ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА
ІМЕНІ ЛЕОНІДА ЮЗЬКОВА

ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ЕКОНОМІКИ

Кафедра: публічного управління та адміністрування

МАГІСТЕРСЬКА РОБОТА

на здобуття освітнього рівня Магістр
на тему:

ДЕРЖАВНЕ УПРАВЛІННЯ У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Виконала: студентка магістратури
за спеціальністю 281 Публічне
управління та адміністрування
Фіярська С. І.
(прізвище та ініціали)

Керівник: кандидат наук з
державного управління,
доцент, доцент кафедри
публічного управління та
адміністрування
М.О. Маланчій
(прізвище та ініціали)

Рецензент: _____
(прізвище та ініціали)

Хмельницький – 2021 рік

Анотація

Фіярська С. І. Державне управління у сфері захисту персональних даних. Кваліфікаційна наукова праця на правах рукопису. Магістерська робота на здобуття освітнього ступеня магістра за спеціальністю 073 Менеджмент. – Хмельницький університет управління та права імені Леоніда Юзькова, Хмельницький, 2021. – 72 с.

Право на захист персональних даних як підгалузь державного права слід розглядати як сукупність правових норм, що регулюють суспільні відносини, що виникають у процесі збирання, зберігання, обробки, видалення, передачі, розкриття та іншого використання персональних даних, що становлять будь-яку інформацію, за допомогою якої можна однозначно ідентифікувати фізичну особу, і осіб що впливають на такі відносини за допомогою імперативно-диспозитивного методу правового регулювання.

Передовими країнами у цьому сенсі стали країни Західної Європи, у котрих були прийняті спеціальні закони про захист персональних даних. Однак, законодавство щодо персональних даних в європейських країнах продовжує розвиватися. У практиці європейських держав сьогодні також виникають нові проблеми, що потребують правового регулювання (наприклад, транскордонна передача персональних даних, використання біометричних персональних даних, даних медико-генетичного характеру, тощо).

Ключові слова: персональні дані, право на персональні дані, немайнові блага, суб’єкт права персональних даних, стандарти правового регулювання цивільних відносин щодо персональних даних, право на мобільність персональних даних, право на забуття, розпорядник, володілець, підстави виникнення правовідносин щодо персональних даних, обробка персональних даних способи захисту, способи захисту персональних даних.

THE SUMMARY

Fiyarska S.I. Public administration in the field of personal data protection. Qualification scientific work on the rights of the manuscript. Master's degree in 073 Management. - Khmelnytsky University of Management and Law named after Leonid Yuzkov, Khmelnytsky, 2021. - 72 p.

The right to protection of personal data as a sub-branch of state law should be considered as a set of legal norms governing public relations arising in the process of collection, storage, processing, deletion, transfer, disclosure and other use of personal data constituting any information by means of which it is possible to unambiguously identify an individual and persons influencing such relations by means of the imperative-dispositive method of legal regulation.

The first rules on the protection of personal data were considered in the context of the right to privacy. However, against the background of the transition to the information society, which is characterized by the widespread use of information technology, active collection and processing of information, including personal information, there is a need for legal regulation of personal data processing. The spread of the "Internet age" only accelerates the need for legal regulation of personal data protection.

The leading countries in this sense were the countries of Western Europe, which adopted special laws on personal data protection. However, legislation on personal data in European countries continues to evolve. In the practice of European countries today, new problems also arise that require legal regulation (for example, cross-border transfer of personal data, use of biometric personal data, medical and genetic data, etc.).

Keywords: Personal Data, Personal Data Right, Intangible Assets, Personal Non-property Rights, Personal Data Right Subject, standards of legal regulation of relations regarding Personal Data, Personal Data Mobility Right, Forgetting Right, holder, owner, basis of arising of Relationship on Personal Data, Personal Data Processing, Law ways of protection; ways of protection of Personal Data.

ЗМІСТ:

ВСТУП

Актуальність теми. Сучасні технології, особливо в інформаційно-телекомунікаційній сфері, розвиваються настільки стрімко, що часто правове регулювання не встигає за цим розвитком, і це породжує безліч як реальних, так і потенційних загроз основним правам і свободам людини. Одна з актуальних проблем полягає в тому, що нові технології створюють безпрецедентні можливості для свідомого чи неусвідомленого порушення права недоторканності приватного життя.

З розвитком комп'ютерних технологій і кіберпростору (WorldWideWeb, соціальні мережі, онлайн-трансляції, передача геоданих та ін) найбільш вразливою для порушень категорією стала особиста інформація (персональні дані).

Поява нових загроз недоторканності приватного життя, що виникають у процесі збирання, обробки, зберігання та іншого використання персональних даних у різних контекстах, очевидно доводить необхідність розробки ефективних заходів з охорони фундаментального права людини на захист особистих даних. Події останнього десятиліття показали, наскільки небезпечною для збереження недоторканності приватного життя можливо неправомірна діяльність за відсутності належних інструментів правового регулювання захисту особистої інформації. Особливо схильні до ризику порушення прав користувачів персональних даних держави, потоки інформації між якими можуть передаватися без будь-яких бар'єрів, зокрема, в рамках міжнародних та регіональних організацій.

