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

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

ЦИВІЛЬНО-ПРАВОВИЙ ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

Студентки 2 курсу, 8 мз групи,
спеціальності 081 «Право»
спеціалізації
«Цивільне право і процес» _____ Чикунської Яни Вадимівни

Науковий керівник
кандидат юридичних наук,
професор _____ Фурса Євген Іванович

Гарант освітньої програми
доктор юридичних наук
_____ Примак Володимир Дмитрович

Київ 2019

ЗМІСТ

ВСТУП

Актуальність теми. Правовий зміст терміну «персональні дані» є вихідним у формуванні підходів щодо законодавчого регулювання захисту персональних даних в Україні. Персональні дані особи є ключовим об'єктом особистих немайнових прав фізичної особи, а тому належне цивільно-правове регулювання правовідносин щодо їх збереження, використання та розповсюдження має вирішальне значення для їх належного правового захисту.

У сучасному світі, в силу широкого використання автоматизованих систем та відповідних технологій, інформація про будь-яку особу може стати тією чи іншою мірою відкритою і призвести до порушення її прав та законних інтересів, заподіяння матеріальної або моральної шкоди. Вказане зумовлює необхідність належного правового регулювання відносин, пов'язаних із охороною і захистом цієї інформації особистого характеру про фізичну особу.

Серед актуальних подій, які прямо пов'язані із покращенням правового регламентування захисту персональних даних є набуття чинності нового Регламенту ЄС про захист даних (GDPR) 25 травня 2018 року. Значення цього нормативного акту полягає в тому, що в ньому відображені такі правові норми, які регулюють захист персональних даних про особу в сучасному світі глобальної комп'ютеризації та інформатизації суспільства.

Теоретичною основою для дослідження цивільно-правового захисту інформації про особу стали наукові праці українських вчених: Ю. Д. Бєлова, І. М. Бем, В. М. Брижко, Н. В. Камінська, К. С. Мельник, А. Л. Петрицький, О. П. Радкевич, В. М. Різак, І. І. Романюк, В. І. Теремецький та інших. Наукові пошуки з даного питання знаходяться у стадії свого розвитку, що потребує подальших досліджень.

Слід зазначити, що питання захисту інформації про особу неодноразово ставало предметом дисертаційних досліджень на

кандидатському рівні з позицій цивільного права: О. А. Дмитренко «Право фізичної особи на власні персональні дані в цивільному праві України», 2010 р.; О. П. Радкевич «Цивільно-правова охорона і захист персональної інформації в мережі Інтернет», 2014 р. та І. І. Романюк «Охорона права на персональні дані в України (цивільно-правовий аспект)», 2015 р., але дана робота істотно відрізняється від попередніх за отриманими результатами.

Мета дослідження. Метою роботи є розкриття теоретично-практичних аспектів цивільно-правового захисту персональних даних в Україні.

Для досягнення вказаної мети поставлено такі **завдання**, що розкривають спрямованість дослідження:

- розкрити сутність поняття «персональні дані» як об'єкта цивільно-правової регламентації;
- визначити поняття, ознаки та види баз персональних даних;
- з'ясувати підстави та вимоги до обробки персональних даних;
- охарактеризувати правовий статус суб'єктів правовідносин, які потребують захисту персональних даних;
- визначити методи та форми захисту персональних даних;
- розкрити перспективи вдосконалення законодавства про захист персональних даних.

Об'єктом дослідження є суспільні відносини, що складаються в процесі цивільно-правового захисту персональних даних особи в Україні.

Предметом дослідження є цивільно-правовий захист персональних даних особи.

Методологічну основу роботи становить сукупність прийомів і методів наукового пізнання. У процесі дослідження цивільно-правового захисту персональних даних були використані такі методи наукового пізнання: діалектичний метод – для аналізу питання цивільно-правового захисту персональних даних у цілісності, всебічності і динаміці; структурно-функціональний – для виокремлення та дослідження чинників, які впливають на захист персональних даних; формально-логічний – при формулюванні

визначень таких понять, як «персональні дані», «обробка персональних даних», «захист персональних даних» тощо; формально-юридичний – при тлумаченні і аналізі положень чинного законодавства, судової практики України та зарубіжних країн.

Наукова цінність випускної кваліфікаційної роботи полягає у розробці доктринальних, теоретичних положень і висновків, практичних рекомендацій щодо вдосконалення цивільно-правового регулювання захисту персональних даних в Україні. Зокрема, елементи наукової новизни містяться у пропозиції щодо надання чіткого визначення терміна «захист персональних даних».

Практична цінність полягає в тому, що матеріали випускної кваліфікаційної роботи можна використовувати при розробці навчальних матеріалів з дисципліни «Цивільне право» та у подальших дослідженнях питання захисту персональних даних. Висновки та пропозиції запропоновані в роботі можуть бути застосовані у правотворчій діяльності з метою вдосконалення законодавства у сфері захисту персональних даних. Окремі положення випускної кваліфікаційної роботи викладено у статті Чикунської Я. В. Персональні дані, які ідентифікують особу, та негативні наслідки оприлюднення даної інформації. *Правове забезпечення підприємницької діяльності* : зб. наук. ст. студ. / відп. ред. О. О. Бакалінська, В. Д. Примак, Ю. В. Тищенко. Київ : Київ. нац. торг.-екон. ун-т, 2019. Ч. 2. С. 156 –161.

Структура випускної кваліфікаційної роботи відповідає її меті та завданням, складається зі вступу, двох розділів, що поділяються на три підрозділи кожний, висновків та пропозицій, списку використаних джерел, який містить 92 найменування. Повний обсяг випускної кваліфікаційної роботи становить 64 сторінки, з яких обсяг основної частини складає 52 сторінки.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ЗАХИСТУ ТА ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

1.1. Персональні дані як об’єкт цивільно-правової регламентації

Передумовою формування правового інституту персональних даних є необхідність правової індивідуалізації фізичної особи як суб'єкта цивільного права. І це цілком розумно, адже будь-яка особа є частиною соціуму і не може бути єдиним володарем інформації про себе. Інформація про особу постійно знаходиться в правовому обігу в суспільстві в тій чи інший формі. Інформаційна персоніфікація фізичної особи також стає передумовою для реалізації її правосуб'єктності, оскільки є необхідною складовою вступу до відповідних цивільних правовідносин.

Реалізуючи порядок оформлення і надання власних персональних даних, фізична особа створює умови включення його в юридичний порядок реалізації власних прав, забезпечення інтересів, а також їх захисту в разі їх порушення [33, с.14].

Інакше кажучи, наявність інформації про особу (персональні дані) дозволяє більш конкретно встановити правові зв'язки між потенційними суб'єктами цивільних правовідносин.

Проблема термінологічного визначення та розуміння поняття «персональні дані» є однією із найскладніших при роботі в цій сфері. Саме у визначенні містяться межі та критерії віднесення тієї чи іншої інформації до цієї категорії.

Аналіз поняття «персональні дані», трактування змісту якого наведено у таких нормативних джерелах (табл. 1.1), свідчить про те, що в основному вони збігаються, ключовим моментом усіх визначень є можливість безпомилкової ідентифікації конкретної особи.

Таблиця 1.1

Нормативне визначення поняття «персональні дані»

Нормативний акт	Зміст поняття
Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року (дата ратифікації Україною: 06.07.2010 року, дата набрання чинності для України: 01.01.2011 року)	Персональні дані - будь-яка інформація, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною.
Закон України «Про інформацію» від 02.10.1992 року № 2657-XIII	Інформація про фізичну особу (персональні дані) - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.
Директива 95/46ASC Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року	Персональні дані означають будь-яку інформацію, що стосується встановленої фізичної особи чи фізичної особи, яку можна встановити («суб'єкт даних»). Особою, яку можна встановити, є така, яка може бути встановленою прямо чи непрямо, зокрема, за допомогою ідентифікаційного коду або одного чи більше факторів, притаманних фізичним, фізіологічним, розумовим, економічним, культурним чи соціальним аспектам її особистості.
Закон України «Про захист персональних даних» від 1.06.2010 року № 2297-VI	Персональні дані - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.
Регламент (ЄС) 2016/679 від 27.04.16 р.	Персональні дані - це будь-яка інформація, яка стосується фізичної особи, що ідентифікована або може бути ідентифікована ("суб'єкт даних").

Передумовою нормативної регламентації поняття «інформації по фізичну особу (персональні дані)» в національному законодавстві України стала Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 р., у ст. 2 якої також міститься визначення терміну «персональні дані». Під ними розуміють будь-яку інформацію, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною [3].

В цілому чинне законодавство України містить близько 3500 нормативно-правових актів, які регламентують правові відносини, пов'язані з обігом інформації про фізичну особу (персональні дані). Більшість з них

конкретизує зміст інформації про особу виключно щодо сфери правового регулювання трудових, адміністративних або кримінально-процесуальних правовідносин. Зміст цієї інформації має розрізнений характер і не підпорядковується єдиним критеріями.

Ключовими в даному відношенні в українському законодавстві є Закони України «Про інформацію», «Про доступ до публічної інформації» та «Про захист персональних даних». Єдиним з цих трьох нормативних актів, який дає пряме визначення інформації про особу, є лише Закон України «Про інформацію». Відповідно до ч.1 ст.11 цього Закону, інформація про фізичну особу (персональні дані) - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [11]. Як видно, йдеться, що інформація про особу ототожнюється з персональними даними. Крім того, підкреслюється, що саме поняття інформації про особу та персональних даних стосується саме фізичної особи.

Хоча законодавство безпосередньо не визначає вимоги до інформації, яка має бути надана суб'єкту персональних даних, вважаємо, що вона повинна бути необхідною, доступною, достовірною та своєчасною. Необхідною інформацію щодо обробки персональних даних слід вважати тоді, коли вона включає відомості про: 1) суб'єктів (володільця чи розпорядника персональних даних, їх місцезнаходження або місце проживання (перебування); третіх осіб, яким передаються його персональні дані); 2) об'єкт (склад та зміст зібраних персональних даних); 3) суб'єктивні умови (права, визначені законом, мету збору персональних даних); 4) об'єктивні умови (джерела збирання, місцезнаходження своїх персональних даних; умови надання доступу до персональних даних; механізм автоматичної обробки персональних даних; які дії з персональними даними передбачатиме їх обробка; скільки часу персональні дані будуть зберігатися у володільця). М. В. Бем зазначає, що доступність інформації вказує на два елементи: 1) зміст її повинен бути доступним для розуміння особою, яка не є спеціалістом у сфері законодавства про захист персональних

даних; 2) інформація повинна подаватись у наочній формі, доступній для сприйняття суб'єктом персональних даних [36, с. 60]. Достовірність інформації вказує на те, що вона повинна відповідати дійсності та не вводити суб'єкта персональних даних в оману. Своєчасність такої інформації означає, що вся необхідна інформація повинна бути надана суб'єкту персональних даних у момент запитування згоди на обробку його персональних даних.

Крім того, згадані закони так чи інакше пояснюють термін «інформація про особу» в контексті терміна «конфіденційна інформація». Відповідно до ч. 2 ст. 21 Закону України «Про інформацію», «конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом. Відносини, пов'язані з правовим режимом конфіденційної інформації, регулюються законом» [11].

Норма ч. 2 ст. 11 зазначеного Закону до конфіденційної інформації відносить інформацію про фізичну особу, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адресу, дату і місце народження [11]. Таким чином, будь-яка інформація про особу називається конфіденційною.

Натомість ч. 1 ст. 7 Закону України «Про доступ до публічної інформації» визначає конфіденційною інформацію, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов [12]. Тобто, на відміну від Закону «Про інформацію», згадка про будь-яку інформацію про особу як конфіденційну тут вже відсутня.

Так само, відповідно до ст. 2 Закону України «Про захист персональних даних» (далі – Закон), персональні дані - відомості чи

сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [10].

Відповідно до ч. 2 ст. 5 цього ж Закону, персональні дані можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою [10]. Отже, розуміння конфіденційної інформації в Законі «Про захист персональних даних», як і в Законі «Про доступ до публічної інформації», є вужчим, ніж зведення її до всієї інформації про особу.

О. Б. Червякова вважає, що як такого переліку персональних даних, що відносяться до конфіденційної інформації, Закон не містить, власне про що конкретно йдеться, коли ми говоримо про віднесення інформації до конфіденційної інформації про особу законом, і чим така інформація відрізняється від тієї конфіденційної інформації, режим конфіденційності якої встановлює сама особа, достеменно незрозуміло [89, с. 102].

О. О. Серебряник вказує, що фактично український законодавець вживає поняття «інформація про фізичну особу» і «персональні дані» як синоніми. Законодавець ототожнює інформацію про фізичну особу та її персональні дані [82, с. 88].

При цьому, відповідно до Закону «Про інформацію», будь-які персональні дані (інформація про фізичну особу) водночас вважаються конфіденційною інформацією [11], тобто інформацією з обмеженим доступом. Трохи вужчим до конфіденційної інформації є підхід, закладений в Законі «Про доступ до публічної інформації» і в Законі України «Про захист персональних даних».

