними. *Право і безпека*. 2015. №2. С.171-176.
63. Тунік А. Персональні дані, інформація про особу, конфіденційна інформація про особу: аспекти співвідношення. *Підприємництво, господарство і право*. 2012. № 5. С. 50-54.
64. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право.* 2012. № 2. С. 162-169.
65. Черниш Р.Ф. Соціальні мережі як один із інструментів накопичення та протиправного використання персональних даних громадян. *Проблеми законності.* 2017. №136. С. 205-214.
66. Чуприна О. Співвідношення понять "персональні дані", "інформація про особу", "конфіденційна інформація про особу". *Підприємництво, господарство і право*. 2013. № 1. С. 104-105.
67. Швець М. Я. Інформатизація шляхом співпраці колективів розробників і користувачів. *Правова інформатика*. 2010. № 3. С. 3-8.
68. Шевченко Я. М. Власник і право власності. Київ: Наук, думка. 1994. 205 с.
69. Шишка Р. Б. Охорона прав суб'єктів інтелектуальної власності у цивільному праві України: дис.докт. юрид. наук : 12.00.03. Харків, 2004. 469 с.
70. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні за 2018 рік. URL: http://www.univ.kiev.ua/content/upload/2019/-697223196.pdf (дата звернення: 09.10.2020)

71. CASE OF FUCHSMANN v. GERMANY. URL: https://hudoc.echr.coe.int/eng#%7B%22fulltext%22:%5B%22fuchsmann%20v%20germany%22%5D,%22kpthesaurus%22:%5B%22149%22,%22640%22,%22148%22,%22156%22,%22157%22,%22158%22,%22160%22,%22161%22,%22608%22,%22230%22,%22382%22,%22409%22,%22105%22,%22201%22,%22265%22,%22235%22,%22259%22,%22326%22,%22327%22,%22331%22,%22356%22,%22362%22,%22579%22,%22379%22,%22389%22,%22488%22,%22316%22,%226%22,%22140%22,%22452%22,%22451%22,%22634%22,%22424%22,%22425%22,%22429%22,%22203%22,%22268%22,%22107%22,%22262%22,%22329%22,%22333%22,%22358%22,%22365%22,%22376%22,%22391%22,%22319%22,%22557%22,%22558%22,%22556%22,%22559%22%5D,%22documentcollectionid2%22:%5B%22JUDGMENTS%22,%22DECISIONS%22%5D,%22kpdate%22:%5B%2220140902T00:00:00.0Z%22,%2220190902T00:00:00.0Z%22%5D,%22itemid%22:%5B%22001-177697%22%5D%7D (дата звернення: 09.10.2020)
72. CASE OF M.L. AND W.W. v. GERMANY. URL: https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-183947%22% 5D%7D (дата звернення: 09.10.2020)
73. CASE OF BENEDIK v. SLOVENIA. URL: https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-182455%22% 5D% 7D (дата звернення: 09.10.2020)
74. Ganslandt M. Social network privacy standards. Talkstandards. 2010. URL: http://www.talkstandards.com/social-network-privacy-standards (дата звернення: 09.10.2020)
75. Google Spain SL Google Inc. V Agencia Española de Protección de Datos (AEPD) Mario Costeja González Judgment of the Court (Grand Chamber) in Case C-131/12, 13 May 2014. URL: http://curia.europa.eu/juris/document/document.

jsf?text=&docid=152065&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=794833 (дата звернення: 09.10.2020)

76. On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) : Reglament (EU) 2016/679 of the European Parlament and of the Council, of 27 April 2016 / Регламент (ЄС) 2016/679 від 27.04.16 р. http://eur-lex.europa.eu/legal-content /EN/ TXT/HTML/?uri=CELEX:32016 R0679&from= EN (дата звернення: 09.10.2020)