Вищезазначене зумовило вибір теми дисертаційного дослідження, *метою якого є* вирішення комплексу теоретичних і практичних проблем, пов’язаних із адміністративно-правовими аспектами захисту прав персональних даних громадян суб’єктами публічної адміністрації; розроблення конкретних пропозицій та рекомендацій щодо удосконалення правового регулювання адміністративно-правових відносин, пов’язаних із персональними даними.

Стан розробки у вітчизняній та зарубіжній науці. Проблемам особливостей правовідносин щодо захисту прав персональних даних громадян суб'єктами публічної адміністрації сьогодні присвячено незначна кількість наукової публіцистики.

Сутність персональних даних і окремі аспекти їх адміністративно-правового захисту досліджували такі вчені: Р.А. Калюжний, В.І. Теремецький, М.Я. Швець.

Серед наукових праць, присвячених проблемам адміністративно-правового регулювання обігу, обробки та захисту персональних даних, слід виділити роботи В.М. Брижко «Організаційно-правові питання захисту персональних даних» (2004 р.), А.М. Чернобай «Правові засоби захисту персональних даних працівника» (2006 р.), Д.В. Цвірюк «Адміністративно-правовий захист персональних даних в Україні» (2014 р.).

Загалом питання комплексного дослідження персональних даних як об'єкту адміністративно-правових відносин є актуальним.

Мета і завдання дослідження. Метою дослідження виступає зміст теоретичні та практичні аспекти формування та реалізації державної політики у сфері забезпечення захисту персональних даних. Досягнення поставленої мети стає можливим завдяки виконання наступних завдань:

- поняття персональних даних та її використання;

- механізм державного управління у сфері захисту персональних даних в ЄС;

- організаційно-управлінські засади державного управління у сфері захисту персональних даних;

- суб'єкти державного управління у сфері захисту персональних даних;

- удосконалення реєстраційних процедур у контексті державного управління у сфері захисту персональних даних;

- напрями удосконалення організаційно-управлінських засад державного управління у сфері захисту персональних даних.

Об'єктом дослідження є суспільні відносини, які виникають у сфері

державного управління у сфері захисту персональних даних.

Предметом дослідження є теоретико-методичні та практичні аспекти механізму державного управління у сфері захисту персональних даних.

Методологічну основу дослідження склали загальнонаукові і спеціальні методи: формально-логічний, аналітичний, історичний, системно-логічний, порівняльно-правовий. За допомогою формально-логічного та історичного методів визначене поняття персональних даних. Аналіз сучасного стану законодавства щодо особливостей державного управління у сфері захисту персональних даних здійснено за допомогою аналітичного методу, який використовувався у процесі розробки пропозицій з удосконалення правової бази щодо статусу зазначених реєстраційних відносин. Системно-логічний метод застосовувався при виявленні ознак механізму державного управління у сфері захисту персональних даних. Аналіз різноманітних підходів до визначення державного управління у сфері захисту персональних даних у інших європейських країнах проведено за допомогою порівняльно-правового методу. Застосування системного підходу дозволило сформулювати пропозиції щодо удосконалення організації механізму державного управління у сфері захисту персональних даних.

Інформаційну базу дослідження склали вітчизняні законодавчі акти у цій сфері та правові акти окремих іноземних держав, які містять положення щодо особливостей механізму державного управління у сфері захисту персональних даних; наукові публікації з досліджуваної проблематики.

Практичне значення отриманих результатів дослідження. Отримані результати, рекомендації щодо організації здійснення механізму державного управління у сфері захисту персональних даних можуть бути використані у сфері законотворчості, зокрема у процесі роботи над проектом нової редакції Закону України про захист персональних даних.

Структура та обсяг зумовлені метою і завданнями здійсненого дослідження. Робота складається зі вступу, трьох розділів, шести підрозділів,

висновків, списку використаних джерел (всього 89 найменувань). Загальний обсяг роботи становить 72 сторінок.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ФУНКЦІОНУВАННЯ СИСТЕМИ ДЕРЖАВНОГО УПРАВЛІННЯ У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

1.1 Поняття персональних даних та її використання

Сучасний етап розвитку цивілізації відзначається всеохоплюючим запровадженням засобів інформатизації процесів державного управління через створення масштабних баз даних та широкого доступу органів влади до персональних даних громадян.

Інформатизація сфери податкової діяльності вимагає узгодження інтересів органів влади та окремих осіб у частині забезпечення захисту персональних даних, що особливо важливо у частині інформації яка акумулюється у податковій звітності та інших документах. Особливого інтересу зазначені питання набувають у контексті запровадження в Україні досвіду використання непрямих методів податкового контролю.