Вказане дозволяє зробити висновок, що зміст інформації про фізичну особу (персональні дані) залежить від характеру правовідносин, в яких вони отримують своє наповнення. Вказане зумовлено специфікою відповідної правової регламентації цих відносин. Власне інформація про фізичну особу (персональні дані) не є універсальним поняттям, що має тотожній зміст у сфері приватного чи публічного права.

Так, В. М. Брижко зазначає, що «персональні дані» - це окремі відомості про фізичну особу чи сукупність таких відомостей про особу, яка ідентифікована, або таку, яка може бути ідентифікованою [42, с. 15].

Головним документом сучасних правових стандартів є Регламент (ЄС) 2016/679 від 27.04.16 р. про захист фізичних осіб у зв'язку з опрацюванням персональних даних та про вільний рух таких даних, а також про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)» (General Data Protection Regulation) [37, с. 34].

Згідно Регламенту (ЄС) 2016/679 «персональні дані» - це будь-яка інформація, яка стосується фізичної особи, що ідентифікована або може бути ідентифікована («суб'єкт даних»); фізична особа, що може бути ідентифікована - це особа, яка може бути ідентифікована, прямо чи опосередковано, зокрема за такими ідентифікаторами, як ім'я, ідентифікаційний номер, відомості про місце розташування, он-лайн-ідентифікатор або на один чи декілька факторів, специфічних для фізичної, фізіологічної, генетичної, ментальної, економічної, культурної або соціальної ідентичності цієї фізичної особи [4].

Якщо раніше персональними даними вважалися тільки документи, що містять імена, адреси й т.ін., то зараз це визначення розширено. Дані, пов'язані з IP-адресами, е-поштою та cookie-файли, що зберігають суто індивідуальні відомості про користувача мережі також охоплюються положеннями Регламенту (ЄС) 2016/679 [4].

Із загального переліку персональних даних виділяються спеціальні, чутливі категорії, обробка яких дозволяється лише у чітко визначених випадках.

До таких категорій вказані правові акти відносять персональні дані про:

- расове або етнічне походження;
- політичні, релігійні або світоглядні переконання;
- членство в політичних партіях та професійних спілках;
- засудження до кримінального покарання;

• дані, що стосуються здоров'я, статевого життя, а також біометричні або генетичні дані.

Крім того, згідно ст. 9 Регламенту (ЄС) 2016/679, до цієї групи віднесені генетичні та біометричні дані, які можуть використовуватися для ідентифікації фізичної особи [4].

Важливим є те, що персональними вважаються тільки ті дані, за якими особу можна ідентифікувати. Наприклад, пошта містить ім'я, прізвище і е-адресу, тому відноситься до персональних даних, а окрема адреса е-пошти - ні; ім'я і номер телефону - персональні дані, телефон/адреса самі по собі - просто дані. Якщо з даних стає щось відомо про людину (її місце роботи, контакти і інше), то вони відносяться до персональних. Також, будь-які відомості, до яких було застосовано псевдонім, який може бути віднесено до фізичної особи за допомогою використання додаткової інформації, повинні розглядатися як відомості про фізичну особу, що може бути ідентифікована.

В. М. Брижко відмічає, що у міжнародних нормативних документах визнається умовний поділ персональних даних на дві групи: дані «загального змісту» та особливі категорії відомостей, що визначаються як «чутливі» дані (sensitive data) [45, с. 51]. До останніх належать відомості про расове походження, політичні, релігійні чи інші вірування, а також щодо здоров'я чи сексуального життя. Для зазначеної категорії даних мають національними законодавствами встановлюватись додаткові заходи забезпечення їх безпеки.

При класифікації персональних даних особливу увагу слід приділяти біометричним даним, тобто даним про фізіологічні особливості людини, на основі яких її можна ідентифікувати (вага, зріст, група крові, відбитки пальців, цифровий образ особи, сітківка ока тощо). Саме біометрична інформація є одним з «найпотужніших» ідентифікаторів.

Таким чином, під поняттям «персональні дані» слід розуміти дані про людину, яка ідентифікована або може бути ідентифікована на основі цих даних або на основі цих даних і додаткової інформації, що може потрапити до особи, яка контролює дані, і які містять вираження ставлення до цієї

людини і вказівку на певну мету або плани відносно цієї людини з боку особи, яка контролює дані, або іншої особи.

Все вищеозначене дозволяє сформулювати загальний висновок про те, що інформація про фізичну особу (персональні дані) - це конкретні відомості про суб'єктивні цивільні права і юридичні обов'язки особи, які забезпечують її правосуб'єктну персоніфікацію, а також про певні характерні особливості особи як особистості.

1.2. Поняття, ознаки та види баз персональних даних

Правове регулювання створення та функціонування баз персональних даних у нашій країні - відносно нове явище, що перебуває на стадії вивчення та системного вдосконалення.

Сьогодні в Україні бази персональних даних активно використовуються у правовідносинах. Початок формування ринку використання баз персональних даних було закладено Законом України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [13]. Згідно з цим нормативним актом формування інформаційного суспільства передбачає появу нових об'єктів інтелектуальної власності, які є основою інноваційної моделі економіки України. Одним з об'єктів, що з'явився завдяки розвитку нових технологій в Україні, є бази персональних даних, які природно виникли з більш широкого об'єкта – бази даних.

В українському законодавстві правова дефініція «база персональних даних» була введена у 2010 р. Законом України «Про захист персональних даних» [10]. Цей Закон приймався з метою врегулювання правовідносин та імплементації в українське законодавство основних принципів Директиви Європейського Парламенту та Ради ЄС «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» 95/46/ЄС від 24.10.1995 р. [5]. У свою чергу, 6 липня 2010 р. Україна

ратифікувала базові європейські стандарти у сфері захисту персональних даних, зокрема Конвенцію Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додатковий протокол до неї щодо органів нагляду та транскордонних потоків даних [3]. Таким чином, як на європейському, так і на українському рівні встановлена правова регламентація обробки персональних даних у систематизований об'єкт збереження.

В. І. Теремецький відзначає, що Закон України «Про захист персональних даних» установив визначення бази персональних даних, що стало додатковою гарантією охорони персональних даних, оскільки невизначеність цього об'єкта у правових нормах надавала можливість передавати його контрагентам без згоди особи, якій належать персональні дані, зокрема від банку до банку на підставі угоди про передачу бази клієнтів, або колекторам. Отже, цей об'єкт став предметом цивільно-правових угод. При їх укладанні не було встановлено обмежень щодо охорони персональних даних. Усе це негативно відбивалось на охороні приватного життя особи, дані якої внесені у бази персональних даних. Прийняття окремого Закону з цього питання надало можливість не тільки захистити права особи, а й розширити сферу застосування баз даних [86, с. 172].

На сьогодні підприємства можуть створювати різні бази персональних даних: контрагентів, працівників, клієнтів, осіб, які можуть підписувати угоди юридичної особи, та інші. Ці сховища інформації містять важливі дані про людину: дані про народження, стать, місце проживання, професію, сімейний стан, інтереси. Необхідно зауважити і те, що наявність у юридичної особи бази персональних даних впливає на процедуру її ліквідації, зокрема одним із етапів процесу ліквідації суб'єкта господарювання є передача необхідних для зберігання баз персональних даних в архів. Все це свідчить про те, що цивільні правовідносини з приводу бази персональних даних

фактично сформувались, однак цей об'єкт все ще не розглянуто в межах цивільного права.

Згідно зі ст.1 Закону України «Про захист персональних даних» база персональних даних – іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних [10]. З цього визначення випливає, що база персональних даних - це система даних про особу, які обробляються та структурно розташовуються у базі даних.

База персональних даних є системою спеціально, комплексно організованих даних, що характеризують стан системи персональних даних, які отримані та оброблені під спеціалізовану базу даних, та розташовуються, упорядковуються, зберігаються за допомогою електронних обчислювальних машин або іншого засобу і можуть бути доступними індивідуально чи за допомогою системи управління базою даних з метою задоволення інформаційних потреб.

У сучасних інформаційних ресурсах бази персональних даних найчастіше існують в електронній, тобто в цифровій, формі. Незважаючи на поширення електронних баз персональних даних, у практичній діяльності ці бази можуть існувати й у формі картотек, що передбачено ст. 2 Закону України «Про захист персональних даних» [10]. Цей поділ за об'єктивною формою існування баз персональних даних має значення для її класифікації. Отже, бази персональних даних за об'єктивною формою існують у вигляді електронної бази та картотеки.

В. М. Брижко виокремив такі ознаки цих баз: зміст бази персональних даних - інформація про фізичну особу; об'єктивна форма існування (це матеріальний носій бази персональних даних у вигляді електронної форми або картотеки); мета існування (база персональних даних завжди створюється з відповідною метою); обов'язкова державна реєстрація бази даних [43, с. 66].

І. І. Романюк дійшов висновку, що виходячи із законодавчих норм і сучасних реалій, поняття «база персональних даних» можна визначити як сукупність персональних даних у довільній формі, зокрема електронній та/або формі картотек, складові частини якої є доступними індивідуально і можуть бути знайдені за допомогою пошукової системи на основі електронних чи інших засобів. За порядком доступу до розміщеної на них інформації розрізняють: 1) бази відкритих персональних даних, які доступні необмеженому колу осіб; 2) бази обмежених у доступі персональних даних, які доступні конкретно визначеному колу осіб; 3) бази змішаних персональних даних, частина яких доступна необмеженому колу осіб, а частина - обмеженому [78, с. 245].

М. В. Різак вважає, що для бази даних, як об'єкта цивільно-правових відносин, характерно: по-перше, наявність змісту, тобто структурованої інформації; по-друге, встановлення порядку систематизації даних, до яких можна отримати доступ; по-третє, наявність режиму доступу до даних за допомогою спеціальної пошукової системи [74, с. 17]. Звернемо увагу на те, що вказані ознаки баз даних також можна застосувати до баз персональних даних. Наприклад, база персональних даних є результатом цілеспрямованої інформаційної діяльності юридичної особи з обробки та зберігання персональних даних; інформація бази персональних даних є актуальною, відзначається повнотою, достовірністю, впорядкованістю.

Слід зазначити, що мета існування баз персональних даних полягає в задоволенні потреб в отриманні інформації про персональні дані особи з метою їх застосування. Це надає можливість виокремити таку ознаку, як придатність до застосування. Ця ознака відображає можливість використання майнових прав на базу персональних даних, зокрема застосування, розпорядження, введення у господарський обіг тощо. Необхідно зауважити, що цей критерій більше додатковий, оскільки можливість і бажання застосування бази – це суб'єктивне право правовласника і ні в якому разі не може розглядатися як обов'язок суб'єкта.

Цілісність бази персональних даних – це наявність у змісті бази єдиної достовірної, повної інформації про персональні дані співробітників, клієнтів та інших осіб; новизна бази персональних даних - це відмінність цієї бази від тих, що вже існують; однорідність інформації бази персональних даних означає, що дані відносяться до однорідної предметної сфери - упорядкування персональних даних; системність вказує на методику організації та розташування інформації у базі персональних даних; динамічність означає, що зміст може доповнюватися або змінюватися (видалення даних за вимогою клієнта або зміна прізвища працівника); об'єктивна форма існування (картотека, електронна форма); незалежність означає, що ця база існує незалежно від конкретних прикладних програм, що забезпечує уніфікацію засобів організації даних, а також від інших локальних документів підприємства; придатність для застосування - база персональних даних може бути використана у діяльності підприємства.

Спеціальною ознакою бази персональних даних є її державна реєстрація. Згідно із п. 1 ст. 9 Закону України «Про захист персональних даних» база персональних даних підлягає державній реєстрації шляхом внесення відповідного запису Державною службою України з питань захисту персональних даних до Державного реєстру баз персональних даних [10].

Таким чином, база персональних даних - це система персональних даних в електронній формі або у формі картотек, що характеризують стан системи персональних даних, які отримані та оброблені під спеціалізовану базу даних, яка реєструється, а також розміщується, упорядковується і зберігається за допомогою електронних обчислювальних машин або іншого засобу та можуть бути доступними індивідуально або за допомогою системи управління базою даних з метою задоволення інформаційних потреб.

Значить, база персональних даних в Україні є окремим об'єктом правовідносин та може бути віднесена до нематеріальних благ, які регламентуються главою 15 Цивільного Кодексу України [6]. Можливість віднесення бази персональних даних до нематеріальних благ пояснюється

тим, що вона складається з двох нематеріальних об'єктів: бази даних та інформації про персональні дані особи. Для нематеріальних благ властива відсутність матеріального (майнового) змісту, невідчужуваність [83, с. 314]. Отже, нематеріальні блага повинні існувати в об'єктивній формі, не мати матеріального змісту, бути новими та в певних випадках бути результатом творчої праці.

Але в даний час між юристами виникають дискусії щодо застосування вимог Закону України «Про захист персональних даних» в нотаріаті.

Частиною 3 статті 5 Закону України «Про нотаріат» передбачено зберігати в таємниці відомості, одержані ним у зв'язку з вчиненням нотаріальних дій [16].

Вичерпний перелік щодо суб'єктів відносин, пов'язаних із персональними даними, встановлений у статті 4 Закону України «Про захист персональних даних» [10]: фізична особа, персональні дані якої обробляються; володілець та розпорядник бази персональних даних (підприємства, установи і організації усіх форм власності, органи державної влади чи органи місцевого самоврядування, фізичні особи — підприємці, які обробляють персональні дані відповідно до закону); будь-яка інша особа, якій володілець або розпорядник бази персональних даних здійснює передачу цих даних; уповноважений державний орган з питань захисту персональних даних; інші державні органи та органи місцевого самоврядування, які здійснюють захист персональних даних.

Таким чином, можна зробити висновок, що нотаріус не є володільцем або розпорядником бази персональних даних. Нотаріус взагалі не являється суб'єктом відносин, пов'язаних із обробкою персональних даних.

Відповідно до частини 5 статті 14 Закону України «Про нотаріат» [16] архів та документи нотаріального діловодства нотаріуса є власністю держави і відповідно в цьому випадку виключно держава є володільцем та розпорядником архіву. Тобто, архів нотаріуса у жодному разі не є базою персональних даних, а картотеки персональних даних в складі архіву немає.

Також необхідно розглянути норми Закону України «Про захист персональних даних», які не можуть бути виконані у сфері нотаріату: серед прав суб'єкта персональних даних, встановлених пунктом 3 частини 2 статті 8 Закону, закріплено право на доступ до своїх персональних даних, що містяться у відповідній базі персональних даних [10]. Також статтею 16 зазначеного Закону встановлено право третіх осіб робити запит про надання персональних даних володільцю бази [10]. Проте жодна фізична особа не може мати доступу до архіву нотаріуса; неприйнятною є вимога, встановлена ч. 2 ст. 12 Закону України «Про захист персональних даних», згідно з якою суб'єкт персональних даних повинен бути повідомлений в письмовій формі про включення своїх даних у базу протягом 10 днів з дня включення [10]; не може застосовуватись до архіву нотаріуса і порядок доступу до персональних даних (стаття 16 Закону [10]), за яким доступ до персональних даних третіх осіб можливий лише за наявності згоди суб'єкта персональних даних. Адже Міністерство юстиції України та управління юстиції здійснюють перевірки діяльності нотаріусів, в ході яких нотаріус зобов'язаний надати всі документи нотаріального діловодства (архіву); не може бути застосована до нотаріусів стаття 19 зазначеного Закону, що стосується плати за доступ до персональних даних.

Відповідно до ч. 4. ст. 24 Закону України «Про захист персональних даних» фізичні особи - підприємці, у тому числі лікарі, які мають відповідну ліцензію, адвокати, нотаріуси особисто забезпечують захист персональних даних, якими вони володіють, згідно з вимогами закону [10].

Так, під час здійснення своєї професійної діяльності на нотаріусів законодавством не покладено обов'язок ведення баз персональних даних клієнтів. Але, якщо нотаріуси формують справи на своїх клієнтів, які вони постійно оновлюють та підтримують в актуальному стані, такі справи є базою персональних даних та підлягають державній реєстрації.

Нотаріуси можуть обробляти персональні дані своїх працівників, клієнтів у базах персональних даних, однак, документи нотаріального

діловодства та архів нотаріуса, визначені у статті 14 Закону України «Про нотаріат» [16] не є базою персональних даних у сенсі Закону України «Про захист персональних даних» та не підлягають державній реєстрації.

Фізичні особи-підприємці та самозайняті особи самостійно визначають чи володіють вони базами персональних даних у сенсі зазначеного Закону.

Законодавець поширив дію Закону України «Про захист персональних даних» на всі види діяльності, пов'язані зі створенням баз персональних даних та обробкою персональних даних у цих базах, за винятком такої діяльності, яка здійснюється:

- фізичною особою - виключно для непрофесійних особистих чи побутових потреб,

- журналістом - у зв'язку з виконанням ним службових чи професійних обов'язків,

- професійним творчим працівником - для здійснення творчої діяльності [52].

З огляду на вищезазначене база персональних даних є упорядкованою сукупністю логічно пов'язаних даних про фізичних осіб в електронній формі та/або у формі картотек персональних даних. Тобто база персональних даних - це не просто безсистемний набір персональної інформації, це певне її угрупування.

1.3. Підстави та вимоги до обробки персональних даних

Обробка персональних даних - це будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем [10].

Всупереч поширеному помилковому твердженню обробкою є не лише вчинення вказаних дій із систематизованою сукупністю персональних даних (базою даних, реєстром, каталогом, досьє тощо). Збір, реєстрація, накопичення чи будь-яка інша дія з боку володільця інформації навіть про одного суб'єкта персональних даних, у будь-якій формі є обробкою відповідно до положень Закону України «Про захист персональних даних».

М. В. Бем зауважує що, відповідно до усталеної практики Ради Європи та Європейського Союзу захист не є елементом обробки, оскільки не передбачає вчинення окремих дій над персональними даними. Використання зазвичай є елементом обробки, однак інколи використання є окремою відносно обробки дією щодо персональних даних. При цьому, за жодних умов обробка не може бути елементом використання. Відповідно, «захист» персональних даних слід розглядати як окрему від їх «обробки» та «використання» дію, а «використання» - як один із елементів «обробки» [35, с. 238].

Якщо говорити про види обробки персональних даних, то як специфічні категорії обробки варто виділити:

• обробку персональних даних у приватних цілях;

• обробку персональних даних у журналістських цілях;

• обробку персональних даних у творчих цілях.

Обробка персональних даних у приватних цілях відповідно до ст. 25 Закону України «Про захист персональних даних» [10] не підпадає під його дію. Слід наголосити, приватний характер цілі передбачає здійснення обробки персональних даних для особистих, наприклад домашніх потреб, а не потреб особи загалом. Наприклад, ведення особою телефонної книги є особистою потребою. Однак, якщо ця особа є власником бізнесу (наприклад, ресторанів чи магазинів) і збирає персональні дані клієнтів (ім'я, прізвище, по батькові і той же номер телефону/адреса проживання) для використання в комерційних цілях, як то реклама та просування власних послуг, то це вже не

може вважатися обробкою у приватних цілях, незважаючи на те, що здійснюється окремою особою для потреб власного бізнесу.

На обробку персональних даних у журналістських та творчих цілях положення Закону не поширюються за умови забезпечення балансу між правом на повагу до особистого життя та правом на свободу вираження поглядів. За звичайних умов специфіка журналістської діяльності не потрапляє в сферу дії Закону. Однак, якщо втручання в право особи на повагу до приватного життя внаслідок обробки її персональних даних журналістами є надмірним, у порівнянні з суспільним інтересом до висвітленої інформації (персональних даних особи) чи її суспільною вагою, можуть підніматися питання додержання законодавства про захист персональних даних.

Тут доцільно буде навести приклад: військовослужбовець у зв'язку з отриманим пораненням під час проведення антитерористичної операції перебував у Головному військово-медичному клінічному центрі «Головний військовий клінічний госпіталь» Міністерства оборони України. Журналіст розмовляв з позивачем 13 жовтня 2014 року під час перебування останнього в госпіталі з метою написання статті для ПрАТ «Сьогодні Мультимедіа», що була опублікована.

Позивач зазначає, що він просив не використовувати інформацію для публікації, проте журналіст скориставшись станом військовослужбовця після операції, отримав подробиці особистого життя позивача та використав їх у своїй статті, яка була опублікована ПрАТ «Сьогодні Мультимедіа» в газеті «Сегодня».

Ухвалою Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ від 27.07.2016 р. № 760/9778/15-ц [27] визнано протиправними дії журналіста щодо передачі конфіденційної інформації стосовно військовослужбовця без його дозволу ПрАТ «Сьогодні «Мультимедіа», оскільки той обсяг інформації, який був викладений у статті стосовно позивача (ім'я, попереднє місце проживання, місце отримання

поранення, хто його звільняв з полону, ім'я командира, місце роботи родичів), дозволяє конкретно ідентифікувати особу позивача, тому отримання згоди військовослужбовця на публікацію цих даних було обов'язковим.

О. В Гронь зазначає, що в основу обробки персональних даних покладено низку базових принципів (правила, що повинні дотримуватися (за незначними винятками) будь-яким володільцем у процесі здійснення будь-якої обробки), мета формулювання яких - визначення правових засад її здійснення. Вони формуються на наднаціональному та національному рівнях [50, с. 103].

Ключові принципи у Європейському Союзі були покладені в основу правового захисту персональних даних Директивою 95/46/ЄС [5]. При цьому зміни, які передбачені новим Регламентом (ЄС) 2016/679 [4] про персональні дані, знаменують якісно нову філософію щодо їх охорони із відповідними жорсткими санкціями за порушення його вимог.

Україна, яка поступово інтегрується до ЄС, вже має відповідні базові положення, спрямовані на створення якісної системи правового захисту персональних даних.

Конституцією України статтею 32 зазначається: «Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини» [1]. Саме це - той «базис», спираючись на який «вбудовуються» усі подальші законодавчі норми щодо захисту персональних даних.

Загальновизнаним постулатом правового регулювання у сфері персональних даних є однозначна заборона безпідставної їх обробки. За відсутності належних правових підстав обробка персональних даних вважається порушенням права людини на приватність і є незаконною.

Стаття 11 Закону України «Про захист персональних даних» визначає вичерпний перелік підстав, за наявності яких обробка персональних даних буде законною [10]:

1) згода суб'єкта персональних даних на обробку його персональних даних;

2) дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень;

3) укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на користь суб'єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних;

4) захист життєво важливих інтересів суб'єкта персональних даних;

5) необхідність виконання обов'язку володільця персональних даних, який передбачений законом;

6) необхідність захисту законних інтересів володільця персональних даних або третьої особи, якій передаються персональні дані, крім випадків, коли потреби захисту основоположних прав і свобод суб'єкта персональних даних у зв'язку з обробкою його даних переважають такі інтереси.

Із цього приводу Ю. Д. Бєлова пояснює, що для того, щоб згода фізичної особи була правомірною підставою для обробки персональних даних, вона повинна відповідати умовам дійсності такої згоди. Аналіз законодавства та практики його застосування дозволяє виділити такі чотири умови: добровільність, поінформованість, конкретність, однозначність. Вказані умови застосовуються у сукупності, тобто відсутність однієї з них свідчить про недійсність згоди на обробку персональних даних. Розглянемо умови дійсності згоди більш детально.

Добровільність як умова дійсності згоди означає, що волевиявлення суб'єкта персональних даних має бути вільним і відповідати його внутрішній волі. Таке волевиявлення не може вважатися вільним, якщо вчинено через

помилку, під впливом обману, насильства, тяжкої обставини. Тобто згода є добровільною, якщо суб'єкт персональних даних самостійно вибирає, надавати таку згоду чи ні. Відсутність контролю з боку інших осіб у контексті згоди є ознакою такого вибору. Тобто, якщо відмова надати згоду є практично нездійсненою через те, що вона або є неможливою, або буде мати дуже негативні наслідки для особи, яка надає таку згоду, тоді справжній вибір, як власне і згода, відсутні [39, с. 318].

Поінформованість як умова дійсності згоди знаходить свій прояв у нормативному закріпленні на рівні прав суб'єкта персональних даних (п. 1, 2, 12 ч. 2 ст. 8 Закону України «Про захист персональних даних») та обов'язків володільця персональних даних (ч. 2 ст. 12 Закону України «Про захист персональних даних») [10].

Також Ю. Д. Бєлова зазначає, що поінформованість згоди суб'єкта персональних даних, крім того, має ще два важливих значення. По-перше, поінформованість є передумовою відкритості та прозорості обробки персональних даних, забезпечує контроль суб'єкта персональних даних за їх обробкою. По-друге, зміна обставин обробки персональних даних, відомості про які були надані суб'єкту під час отримання його згоди, ставлять під сумнів поінформованість згоди щодо подальшої обробки персональних даних. Це призводить до необхідності повідомити суб'єкта персональних даних про вказані зміни, а в окремих випадках - отримати нову згоду суб'єкта персональних даних (наприклад, у разі зміни мети) [39, с. 321].

З поінформованістю тісно пов'язана інша умова дійсності згоди, а саме її конкретність, тобто згода повинна визначати мету та конкретні цілі обробки персональних даних.

Для того щоб відстоювати свої права, згідно із Законом України «Про захист персональних даних», суб'єкт персональних даних повинен мати чітке уявлення про:

- мету збору персональних даних (має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших

документах, які регулюють діяльність власника персональних даних, та відповідати законодавству про захист персональних даних);

- володільця персональних даних (фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом);

- розпорядника персональних даних (фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця);

- склад та зміст персональних даних (мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їх обробки) [10].

О. А. Заярний пояснює, що мета обробки персональних даних зумовлює цілі, для реалізації яких може надаватися згода фізичною особою на використання конкретної інформації [56, с. 59].

Зміна визначеної мети обробки персональних даних на нову мету, яка є несумісною з попередньою, тягне за собою необхідність отримати згоду суб'єкта персональних даних на обробку його даних відповідно до зміненої мети. З цього приводу Н. В. Камінська зазначає, що критерій сумісності/несумісності є суто відносним, що створює передумови для його вільного тлумачення як володільцями персональних даних, так і суб'єктами юрисдикційних повноважень. Ця обставина зумовлює ризик маніпуляцій, в ході яких первинна (узгоджена із суб'єктом персональних даних) мета обробки інформації без його згоди може бути змінена на іншу, зовні подібну, але відмінну по суті [57, с. 108]. Прикладом є рішення Європейського суду з прав людини у справі «Deutsche Telekom AG v. Germany» від 05.05.2011 р. [24], яка стосувалася питання необхідності отримувати нову згоду суб’єктів персональних даних при зміні назви третьої особи, якій такі дані передавались. Суд ЄС постановив, що не було необхідності в отриманні нової згоди, тому що суб’єкти персональних даних мали можливість надати згоду тільки для цілей здійснення обробки, які полягали в оприлюдненні їхніх даних, і не могли вибирати між різними адресними книгами, в яких

могли бути надруковані ці дані. Тобто «сумісність» у даному контексті є оціночним поняттям та може бути встановлена щодо кожного випадку окремо.

Окремий складник обізнаності суб'єкта персональних даних – це досконале знання свої прав, які встановлені статтею 8 Закону [10], що дозволяє обґрунтовано та якісно відстоювати свої інтереси у разі, коли персональна інформація стає відомою стороннім особам, тоді, коли це не пов'язано із питаннями державної та громадської безпеки, боротьби з злочинністю, запобіганню правопорушенням та ін.

Наступною умовою дійсності згоди суб'єкта персональних даних є її однозначність. Так, згода повинна бути явно вираженою, зрозумілою та безсумнівною. З цієї ж причини згода повинна, очевидно, походити від конкретного суб'єкта персональних даних, при цьому не залишаючи сумнівів щодо його дозволу на обробку персональних даних.

Ю. Д. Бєлова зазначає, що така вимога змушує володільця персональних даних створювати механізм надання фізичними особами згоди, який би забезпечував, щоб така згода була або безпосередньо виражена, або випливала з поведінки суб'єкта персональних даних. Тобто дії суб'єкта повинні призводити до безпомилкового висновку про надання ним згоди. Однак це залежить від того, наскільки повну, достовірну та своєчасну інформацію отримав суб'єкт персональних даних, яка дала можливість йому прийняти відповідне рішення. При цьому згода суб'єкта персональних даних не може випливати з його бездіяльності чи мовчання, оскільки мовчанню та бездіяльності притаманна неоднозначність. Тому з двох застосовуваних моделей отримання згоди суб'єкта персональних даних «opt out» (яка полягає в тому, що володілець персональних даних не повинен уводити в оману суб'єктів стосовно обробки їхніх даних, а останні, у свою чергу, повинні мати можливість відмовитися від подальшої обробки) та «opt in» (відповідно до якої правомірною є тільки така обробка персональних даних, що

здійснюється після попередньо отриманої згоди суб'єктів персональних даних) стандартам ЄС відповідає лише остання [35, с. 326].

Так, згода суб'єкта персональних даних може бути вчинена в письмовій формі, як правило, у вигляді окремого документа (згода на обробку персональних даних) або як одна з умов договору.

Також Ю. Д. Бєлова вважає, що згода суб'єкта персональних даних може бути надана шляхом конклюдентних дій, тобто якщо його поведінка засвідчує волю на обробку персональних даних, зокрема, шляхом проставлення відмітки про надання дозволу на обробку своїх персональних даних під час реєстрації в інформаційно-телекомунікаційній системі суб'єкта електронної комерції [40, с. 132]. Щодо усної форми згоди, то, фактично, вона не заборонена, однак навряд чи усна форма зможе надати володільцю змогу підтвердити наявність згоди впродовж всього часу здійснення обробки персональних даних. Як вже було встановлено, згода суб'єкта персональних даних не може виражатися її мовчанням. Згода, вчинена у формі, яка не відповідає зазначеним вимогам, не може бути підставою правомірної обробки персональних даних.

Національне законодавство, так само як і стандарти ЄС, не визначають безпосередньо момент, коли згода повинна бути надана. Однак з аналізу та тлумачення окремих положень можна встановити, що згода повинна бути надана до того, як процес обробки персональних даних почнеться. Тобто отримання згоди на обробку персональних даних до початку самої обробки є найголовнішою умовою правомірності такої обробки. При цьому, якщо обробка персональних даних була розпочата без згоди суб'єкта персональних даних, законодавство не надає йому можливість схвалити таку обробку згодом.

Серед основних прав, які були вдосконалені Регламентом (ЄС) 2016/679 [4], варто виділити такі:

1. 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.

2. 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.

Прикладом є справа Європейського Суду з прав людини «Бернх Ларсен Холдінг АС» та інші проти Норвегії» № 24117/08 від 14.03.2013 р. [25], що стосувалася оскарження трьома норвезькими компаніями наказу податкового органу щодо надання податковим аудиторам копії усіх даних з комп'ютерного серверу, яким усі три компанії спільно користувалися.

Європейський Суд з прав людини визнав, що факт вимагання такої інформації від заявника (компанії) є втручанням у його право на повагу до «житла» і «кореспонденції» у значенні статті 8 Конвенції про захист прав людини і основоположних свобод [2]. Проте Суд визнав, що у податкових органів були ефективні та адекватні гарантії проти зловживань: заявника (компанії) було завчасно повідомлено; компанії були на місці і могли відразу подати заперечення проти втручання; матеріал міг бути знищеним після завершення аудиту. За таких обставин було дотримано справедливий баланс між правом заявника (компаній) на повагу до «житла» та «кореспонденції », інтересом заявника щодо захисту приватності осіб, які на нього працюють, з одного боку, та інтересами суспільства щодо забезпечення ефективного аудиту в цілях податкової оцінки, з іншого. Суд постановив, що за цих причин не було порушено статтю 8 [2].

Також необхідно зазначити, що правоохоронні органи не завжди можуть опрацьовувати ваші персональні дані.

Наприклад, рішення Європейського Суду з прав людини «Хелілі проти Швейцарії» № 16188/07 [26]. Під час поліцейського рейду поліція виявила заявницю, у якої були візитки з таким текстом:: «Симпатична, гарна жінка, за тридцять, хотіла б зустріти чоловіка, щоб іноді разом випити або провести час. Номер телефону ...»

Після цього поліцейські внесли в базу її ім'я як повії, якою вона ніколи не була. Європейський Суд з прав людини визнає, що, збереження персональних даних особи на тій підставі, що ця особа могла вчинити інший злочин, може за певних умов бути пропорційним.

Проте у справі заявниці необґрунтоване обвинувачення у незаконній проституції виявилося занадто розпливчастим і загальним і не було обґрунтовано конкретними фактами, оскільки її ніколи не було засуджено за незаконне заняття проституцією, і тому не може розглядатися як таке, що відповідає «нагальній суспільній потребі» у розумінні статті 8 Конвенції про захист прав людини і основоположних свобод [2]. Розглядаючи питання доказування достовірності збережених про заявницю даних як питання, що відноситься до повноважень органів влади, а також серйозності втручання в права заявниці, Суд постановив, що збереження слова «повія» в файлах поліції протягом багатьох років не було необхідним у демократичному суспільстві. Суд дійшов висновку, що було порушено статтю 8 Конвенції про захист прав людини і основоположних свобод [2].

Базовою метою захисту персональних даних повинно бути забезпечення ключових прав та свобод громадян. Організаційно-економічною основою для її реалізації повинен стати відповідний механізм, в якому основою має бути чинний Закон України «Про захист персональних даних» та в який гармонічно будуть імплементовані ключові європейські норми з чітким визначенням норм щодо свободи інформації та захистом персональних даних, а також деталізацією взаємодії та фіксацією відповідальності за порушення норм у сфері захисту персональних даних.

РОЗДІЛ 2
ПРАКТИЧНІ АСПЕКТИ ЦИВІЛЬНО-ПРАВОВОГО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

2.1. Правовий статус суб'єктів правовідносин, які потребують захисту персональних даних

До суб'єктів відносин, пов'язаних з персональними даними, ст. 4 Закону України «Про захист персональних даних» [10] відносить: суб'єкта персональних даних, володільця персональних даних, розпорядника персональних даних, третю особу, Уповноваженого Верховної Ради України з прав людини (далі - Уповноважений з прав людини). При цьому, суб'єкт персональних даних - це фізична особа, якій належить персональна інформація, тобто без нього відносини, пов'язані з персональними даними, фактично, втрачають сенс.

Відповідно до статті 8 Закону України «Про захист персональних даних» [10] суб'єкт персональних даних має право: знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки; отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані; мають право на доступ до своїх персональних даних; пред'являти обґрунтовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних чи щодо зміни або знищення своїх персональних даних; відкликати згоду на обробку персональних даних; знати механізм автоматичної обробки персональних даних.

В. І. Теремецький зазначає, що володілець і розпорядник є суб'єктами, які безпосередньо здійснюють обробку та захист персональних даних, а отже на них покладено важливі функції у цих правовідносинах. Слід зауважити, що розпорядник є суб'єктом, участь якого може мати факультативний характер, тобто володілець може взагалі його не залучати до обробки або

делегувати функцію обробки та захисту персональних даних на договірних засадах. Третьою особою можуть виступати органи влади, діяльність яких потребує використання персональних даних фізичної особи. В основному це центральні та територіальні органи виконавчої влади, а також правоохоронні органи, які використовують відомості про особу для потреб державного управління і забезпечення законності та правопорядку в державі. Уповноважений з прав людини є суб'єктом, який у правовідносинах представляє інтереси держави, а його повноваження переважно спрямовані на забезпечення законності при обробці та захисті персональних даних [86, с. 172].

Важливе значення має дослідження правового статусу таких суб'єктів, як володілець та розпорядник персональних даних, оскільки вони є обов'язковими учасниками правовідносин у сфері захисту персональних даних. Відповідно до ст. 2 закону України «Про захист персональних даних» володілець персональних даних - це фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом [10]. Отже, володілець є важливим суб'єктом правовідносин, який безпосередньо здійснює обробку персональних даних та визначає її мету. Виходячи з положень законодавства, володільців можна поділити на фізичних та юридичних осіб, при цьому фізична особа - це, наприклад, приватний підприємець, який самостійно обробляє персональні дані своїх працівників, а юридична особа - це підприємство, установа чи організація, яка також здійснює обробку персональних даних фізичних осіб [10].

Також В. І. Теремецький зауважує, що правовий статус володільця та розпорядника персональних даних, регламентований вітчизняним законодавством, не в достатній мірі відповідає вимогам законодавства країн Європейського Союзу. Зокрема, є певні суперечності стосовно умов здійснення обробки персональних даних вказаними учасниками

правовідносин та нормативно-правового закріплення основ здійснення ними своїх повноважень [86, с. 174].

Дослідження суб'єктів відносин, пов'язаних з обробкою персональних даних, вимагає також аналізу статусу третьої особи як учасника цих правовідносин. У законодавстві вказаний суб'єкт визначається як будь-яка особа, за винятком суб'єкта персональних даних, володільця чи розпорядника персональних даних та Уповноваженого з прав людини, якій володільцем чи розпорядником персональних даних здійснюється передача персональних даних [10, ст. 2]. Аналізуючи вказане положення, можна зробити висновок, що третя особа - це суб'єкт, який не обробляє персональні дані, не укладає жодних договорів стосовно них, а лише отримує відомості про фізичну особу використання з відповідною метою. Потреба використання персональних даних такими учасниками правовідносин обумовлена особливостями сфери державного управління та сфери господарювання, які передбачають оперування відомостями про особу. Враховуючи наведене, виникає потреба розмежування третьої особи як представника владно-розпорядчої діяльності та представника господарської діяльності. До представників владно-розпорядчої діяльності слід віднести податкові та митні органи, органи статистики, органи Пенсійного фонду, правоохоронні та судові органи тощо. До представників господарської діяльності належать страхові компанії, банківські та кредитні установи, оператори мобільного зв'язку та ін.

М. В. Різак підкреслює, що становище третьої особи у відносинах, пов'язаних з персональними даними, має дві істотні особливості, які визначають індивідуальність цього суб'єкта. По-перше, третя особа отримує відомості про фізичну особу не від самого суб'єкта персональних даних, а від володільця або розпорядника. Завдяки цьому третя особа - єдиний суб'єкт, який може використовувати персональні дані навіть без згоди самої фізичної особи. По-друге, мета обробки персональних даних третьою особою не співпадає з метою обробки таких даних володільцем чи розпорядником, які їх надають [75, с. 621]. Наприклад, якщо вищий навчальний заклад обробляє

персональні дані студентів з метою їх обліку або нарахування стипендії, то органи внутрішніх справ можуть отримати ці дані від закладу та використати їх для ідентифікації особи в рамках оперативно-розшукової діяльності.

Отже, третя особа є факультативним суб'єктом відносин, пов'язаних з персональними даними, тому закріплення її правового статусу в законодавстві є необхідним. Вбачається, що зазначений суб'єкт має важливе значення для сфери державного управління, оскільки персоніфікована інформація здебільшого використовується саме в інтересах цієї сфери, ніж для потреб володільця.

В. І. Теремецький запропонував поділити суб'єктів відносин, пов'язаних з персональними даними за спрямованістю, на три основні групи:

1) суб'єкт персональних даних, тобто особа, якій належать персональні дані, та особи, які дають згоду на обробку персональних даних суб'єкта (батьки, опікуни, піклувальники та ін.). До цієї групи доцільно віднести тільки осіб, яким прямо чи опосередковано належать права на персональні дані;

2) суб'єкти, які здійснюють обробку персональних даних, тобто володілець і розпорядник персональних даних. Ця група суб'єктів характеризується тим, що їм не належить право на персональні дані, адже вони лише виконують певні операції з цими відомостями відповідно до встановленої мети. Вбачається, що до цієї групи також слід віднести третю особу як суб'єкта відносин, пов'язаних з персональними даними, адже фактично вона здійснює обробку відомостей про особу, але з іншою метою;

3) суб'єкти забезпечення захисту персональних даних (наприклад, Уповноважений з прав людини) [86, с. 172].

Згідно із статтею 23 Закону України «Про захист персональних даних» [10] Уповноважений з прав людини у сфері захисту персональних даних має багато повноважень, але в основному вони носять декларативний характер. Він має право отримувати пропозиції, скарги та інші звернення фізичних і юридичних осіб з питань захисту персональних даних. Але, якщо

враховувати кількість скарг, які надходять до нього, то просто неможливо детально всі їх розглянути та врахувати обставини подій, які сталися при вчинення порушення прав на захист персональних даних, а також приймати обґрунтовані рішення за результатами їх розгляду. З тих самих причин Уповноваженому з прав людини, навіть при наявності певної кількості підлеглих фізично неможливо проводити на підставі звернень або за власною ініціативою виїзні та безвиїзні, планові, позапланові перевірки володільців або розпорядників персональних даних.

М. В. Різак вказує, що за підсумками перевірки, розгляду звернення Уповноважений має право видавати обов'язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних. Але в нашій країні ще не має чіткого механізму здійснення контролю за чітким виконанням даних приписів [75, с. 623].

З метою забезпечення виконання Уповноваженим з прав людини функцій контролю за виконанням законодавства в сфері захисту персональних даних в Секретаріаті Уповноваженого Верховної Ради України з прав людини створено Департамент з питань захисту персональних даних. Однак, автор вважає, що Уповноважений Верховної Ради України з прав людини не повинен розцінюватися як суб’єкт таких відносин і виконувати постійно діючу функцію щодо забезпечення законності при обробці та захист персональних даних, оскільки: 1) штат цієї посадової особи не здатен виконувати відповідну функцію через величезний обсяг інформації, яка може кваліфікуватися як персональні дані; 2) безпосередніх заходів щодо впливу на правопорушників ця посадова особа не має, оскільки перелічені вище повноваження мають декларативний характер, тому її функції не можуть розцінюватися як альтернатива зверненню до суду; 3) функції представництва інтересів осіб, які постраждали при обробці персональних даних мають бути закладені у Цивільний процесуальний кодекс України [7]. Створення ж Департаменту з питань захисту персональних даних можна асоціювати зі спробою перетворити Уповноваженого Верховної Ради

України з прав людини на постійно діючий механізм державної влади – адміністративний орган, але його функції, на наш погляд, полягають у контролі за діяльністю органів державної влади щодо недопущення порушення прав людини.

2.2. Методи та форми захисту персональних даних

Поняття захисту персональних даних є доволі широким та, зазвичай, включає два ключових елемента. Перш за все, це зобов'язання володільця вживати організаційних та технічних заходів з метою запобігання їх випадкової втрати або знищення, незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних (стаття 24) [10]. По-друге, це зобов'язання кожного працівника володільця та розпорядника не допускати розголошення персональних даних, які стали йому відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, так зване зобов'язання конфіденційності (стаття 10) [10].

Володілець персональних даних самостійно повинен визначати, яких заходів слід вживати з метою забезпечення захисту персональних даних. При цьому слід враховувати вимоги законодавства у сфері захисту персональних даних та інформаційної безпеки. Вказана вимога стосується усіх володільців. Перелік обов'язкових заходів захисту, які повинні вживатися всіма володільцями, визначено Типовим порядком обробки персональних даних, затвердженим наказом Уповноваженого від 08.01.2014 № 1/02-14 [20]. Ці вимоги носять загальний характер і є мінімальними вимогами у сфері захисту персональних даних, а шляхи їх практичної імплементації вирішуються в індивідуальному порядку кожним окремим володільцем.

Згідно з пунктом 3.4 Типового порядку обробки персональних даних організаційні заходи охоплюють:

- визначення порядку доступу до персональних даних працівників володільця/розпорядника;

- визначення порядку ведення обліку операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них;

- розробку плану дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій;

- регулярне навчання співробітників, які працюють з персональними даними [20].

Відповідно до зазначеного Типового порядку володілець/розпорядник веде облік працівників, які мають доступ до персональних даних суб'єктів. Володілець/розпорядник визначає рівень доступу зазначених працівників до персональних даних суб'єктів. Кожен із цих працівників користується доступом лише до тих персональних даних (їх частини) суб'єктів, які необхідні йому у зв'язку з виконанням своїх професійних чи службових або трудових обов'язків.

Працівники, які мають доступ до персональних даних, дають письмове зобов'язання про нерозголошення персональних даних, які їм було довірено або які стали їм відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків [20].

Стрімкий розвиток соціальної активності та необдумане бажання висвітлити інформацію про цікаві події у соціальних мережах може спричинити порушення законодавства про захист персональних даних осіб. Кожна посадова особа повинна розуміти ту відповідальність, яка на неї покладається, коли їй дається доступ до обробки персональних даних осіб, і бути готовою до наслідків, при вчиненні неправомірних дій.

Наприклад, рішенням Господарського суду м. Києва від 11 грудня 2018 р. по справі № 910/6647/18 [30] визнано недостовірною та такою, що порушує особисте немайнове право інформацію, оприлюднену та поширену відповідачем на веб-сайті «Актуальна правда» (http://apravda.com) та на

власному YouTube-каналі, зобов'язано спростувати поширену ним недостовірну інформацію та видалити її з веб-сайту «Актуальна правда» (http://apravda.com) та з веб-сайту «Youtube» (http://youtube.com), з відповідача стягнуто 125000 гривень збитків, 7 161 гривень витрат на оплату судового збору та 98 340 гривень інших судових витрат.

Кожна посадова особа повинна розуміти ту відповідальність, яка на неї покладається, коли їй дається доступ до обробки персональних даних осіб, і бути готовою до наслідків, при вчиненні неправомірних дій.

І. М. Бем зазначає, що у разі звільнення працівника, який мав доступ до персональних даних, або переведення його на іншу посаду, що не передбачає роботу з персональними даними суб'єктів, вживаються заходи щодо унеможливлення доступу такої особи до персональних даних, а документи та інші носії, що містять персональні дані суб'єктів, передаються іншому працівнику [37, с. 86].

Таким чином, перш за все, володілець повинен забезпечити, щоб до персональних даних мали доступ лише ті працівники, які з ними працюють. Кожному з таких працівників повинен надаватися доступ до тих даних, які йому необхідні у зв'язку з виконанням його службових обов'язків. Окрім цього, володілець повинен зберігати інформацію/документи щодо того, які працівники та впродовж якого часу мали доступ до тих чи інших персональних даних. Такі заходи необхідні для того, щоб у разі поширення, втрати, знищення персональних даних звузити коло осіб, що можуть бути до цього причетними. Для цього, володільцю (в залежності від масштабу діяльності, кількості працівників володільця) доцільно визначити типові рівні доступу.

Також І. М. Бем пояснює, що перед отриманням доступу до персональних даних кожен працівник повинен пройти процедуру ідентифікації/автентифікації, зокрема шляхом особистого введення індивідуального та відомого лише йому паролю (чи іншим способом, наприклад шляхом використання індивідуальної картки з вбудованою

мікросхемою, яка автоматичну запускає визначені для конкретного користувача налаштування та ін.). Це повинно забезпечити, що лише визначений працівник зможе працювати за певним робочим місцем чи за будь-яким робочим місцем, однак із визначеними особисто для нього налаштуваннями доступу до персональних даних. Окрім цього, це дасть змогу ідентифікувати працівників, які працюють в системі, за допомогою присвоєного ними ідентифікатора [35, с. 107].

Прикладом є рішення Європейського Суду з прав людини у справі «Суріков проти України» від 26 січня 2017 року [26]. Роботодавець заявника довільно збирав, зберігав та використовував дані стосовно його психічного здоров'я у зв'язку із заявою останнього про підвищення, а також відкрив ці дані колегам заявника та суду в ході відкритого розгляду справи.

Законодавство дозволяло зберігання даних стосовно здоров'я заявника протягом тривалого часу та дозволяло її оприлюднення та використання для цілей, які не відповідали початковій меті їх збору. Європейський суд з прав людини вказав, що це непропорційне втручання в право заявника, що не було необхідним у демократичному суспільстві, тому є порушення.

Персональні дані, залежно від способу їх зберігання (паперові, електронні носії), мають оброблятися у такий спосіб, щоб унеможливити доступ до них сторонніх осіб.

А. Л. Петрицький зазначає, що з метою забезпечення безпеки обробки персональних даних вживаються спеціальні технічні заходи захисту, у тому числі щодо виключення несанкціонованого доступу до персональних даних, що обробляються та роботі технічного та програмного комплексу, за допомогою якого здійснюється обробка персональних даних [68, с. 194].

Володілець може здійснювати контроль доступу до приміщень, де зберігаються картотеки/сервери з персональними даними, та робочих приміщень загалом. Залежно від важливості інформації, що зберігається в базі даних, приміщення можуть обладнуватися автоматичними електронними замками, сигналізацією, ґратами на вікнах та дверях тощо. В якості

додаткового заходу безпеки володільці можуть (з дотриманням певних гарантій) із метою контролю за виробничою дисципліною, дотриманням правил трудової етики здійснювати відеоспостереження за працівниками.

Якщо володільцем здійснюється автоматизована обробка персональних даних, рекомендується вжити заходів щодо створення резервної копії інформації, антивірусного захисту, захисту каналів передачі інформації (криптографічного, фізичного) від несанкціонованого втручання.

Відповідно до вимог нового Регламенту ЄС про захист даних (GDPR) організації повинні: передавати дані тільки авторизованим особам, забезпечити точність та цілісність даних, мінімізувати розкриття особистості суб'єкта, застосовувати заходи із убезпечення даних [4].

Шифрування – це саме той метод, при якому дані знаходяться в нечитабельному вигляді, якщо тільки користувач або процес не надасть відповідний ключ. Відповідно до Регламенту ЄС про захист даних, цей простий метод може забезпечити доступ до персональних даних тільки авторизованим користувачам, а також контролювати час, протягом якого цей доступ може бути здійснений.

О. О. Шевчук відзначає, що багатофакторна автентифікація – ще один метод, що забезпечує надійну авторизацію об'єкта, який здійснює обробку конфіденційних даних, а також значно зменшує ризики доступу неавторизованих користувачів до персональних даних [92, с. 167].

Регламент ЄС про захист даних (GDPR) спеціально вказує на шифрування, як на основну вимогу безпеки даних. Крім того, організаціям потрібно провести оцінку ризиків, а потім прийняти заходи, що пом'якшують ризики, які вони виявлять. Оскільки жодна організація не може повністю визначити або передбачити всі ризики для своїх даних, і жоден підхід до периметра безпеки не є надійним, організації повинні шифрувати свої дані, щоб забезпечити відповідність до GDPR. За допомогою шифрування неважливо, чи є порушення – дані будуть належно захищені. Навіть після того, як дані вже зібрані, суб'єкти даних все одно мають певний контроль над

цими даними. "Право на видалення" розглядається у статтях 17 та 28 [4]. Регламент ЄС про захист даних (GDPR) вимагає від організацій повністю видалити дані з усіх сховищ в разі, якщо: користувач відкликає свої дані, партнерська організація вимагає видалення персональних даних своїх користувачів, що були наданні для обробки, термін дії угоди про використання персональних даних скінчився [4].

Згідно цієї норми, передбачаються випадки, коли організація повинна буде забезпечити повне видалення персональних даних своїх користувачів. Це дуже складна вимога, тому що навіть після видалення дані все-одно зберігаються на магнітних носіях інформації. Але щоб повністю відповісти нормі, організації можуть шифрувати дані, а потім видалити тільки ключ шифрування. Цей метод перетворює дані в повністю і назавжди нечитабельний масив інформації.

Організації повинні самостійно оцінювати ризики, що пов’язані з конфіденційністю та безпекою даних, а також демонструвати, що вони вживають всіх відповідних заходів з урахуванням зроблених ними висновків. Ці обов'язки викладені у статтях 2, 24 та 28 Регламенту ЄС про захист даних (GDPR) [4].

Коли порушення безпеки загрожує правам та конфіденційності суб'єкта даних, організаціям необхідно повідомити клієнтів та їх наглядовий орган. В рамках GDPR організації зобов'язані:

- повідомити свій наглядовий орган протягом 72 годин
- описати наслідки порушення безпеки даних
- повідомити про порушення безпосередньо суб'єктів даних) [4].

М. В .Бем зазначає, якщо у результаті витоку розкриваються незахищені дані, організація зобов’язана повідомити місцевий орган нагляду та клієнта, що постраждав. Проте у випадку, якщо дані зашифровані та використовуються найкращі методи управління ключами шифрування, організація позбувається потреби у таких повідомленнях [34, с. 248].

2.3. Перспективи вдосконалення законодавства про захист персональних даних

Як вже зазначалося, 25 травня 2018 р. набув чинності загальний регламент захисту персональних даних (GDPR, General Data Protection Regulation) - відповідна інструкція про захист даних, або нові правила захисту персональних даних, прийняті Євросоюзом [34, с. 239].

Беззаперечно можна визнати, що оновлення законодавства в сфері захисту персональних даних спрямовані на те, щоб люди мали змогу керувати потоками власних даних, усвідомлювали можливості, які виникають внаслідок їх збору, обробки та подальшого продажу, а головне – могли захистити свою приватність.

В більшості випадків люди не розуміють небезпеки та шкоди від витоків персональних даних, оскільки максимальну незручність, яку ми можемо уявити – це постійні рекламні повідомлення від служб таксі та інших компаній. Проте використання персональної інформації надасть змогу її розпорядникам знати ваше місцезнаходження, впізнавати вас в обличчя, користуватись вашими реквізитами не лише в комерційних, а й злочинних цілях. Саме тому постійні неправомірні порушення приватності особи змушують зрозуміти, що необхідно докладати більше зусиль для власного захисту. І це повинно організовуватися та регулюватися не тільки на державному рівні, а й на персональному.

М. І. Саєнко пояснює, що надання суб'єктом персональних даних письмової згоди на збір, обробку, використання таких даних, яка була впроваджена згідно із Законом України «Про захист персональних даних», на перший погляд, є логічним кроком, коли особа сама вирішує, хто, коли і в якому обсязі зможе обробляти її персональні дані. Проте поточна практика ставить питання в доцільності застосування такої згоди (принаймні, у тому форматі, що передбачений чинним законодавством) та пошуках більш оптимальних механізмів [81, с. 105].

Основна проблема виникає вже на початковому етапі надання згоди на обробку персональних даних. У особи, зазвичай, немає можливості змінити текст «згоди на обробку персональних даних», наприклад, обмеживши можливість передачі інформації третім особам або визначивши час, після якого персональні дані мають бути видалені. Крім цього, у більшості випадків немає можливості скористатися відповідною послугою, взагалі без надання згоди на обробку персональних даних.

Також М. І. Саєнко зазначає, що компаніям, які збирають та ведуть бази персональних даних своїх клієнтів, зручно просити надати згоду «одразу на все», щоб у випадку реорганізації чи змін у бізнес-процесах (наприклад, передача функцій із ведення клієнтської бази на аутсорсинг), робота з базами даних залишалась формально санкціонованою [81, с. 106].

Законодавство і рекомендації Уповноваженого Верховної Ради України з прав людини вказують на те, що згода на обробку персональних даних повинна бути пропорційною меті обробки; і навіть якщо особа надала згоду на обробку персональних даних, частина з яких по своїй суті не потрібна для досягнення поставленої мети обробки, то така обробка розглядатиметься як непропорційна та становитиме порушення законодавства про захист персональних даних. Разом із тим, враховуючи, що суди часто схиляються до формалізму, буде важко довести незаконність обробки надмірного обсягу персональних даних в умовах, коли особа добровільно надала свою згоду, підписавши відповідний бланк.

Замовляючи товари і послуги, пересічна особа вимушена регулярно підписувати бланки згоди на обробку своїх персональних даних. У результаті, практично кожен опиняється в ситуації, коли його рукою підписані сотні «згод на обробку персональних даних», часто з надмірним обсягом повноважень щодо їхньої обробки та використання, проте немає жодної можливості згадати і встановити всіх суб’єктів, яким така згода була надана.

Існування вимоги закону про підписання згоди на обробку персональних даних не заважає недобросовісному поширенню персональних даних. У публічному доступі безперешкодно циркулюють т.зв. «телефонні довідники», в яких можна знайти повне ім'я, адресу, телефон та дату народження фактично будь-якого громадянина України. Залишається актуальною проблемою розсилка небажаних повідомлень (через SMS-повідомлення, електронну пошту).

На наш погляд, необхідно на законодавчому рівні більш жорстоко контролювати використання та розповсюдження інформації про персональні дані працівниками банківських установ. В даний час дуже велика кількість скарг громадян України на те, що їх персональні дані передаються в колекторські контори з ціллю повернення кредитних грошей. Так, є випадки, коли дійсно фізична особа бере велику суму грошей та не повертає її вчасно, при цьому підписує стандартну форму на дозвіл опрацювання особистих даних і передачу їх третім особам. Разом з цим, статтею 512 Цивільного кодексу України визначені підстави заміни кредитора у зобов'язанні [6]. За однією з таких підстав кредитор у зобов'язанні може бути замінений іншою особою внаслідок передавання ним своїх прав іншій особі за правочином. Крім того, статтею 516 Цивільного кодексу України також встановлено, що заміна кредитора у зобов'язанні здійснюється без згоди боржника, якщо інше не встановлено відповідним договором або законом [6].

В дійсності виникають ситуації, коли банківські установи передають персональні дані боржників, а також інформацію про історію платежів та переказів клієнта. Використовуючи цю інформацію, співробітники банків та колекторських контор отримують дані родичів та друзів особи, яка користується кредитним рахунком. На жаль, такі випадки не поодинокі і ніхто не несе відповідальності за розповсюдження персональних даних, навіть банківські установи.

Уповноважений Верховної Ради України з прав людини вказав, що чинним законодавством діяльність колекторських фірм не регламентована,

але згідно зі ст. 42 Конституції [1] кожному гарантовано право на підприємницьку діяльність, не заборонену законом. В даний час обговорюються два варіанти регламентації діяльності колекторських фірм – це законопроекти «Про колекторську діяльність» та «Про запровадження ліцензування колекторської діяльності».

За Законом України «Про банки і банківську діяльність» інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третіми особами при наданні послуг банку і розголошення якої може завдати матеріальної чи моральної шкоди клієнту, є банківською таємницею (стаття 60) [15].

У частині передачі (розкриття) персональних даних клієнтів Банк зобов'язаний дотримуватися режиму банківської таємниці відповідно до ст. 1076 Цивільного кодексу України [6] та ст. ст. 61-62 Закону України «Про банки і банківську діяльність» [15] і тому зобов'язаний зберігати таємність всієї інформації, пов'язаної з клієнтами, і відомості щодо діяльності та фінансового стану клієнтів, яка стала відомими Банку в процесі обслуговування клієнта та взаємовідносин з ним. Банк може розкривати персональні дані лише у тому випадку, якщо суб’єкт персональних даних-клієнт, який є власником цієї інформації, надав Банку згоду на її розкриття, або якщо Банк відповідно до законодавства зобов'язаний здійснити розкриття такої інформації [15]. Отримувачами персональних даних клієнтів Банку, які є банківською таємницею, можуть бути особи та державні органи, які відповідно до законодавства мають право вимагати від банків розкриття цієї інформації.

Стаття 62 зазначеного Закону містить виключний перелік підстав, які дозволяють банку розкривати інформацію, що становить банківську таємницю. Так, однією з підстав, за умови наявності якої розкривається банківська таємниця, є письмовий запит або письмовий дозвіл власника такої інформації. Тобто, банки мають право надавати інформацію, яка становить

банківську таємницю, у порядку та у спосіб, встановлений статтею Закону України «Про банки і банківську діяльність» [15].

У зв'язку з цим, на думку Міністерства юстиції України, залучення банками "колекторських" організацій для вимагання виконання зобов'язань боржниками за кредитними договорами можливо лише за наявності письмового запиту або письмового дозволу боржника на розкриття банківської таємниці. За інших умов така діяльність порушує права та охоронювані законом інтереси громадян і може кваліфікуватися як злочин, передбачений, зокрема, статтею 182 Кримінального кодексу України [8], що передбачає відповідальність за порушення недоторканності приватного життя, статтею 189 - за вимагання, статтею 355 – за примушування до виконання чи невиконання цивільно-правових зобов'язань [72].

Слід звернути увагу, що часто у відносинах щодо надання згоди на обробку персональних даних виступають нерівні за економічною силою суб'єкти (наприклад, окремий громадянин із однієї сторони, та популярна соціальна мережа – з іншої). У таких випадках завданням законодавства є встановити умови та запобіжники зловживанням із боку більш економічно сильної сторони, аналогічно до того, як передбачені умови договорів із суб'єктами природних монополій, регульовані ціни тощо.

За словами С. С. Виноградова, що стосується захисту персональних даних, то доцільно законодавчо визначити критерії пропорційності між змістом згоди на обробку персональних даних та метою їх обробки (за відсутності дотримання яких згода на обробку персональних даних не буде вважатись дійсною), передбачити допустимі напрямки використання персональних даних, встановити стандарти доведення вини та методики визначення завданої шкоди у випадках «витоку інформації» чи іншого незаконного використання персональних даних [46, с. 649].

Інакше, в сьогоденних умовах «добровільна згода на обробку персональних даних» є лише формальністю і дає право великим компаніям

використовувати персональну інформацію про суб'єкта, але не гарантує захист його прав.

Практика судових рішень щодо предметного розгляду справ про витоки інформації з баз персональних даних, про несанкціонований збір та використання персональних даних, про оскарження непропорційності та надмірності існуючих баз персональних даних та вирішення спорів на користь позивача (звичайного пересічного громадянина) дуже мала. В той же час практика застосування законодавства про захист персональних даних на користь держслужбовців зустрічається частіше.

Наприклад, на необхідність захисту персональних даних нерідко посилаються держслужбовці, намагаючись уникнути виконання обов'язку розголошення інформації та оприлюднення документів.

Відповідно до Постанови Верховного Суду від 08.02.2019 року № 855/17/19 та № А/9901/15/19, [27, 28] судами було відмовлено в задоволенні позову 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, а також дій Центральної виборчої комісії щодо зобов'язання кандидата на пост Президента України Гриценка А. С. перевіряти повноту та достовірність персональних даних Реєстру виключно в приміщенні та з обладнанням Комісії, зобов'язання Центральної виборчої комісії надати кандидату на пост Президента України Гриценку А. С. електронної копії бази даних Реєстру з можливістю доступу до такої з його обладнанням у будь-якому місці (приміщенні). Суд дійшов висновку, що надання позивачу електронної копії бази даних Реєстру разом із програмним забезпеченням для перегляду цієї копії у неконтрольованому та незахищеному просторі, поза межами приміщення Комісії, унеможливить забезпечення нею як розпорядником Реєстру законності і пріоритету прав людини, а також захищеності його

відомостей, а отже, призведе до порушення вимог Конституції України, законів про захист інформації, а також міжнародних договорів у цій сфері.

В іншій справі згідно з Постановою Київського апеляційного адміністративного суду від 26.04.2018 року справа № 826/15225/17 [31] були визнані правомірними дії Адміністрації Президента України, що відмовилася надати Указ Президента України про втрату громадянства України, посилаючись на необхідність захисту персональних даних. Суд встановив, що станом на час надіслання позивачем запиту на отримання публічної інформації (липень 2017 року), особа, про яку йшлося в запиті, не займала посаду, пов'язану з виконанням функцій держави або органів місцевого самоврядування; інформація про згоду особи на оприлюднення її персональних даних відсутня. Також суд врахував, що обмеженню доступу підлягає інформація, а не документ (тобто, якщо документ містить інформацію з обмеженим доступом, для ознайомлення надається інформація, доступ до якої необмежений). Разом із тим, було зазначено, що в Указах Президента України про прийняття до громадянства України або припинення громадянства України за вирахуванням персональних даних про осіб, яких вони стосуються, не залишається іншої публічної інформації, що могла б бути оприлюднена.

І. М. Сопілко зазначає, що за відсутності реального контролю та невідворотної відповідальності за «витоки інформації» з баз персональних даних, випадки незаконного доступу і поширення персональних даних продовжуються. В цих умовах встановлений законом механізм надання «згоди на обробку персональних даних» не досягає запланованої мети обмежити втручання у приватне життя особи, натомість, навпаки створює додаткові проблеми, покладаючи зайві обов'язки на бізнес та санкціонуючи (за формальної згоди самої особи) загалом невизначене коло суб'єктів на найширші повноваження щодо збирання та обробки персональних даних [84, с. 68].

Висуваються пропозиції стосовно посилення спроможності наглядового органу щодо захисту персональних даних у світовій мережі Інтернет. Незаконне поширення персональних даних у мережі Інтернет залишається практично безкарним, оскільки особу, яка поширила персональні дані, як правило, просто неможливо встановити, оскільки доменне ім'я сайта, на якому незаконно поширені персональні дані, зареєстроване зазвичай в іншій державі. Більше того, інформація, надана хостинг-провайдером щодо особи, яка зареєструвала доменне ім'я, також не завжди відповідає дійсності. Проте в зарубіжних країнах у таких випадках є можливість заблокувати доступ до веб-сторінки чи видалити її. Сьогодні в Україні не існує спеціальних юридичних механізмів такого характеру. Як наслідок, ні встановити особу, яка причетна до незаконного поширення інформації, ні заблокувати доступ до такої інформації немає можливості.

Сьогодні 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.

На думку К. С. Мельника, запропонована сьогодні державна модель покладення повноважень у сфері захисту персональних даних на Уповноваженого Верховної Ради України з прав людини та закріплення за ним функцій контролю за додержанням вимог законодавства у сфері захисту персональних даних не відповідає існуючій в ЄС моделі діяльності національного уповноваженого органу в цій сфері [65, с. 12].

А. Л. Петрицький пропонує створити в структурі Міністерства юстиції спеціальний підрозділ з питань управління та координації у сфері захисту персональних даних; збільшити штатну чисельність Департаменту з питань захисту персональних даних Секретаріату Уповноваженого Верховної Ради України з питань захисту прав людини до показників, зумовлених

об’єктивними потребами практики; здійснити чітке розмежування функцій, повноважень і меж компетенції суб’єктів, задіяних у формуванні та реалізації державної політики в сфері захисту персональних даних [69, с. 5-6].

З метою подальшого розвитку вітчизняного законодавства щодо відповідальності за порушення стандартів захисту персональних даних та приведення його у відповідність до чинних стандартів ЄС необхідно внести зміни у правове регулювання із таких напрямів:

1) надати більш чітке визначення згоди на обробку персональних даних. У статті 2 Закону України «Про захист персональних даних» [10] надано визначення поняття «згода», де вказано, що передумовою її надання є «поінформованість» суб'єкта персональних даних. У цьому випадку така «поінформованість» передбачає виконання володільцем персональних даних положень статті 12 Закону [10] щодо надання суб'єкту персональних даних завчасно інформації, необхідної для прийняття рішення про надання згоди на обробку його персональних даних. Проте, це явно не визначено у зазначеному Законі. Це положення повинно бути чітко зазначене та обов’язково виконуватися. Особливо це стосується по відношенню до людей похилого віку та малозабезпечених (соціально незахищених) верст населення. Так як люди похилого віку не завжди розуміють всі наслідки, які можуть виникнути під час передачі персональних даних, то найчастіше саме вони стають жертвами шахраїв в економічних махінаціях. Крім цього, у Законі слід прямо визначити, що тягар доведення того, що суб'єкт надав згоду на обробку персональних даних лежить саме на володільці.

2) потрібно ввести окреме положення до статті 10 Закону України «Про захист персональних даних», яким зобов'язати власника та розпорядника персональних даних вести облік операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них, та з цією метою зберігати інформацію про те, хто (зокрема, з працівників чи ін.), коли та з якою метою здійснював збір, зміну, перегляд, передачу (у такому випадку кому), видалення (знищення) персональних даних.

3) удосконалити перелік фактичних підстав відповідальності за порушення стандартів захисту персональних даних. Також необхідно окремо надати детальне роз'яснення можливих ситуацій порушення стандартів захисту персональних даних в таких сферах, як банківська справа, діяльність державних організацій, соціальні мережі, он-лайн комерція та ін.

4) вдосконалити законодавчі норми, що регулюють відповідальність за порушення відповідних стандартів захисту персональних даних. Необхідно чітко визначити, які саме наслідки можуть виникнути після оприлюднення персональних даних та рівень відповідальності, яку несуть відповідальні особи. Потрібно чітко встановити систему штрафів, та визначити рівень компенсації за моральну шкоду.

5) необхідно на законодавчому рівні врегулювати діяльність інституційної системи притягнення до відповідальності та покращити контроль за діяльністю власників баз персональних даних. Окрім проведення перевірок і накладення штрафів уповноважений має володіти більш ефективним арсеналом правових засобів щодо нагляду у відповідній сфері. Для цього необхідно наділити його правом вимагати від порушника, а також звертатися до суду з вимогою в найкоротший строк припинити порушення права на недоторканність приватного життя в сфері персональних даних, можливістю блокування Інтернет-ресурсів у судовому порядку. Потрібно також вдосконалити процедуру повідомлення про обробку бази персональних даних – повідомлення має здійснювати перед початком відповідних операцій тощо.

8) також потрібно розглянути необхідність розробки кодексів у сфері захисту персональних даних, особливо зважаючи на те, що набрав чинності Загальний регламент ЄС «GDPR».

На нашу думку, ці зміни допоможуть більш ефективно захистити відповідні права та інтереси громадян України, а також сприятимуть подальшій інтеграції України у правовий простір ЄС.

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

Результати проведеного дослідження щодо цивільно-правового захисту персональних даних дають підставу зробити такі висновки:

1. На підставі аналізу діючого законодавства персональною конфіденційною інформацією про фізичну особу є дані про її місце проживання та реєстрації, дату і місце народження, національність, релігійні переконання, освіту, сімейний стан, а також стан здоров'я. До конфіденційної відноситься також інформація, доступ до якої обмежено власне фізичною або юридичною особою, крім суб'єктів владних повноважень. Персональна інформація особи може поширюватися тільки за її згодою, за умовами і порядком, визначених нею, а також в інших випадках, визначених законом.

2. Також в роботі були розкриті ознаки баз персональних даних та зазначено, що в них систематизовано персональні дані в електронній формі або у формі картотек. На законодавчому рівні визначено, що база персональних даних обов’язково повинна реєструватися, розміщуватися, упорядковуватися і зберігатися таким чином, щоб забезпечити максимальний захист персональних даних осіб. Однак, слід зауважити, що документи нотаріального діловодства та архів нотаріуса не являються базою персональних даних та не підлягають державній реєстрації.

3. Зазначено, що до обробки персональних даних відносяться будь-які дії такі, як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання, розповсюдження, реалізація, передача, знищення, у тому числі з використанням інформаційних систем. Визначено підстави та вимоги до обробки персональних даних. Отримання згоди на обробку персональних даних до початку самої обробки є найголовнішою умовою правомірності такої обробки.

4. В роботі встановлено, що до суб'єктів відносин, пов'язаних з персональними даними відносяться: особа, якій належать персональні дані,

та особи, які дають згоду на обробку персональних даних суб'єкта; суб'єкти, які здійснюють обробку персональних даних, тобто володілець і розпорядник персональних даних; суб'єкти забезпечення захисту персональних даних. Контроль за додержанням законодавства про захист персональних даних у межах повноважень, передбачених законом, здійснює Уповноважений Верховної Ради України з прав людини. Однак, на нашу думку, потрібно зауважити, що Уповноважений з прав людини не повинен розцінюватися як суб'єкт таких відносин і виконувати постійно діючу функцію щодо забезпечення законності при обробці та захист персональних даних, оскільки: штат цієї посадової особи не здатен виконувати відповідну функцію через величезний обсяг інформації, яка може кваліфікуватися як персональні дані; безпосередніх заходів щодо впливу на правопорушників ця посадова особа не має, оскільки його повноваження мають декларативний характер. Отже, функції Уповноваженого з прав людини, на наш погляд, полягають у контролі за діяльністю органів державної влади щодо недопущення порушення прав людини.

5. Персональні дані, залежно від способу їх зберігання мають оброблятися у такий спосіб, щоб унеможливити доступ до них сторонніх осіб. З метою забезпечення безпеки обробки персональних даних вживаються спеціальні технічні заходи захисту, у тому числі щодо виключення несанкціонованого доступу до персональних даних, що обробляються та роботі технічного та програмного комплексу, за допомогою якого здійснюється обробка персональних даних.

6. Безумовно можна визнати, що оновлення законодавства в сфері захисту персональних даних спрямовані на те, щоб люди мали змогу керувати потоками власних даних, усвідомлювали можливості, які виникають внаслідок їх збору, обробки та подальшого використання, а головне – могли захистити свою приватність.

З метою удосконалення норм чинного законодавства щодо цивільно-правового регулювання захисту персональних даних та приведення його у

відповідність до чинних стандартів ЄС необхідно внести наступні зміни та доповнення у діюче законодавство, які сформувались з наступних пропозицій:

1. Навести визначення терміну «захист персональних даних» у статті 2 Закону «Про захист персональних даних» в такій формі: «захист персональних даних – форма забезпечення на території України для кожної особи, незалежно від її громадянства або місця проживання, дотримання її прав й основоположних свобод, зокрема її права на недоторканність приватного життя, у зв'язку з автоматизованою обробкою персональних даних, що її стосуються».

2. Викласти частину 2 статті 12 Закону «Про захист персональних даних» в наступному вигляді: «Суб'єкт персональних даних отримує докладну та повну інформацію, необхідну для прийняття рішення про надання згоди на обробку його персональних даних: дані про володільця персональних даних, склад та зміст зібраних персональних даних, свої права, визначені цим Законом, мету збору персональних даних та осіб, яким передаються його персональні дані: ...».

3. Доповнити статтю 12 Закону України «Про захист персональних даних» частиною 3 та викласти у такій редакції: «Тягар доведення того, що суб'єкт надав згоду на обробку персональних даних лежить саме на володільці».

4. Додати окремі положення до частини 2 статті 10 Закону України «Про захист персональних даних» та викласти в наступному вигляді: «Володілець та розпорядник персональних даних повинні вести облік операцій, які були пов'язані з обробкою та доступом до персональних даних особи. Автоматизовано повинна реєструватися інформація про те, хто, коли та з якою метою здійснював збір, зміну, перегляд, передачу (у такому випадку кому), видалення (знищення) персональних даних. Володільцю забороняється обробку персональних даних, які не мають певної системи захисту інформації або які мають порушення у цій сфері».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

2. Конвенція про захист прав людини і основоположних свобод : Міжнародний документ від 04.11.1950 р. *Урядовий кур'єр.* 2010. № 215.

3. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : Міжнародний документ від 28.01.1981 р. *Офіційний вісник України*. 2011. № 11, № 58. 2010. Ст. 1994. Ст. 85.

4. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27.04.2016 р. 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). *Офіційний вісник Європейського Союзу*. 2016. L 119. Ст. 1.

5. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» : Міжнародний документ від 24.10.1995 р. URL : http://zakon3.rada.gov.ua/laws/show/994_242 (дата звернення 14.08.2019).

6. Цивільний кодекс України : Кодекс України від 16.01.2003 р. № 435-IV. *Офіційний вісник України*. 2003. № 11. Ст. 461.

7. Цивільний процесуальний кодекс України : Кодекс України від 18.03.2004 р. № 1618-IV. *Урядовий кур'єр.* 2004. № 130.

8. Кримінальний кодекс України : Кодекс України від 05.04.2001 р. № 2341-III. *Відомості Верховної Ради України*. 2001. № 25. Ст. 131.

9. Кодекс України про адміністративні правопорушення : Кодекс України від 07.12.1984 р. № 8073-X. *Відомості Верховної Ради УРСР*. 1984. № 51. Ст. 1122. URL : https://zakon.rada.gov.ua/laws/show/80731-10 (дата звернення 29.07.2019).

10. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. *Урядовий кур'єр*. 2010. № 122.

11. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650.

12. Про доступ до публічної інформації : Закон України від 13.01.2011 р. № 2939-VI. *Відомості Верховної Ради України*. 2011. № 32. Ст. 314.

13. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки : Закон України від 09.01.2007 р. № 537-V. *Голос України.* 2007. № 21.

14. Про авторське право і суміжні права : Закон України від 23.12.1993 р. № 3792-XII. *Відомості Верховної Ради України*. 1994. № 13. Ст. 64.

15. Про банки і банківську діяльність : Закон України від 17.12.2000 р. № 2121- III. *Офіційний вісник України*. 2001. № 1. Ст.1

16. Про нотаріат : Закон України від 02.09.1993 р. № 3425-XII. URL: https://zakon.rada.gov.ua/laws/show/3425-12/ed20170604 (дата звернення 21.07.2019)

17. Про внесення змін до деяких законів України щодо діяльності Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних : Закон України від 13.05.2014 р. № 1262-VII. *Відомості Верховної Ради України*. 2014. № 27. Ст. 914.

18. Про внесення змін до деяких законодавчих актів України щодо створення економічних передумов для посилення захисту права дитини на належне утримання : Закон України від 19.07.2018 р. № 2475-VIII. *Відомості Верховної Ради України*. 2018. № 36. Ст. 272.

19. Про затвердження документів у сфері захисту персональних даних : Наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 р. № 1/02-14. *Бізнес-Бухгалтерія-Право. Податки. Консультації.* 03.03.2014. № 9. Ст. 14.

20. Типовий порядок обробки персональних даних : Наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 р. №

1/02-14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14 (дата звернення 21.08.2019).

21. Правила зберігання, захисту, використання та розкриття банківської таємниці : Постанова Національного банку України від 14.07.2006 р. № 267. URL: https://zakon.rada.gov.ua/laws/show/z0935-06 (дата звернення: 21.08.2019).

22. Щодо законодавчого регулювання діяльності колекторських фірм: Держпідприємництво України. Лист від 27.08.2013 р. № 7747/0/20-13. URL: https://zakon.rada.gov.ua/rada/show/v7747773-13 (дата звернення: 15.07.2019).

23. Рішення Європейського Суду з прав людини у справі «Суріков проти України» (Case Of Surikov V. Ukraine), № 42788/06 від 26.04.2017 р. URL:https://jurisprudencia.mpd.gov.ar/Jurisprudencia/Surikov%20vs%20Ukraine.pdf (дата звернення: 05.11.2019).

24. Рішення Європейського Суду з прав людини у справі Deutsche Telekom AG v. Bundesrepublik Deutschland: Judgment of the Court (Third Chamber) of 5 May 2011. URL: http://curia.europa.eu/juris/celex.jsf?celex=62009CJ0543&lang1=en&type=TXT&ancre= (дата звернення 04.11.2019)

25. Рішення Європейського Суду з прав людини у справі «Бернх Ларсен Холдинг АС» та інші проти Норвегії» (Bernh Larsen Holding AS and Others v. Norway), № 24117/08 від 14 березня 2013 р.

26. Рішення Європейського Суду з прав людини у справі «Хелілі проти Швейцарії» (Khelili v. Switzerland), № 16188/07 від 18.10.2011 р.

27. Постанова Верховного Суду від 08.02.2019 року № 855/17/19. URL : http://www.reyestr.court.gov.ua/Review/79699192 (дата звернення : 28.08.2019).

28. Постанова Верховного Суду від 08.02.2019 року № А/9901/15/19. URL : http://www.reyestr.court.gov.ua/Review/79699192 (дата звернення : 28.08.2019).

29. Ухвала Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ від 27.07.2016 р. № 760/9778/15-ц. URL : http://www.reyestr.court.gov.ua/Review/59288070 (дата звернення: 05.11.2019)

30. Рішення Господарського суду міста Києва від 11.12.2018 Справа № 910/6647/18; URL : http://www.reyestr.court.gov.ua/Review/78926333 (дата звернення:04.11.2019)

31. Постанова Київського апеляційного адміністративного суду від 26.04.2018 р., справа № 826/15225/17. URL : http://www. reyestr. court. gov.ua/Review/73698617 (дата звернення : 02.09.2019).

32. Асірян С. Р. Про аспекти захисту персональних даних як ключового елементу права на приватність. *Міжнародний науковий журнал «Інтернаука»*. 2018. № 10(4). С. 12–17.

33. Бачило И. Л., Сергиенко Л. А., Кристальный Б. А., Арешев А. Г. Персональные данные в структуре информационных ресурсов. Основы правового регулирования. Минск: Беллітфонд, 2006. 474 с.

34. Бем М. В. Відповідальність за порушення законодавства про захист персональних даних : проблеми відповідності законодавства України вимогам регламенту Європейського Союзу щодо захисту персональних даних (GDPR). *Право України*. 2019. № 2. С. 237–255.

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

36. Бем М. В., Городиський І. М. Левицька М. П. Європейські стандарти захисту персональних даних і е-врядування: Звіт за результатами моніторингу стану дотримання європейських стандартів захисту персональних даних при впровадженні електронних сервісів на регіональному рівні. Львів : ГО «Львівський центр міжнародного права та прав людини», 2018. 66 с.

37. Бем М. В., Городиський І. М. Стандарти захисту персональних даних в соціальній сфері. Львів : б.в., 2018. 110 с.

38. Берназ-Лукавецька О. М. Захист персональних даних у соціальній мережі. *Часопис цивілістики*. 2018. Вип. 30. С. 56–59.

39. Бєлова Ю. Д. Система спеціальних цивільно-правових способів захисту права на персональні дані. *Право України*. 2019. № 1. С. 314–327.

40. Бєлова Ю. Д. Стандарти захисту права на персональні дані відповідно до Директиви 95/46/ЄС. *Університетські наукові записки*. 2017. № 3. С. 130–140.

41. Блінова Г. О. Державний контроль за дотриманням законодавства про захист персональних даних. *Право і суспільство*. 2014. № 6.1. С. 68–74.

42. Брижко В. М. До гносеології категорії «інформація». *Інформація і право.* 2011. № 2 (2). С. 13–20.

43. Брижко В. М. Правовий механізм захисту персональних даних: Київ: Парламентське вид-во. 2013. С. 120.

44. Брижко В. М. Приватність даних у хмарних технологіях. *Інформація і право*. 2016. № 4(19). С. 47–59.

45. Брижко В. М. Сучасні основи захисту персональних даних в європейських правових актах. *Інформація і право*. 2016. № 3(18). С. 45–57.

46. Виноградов С. С. Проблема обігу персональних даних в мережі Інтернет. Молодий вчений. 2018. № 1(2). С. 650–653. URL: http://nbuv.gov.ua/UJRN/molv_2018_1(2)__23 (дата звернення: 03.08.2019)

47. Вишновецький В. М. Персональні дані працівника та їх захист. *Юридичний вісник*. Повітряне і космічне право. 2017. № 2. С. 100–106.

48. Волосецький В. О. Законодавство ЄС у сфері захисту персональних даних. *Гілея: Науковий вісник*. Збірник наукових праць. 2016. Вип. 115. С. 471–474.

49. Волосецький В. О. Іноземний досвід правового регулювання захисту персональних даних. *Міжнародний науковий журнал «Інтернаука»*. 2016. № 12(1). С. 148–151.

50. Гронь О. В. Проблеми захисту персональних даних у контексті сучасної комунікації. *Науковий вісник Ужгородського національного*

університету. Серія : Міжнародні економічні відносини та світове господарство. 2018. Вип. 19(1). С. 102–108.

51. Гулак Г. М. Системи захисту персональних даних в сучасних інформаційно-телекомунікаційних системах. *Сучасний захист інформації.* 2017. № 2. С. 65–71.

52. Деякі питання практичного застосування Закону України «Про захист персональних даних»: роз'яснення Міністерства Юстиції України від 21.12.2011 р. *Бізнес-Бухгалтерія-Право. Податки. Консультації.* 2012. № 25. Ст. 54.

53. Дмитренко О. А. Право фізичної особи на власні персональні дані в цивільному праві України: дис., канд. юр. наук. Київ, 2010. 210 с.

54. Дяковський О. С. Визначення поняття персональних даних як правової категорії: сучасні проблеми та шляхи вирішення. *Інформація і право*. 2017. № 3. С. 51–56.

55. Захист персональних даних: правове регулювання та практичні аспекти: наук.-практ. посіб. Бем М. В. [та ін.]; Спіл. програма Європ. Союзу та Ради Європи «Зміцнення інформ. сусп-ва в Україні». Київ : К.І.С, 2015. С. 219.

56. Заярний О. А. Адміністративна деліктність у сфері використання персональних даних та засоби її запобігання. *Вісник Київського національного університету імені Тараса Шевченка*. *Юридичні науки*. 2013. Вип. 95. С. 57–63.

57. Камінська Н. В. Захист персональних даних: проблеми внутрішньодержавного, наднаціонального і міжнародно-правового регулювання. Н*ауковий вісник Національної академії внутрішніх справ*. 2015. № 3. С. 106–114.

58. Кардаш А. В. Уповноважений орган у сфері захисту інформації про особу в Україні: проблеми правового регулювання. *Науковий вісник Херсонського державного університету*. *Серія «Юридичні науки».* 2017. № 5. С. 64–67.

59. Каретник О. С. Поняття інформації про фізичну особу (персональні дані) в цивільному праві України. *Часопис Київського університету права*. 2013. № 2. С. 228–231.

60. Конончук О. Б. Захист персональних даних в умовах соціалізації інтернет-сервісів. *Юридична наука*. 2015. № 2. С. 187–193.

61. Концевой Р. С. До питання визначення поняття «персональні дані». *Інформація і право*. 2012. № 2. С. 23–28.

62. Кохановська О. В. До питання про захист персональних даних в Україні. *Вісник Верховного Суду України*. 2011. № 6. С. 28–33.

63. Крилова Ю. І. Захист персональних даних: вітчизняний та зарубіжний досвід. *Інформація і право*. 2017. № 3. С. 57–63.

64. Мельник К. С. Обробка та захист персональних даних в соціальних мережах. *Інформація і право*. 2014. № 3. С. 64–69.

65. Мельник К. С. Правові та організаційні засади захисту персональних даних в умовах євроінтеграції України : автореф. дис., канд. юрид. наук. Київ, 2016. 20 с.

66. Мельник К. С. Удосконалення нормативно-правового регулювання захисту персональних даних в Україні. *Правова інформатика*. 2014. № 1 (41). С. 30–44.

67. Обуховська Т. І. Державні механізми забезпечення захисту персональних даних в Україні: дис. канд. наук з держ. упр.: 25.00.02. Київ, 2016. 229 с.

68. Петрицький А. Л. Питання захисту персональних даних у сучасній правничій думці. *Право і суспільство*. 2014. № 6.1(2). С. 190–197.

69. Петрицький А. Л. Правові та організаційні засади захисту персональних даних: автореф. дис., канд. юрид. наук. Київ, 2015. 21 с.

70. Пилипчук В. Г., Брижко В. М. Реформування і розвиток системи захисту персональних даних в Україні. *Інформація і право*. 2017. № 3(22). С. 5–21.

71. 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.

72. Правова позиція Міністерства юстиції України щодо діяльності "колекторських" організацій. URL: https:// minjust.gov.ua/ news/ ministry/pravova-pozitsiya-ministerstva-yustitsii-schodo-diyalnosti-kolektorskih-organizatsiy-9801 (дата звернення: 05.02.2019).

73. Размєтаєва Ю. С. Приватність в інформаційному суспільстві: проблеми правового розуміння та регулювання. *Науковий вісник Ужгородського національного університету*. 2016. Вип. 37. С. 43–46.

74. Різак М. В. Правовий статус автора (творця, розробника) бази персональних даних. *Віче*. 2014. № 18. С. 16–19.

75. Різак М. В. Правовий статус Уповноваженого органу з питань захисту персональних даних: досвід зарубіжних країн. *Форум права*. 2012. № 3. С. 619–625.

76. Різак М. В. Практика країн Європейського Союзу та України у сфері судочинства щодо гарантування безпеки обігу та обробки персональних даних. *Підприємництво, господарство і право*. 2017. № 7. С. 68-72.

77. Розпашнюк І. О. Відповідність законодавства України законодавству ЄС в сфері захисту персональних даних. *Публічне право*. 2017. № 2. С. 304–310.

78. Романюк І. І. Охорона права на персональні дані в Україні (цивільно-правовий аспект) : Дис. ... канд. юрид. наук. Київ, 2015. 267 с.

79. Романюк І. І. Персональні дані особи як об'єкт цивільного обороту. *Право і суспільство*. 2014. № 6.1(2). С. 58–65.

80. Русак Д. М. Вдосконалення правового регулювання захисту персональних даних в мережі Інтернет в контексті інтеграції України в світовий інформаційний простір. *Актуальні проблеми міжнародних відносин*. 2015. Вип. 124(2). С. 74–84.

81. Саєнко М. І. Сучасне правове регулювання інформаційних відносин у сфері захисту персональних даних в Україні. *Право і суспільство*. 2015. № 3. С.102–107.

82. Серебряник О. О. Інформація про особу як об'єкт цивільних справ: дис. ... канд. юрид. наук : 12.00.03. Івано-Франківськ, 2016. 209 с.

83. Сергеев А. П., Толстой Ю.К. Гражданское право. Москва : Проспект, 1999. 632 с.

84. Сопілко І. М. Механізм захисту персональних даних: проблеми та перспективи. *Юридичний вісник*. 2013. № 2(27). С. 66–70.

85. Сучасні правові стандарти Європейського Союзу у сфері захисту персональних даних: зб. документів; [неоф. пер. з англ. І. Майстренко]; за ред. В. Брижко; передмова В. Пилипчука. (НДІ інформатики і права Національної академії правових наук України). Київ : ТОВ «Видавничий дім «АртЕк»». 2018. 180 с.

86. Теремецький В. І. Суб'єкти відносин, пов'язаних з персональними даними. *Право і безпека*. 2015. № 2(57). С. 171–176.

87. Тунік А. В. Персональні дані, інформація про особу, конфіденційна інформація про особу: аспекти співвідношення. *Підприємництво, господарство і право*. 2012. № 5. С. 50–54.

88. Усенко І. Б. Коментар до Закону України «Про захист персональних даних». URL: http://khpg.org/index.php?id=1330343937 (дата звернення: 25.04.2019)

89. Червякова О. Б. Закон України «Про захист персональних даних»: проблеми та шляхи вдосконалення. *Проблеми законності*. 2013. № 122. С. 96–106.

90. Черниш Р. Ф. Соціальні мережі як один із інструментів накопичення та протиправного використання персональних даних громадян. *Проблеми законності*. 2017. Вип.136. С. 205–214.

91. Чуприна О. А. Співвідношення понять «персональні дані», «інформація про особу», «конфіденційна інформація про особу». *Підприємництво, господарство і право*. 2013. № 1. С. 104–105.

92. Шевчук О. О. Механізми забезпечення контролю за дотриманням правил захисту персональних даних в ЄС. *Актуальні проблеми правознавства.* 2017. Вип. 4. С. 164–169.