Виникнення персональних даних як категорії в інформаційному праві та праві в цілому тісно пов'язане з ідеєю захисту приватного життя, яке в умовах розвитку інформаційного суспільства все частіше наражається на різний вид загроз. Саме бажання забезпечити належний рівень захисту особистості від інформаційних загроз призвело до ідеї контролю за оборотом інформації про індивідів - персональних даних, виділивши їх у особливий вид інформації, що потребує захисту.

Персональні дані - відомості про фізичну особу або дані, які відносяться прямо чи опосередковано до певної або визначеної на підставі таких відомостей фізичної особи (суб'єкту персональних даних), у тому числі її прізвище, ім'я, по батькові, рік, місяць, дата та місце народження, адреса, сімейний , соціальний, майновий стан, освіта, професія, доходи, а також інша інформація, яка, як правило, представлена у формалізованому вигляді, що забезпечує можливість її

обробки в інформаційних системах, переважно за допомогою засобів автоматизації, повністю або частково.

Для відмежування персональних даних від інших видів інформації обґрунтовується використання як основної ознаки персональних даних про наявність взаємозв'язку між суб'єктом та змістом відповідної інформації про нього. Такий зв'язок може бути очевидним через пряму вказівку на суб'єкта даних з використанням ідентифікуючої інформації, або він може бути потенційно встановлений. Як додаткову ознаку персональних даних слід розглядати їх формалізований характер, тобто. обумовлений цілями та завданнями обробки в інформаційній системі набір відомостей та їх зв'язок з інформаційною системою.

З метою впорядкування існуючих уявлень про місце правового режиму персональних даних серед інших режимів інформації обґрунтовано висновок про відсутність єдиного правого режиму персональних даних, оскільки вони можуть бути як у режимі загальнодоступної інформації, так і в режимі обмеженого доступу. Стосовно персональних даних у режимі обмеженого доступу слід виділити особливо «правовий режим конфіденційності персональних даних», який має власний зміст і поширюється на випадки обробки персональних даних на умовах дотримання конфіденційності (за винятком державної таємниці). Режим конфіденційності персональних даних, у свою чергу, включає режим спеціальних категорій персональних даних і режим біометричних персональних даних, кожен з яких також має свої особливі параметри.

Обґрунтовується висновок, що конфіденційність персональних даних є встановленою законодавством вимогою, зверненою виключно до оператора, обробника персональних даних, органу захисту персональних даних, працівника оператора, а також іншої особи, тобто конфідентам, які отримали доступ до персональних даних на законній підставі. Конфіденційність, як обов'язкова вимога, виникає з отримання доступу до персональних даних конфіденту, за відсутності у нього законних підстав для обробки їх у режимі загальнодоступної інформації.

З метою усунення колізій, що виникають пов'язаних із співвідношенням правового режиму конфіденційності персональних даних з іншими правовими режимами конфіденційної інформації, такими як: лікарська таємниця, таємниця зв'язку, адвокатська, нотаріальна, банківська таємниці та ін., обґрунтовується необхідність закріплення в законі «Про персональні дані» колізійної норми-правила, яка б встановила пріоритет вимог режиму конфіденційності персональних даних, які мають бути виконані конфідентами, за умов, коли іншими режимними вимогами передбачається нижчий рівень захищеності інформації.

Для вирішення проблем, що виникають у правозастосовній практиці, автором пропонується використання та пряме закріплення в законодавстві положення про «презумпцію конфіденційності персональних даних» як один із принципів, передбачених статтею закону «Про персональні дані» [53].

Поняття персональних даних пропонуємо визначати, як відомості або сукупність відомостей, що торкаються інформації щодо громадянина, яка є їх власником, та дозволяють здійснити її ідентифікацію.

1.2 Механізм державного управління у сфері захисту персональних даних в Європейському Союзі

У Європейському Союзі спеціальні нормативні акти про захист персональних даних існують уже понад двадцять років, а у 2018 р. набули чинності нові правові акти, які здійснили справжню революцію європейського правового регулювання захисту особистих даних. У процесі підготовки нових правових актів стало очевидним, що потрібно впровадження нових способів захисту даних, таких як профілювання та псевдонімізація, оскільки глобалізація зумовлює активний розвиток та вдосконалення інформаційних технологій, стирання меж передачі даних, використання нових типів персональних даних (наприклад, біометричних, генетичних) та автоматизованих систем обробки.

У процесі формування та розвитку правове регулювання захисту персональних даних у Європейському Союзі пройшло чотири етапи.

Кожен з цих етапів має характерні особливості і, зокрема, пов'язаний із впровадженням у правову систему Союзу певних нормативних актів, що заповнюють прогалини у правовому регулюванні та відповідають на існуючі виклики та ризики для персональної інформації. Прийняття цих актів зумовлювалося різними причинами політичного, економічного, технологічного, соціального характеру. Перший етап має часові рамки з 1995 по 2001 рр., другий етап – з 2002 по 2009 рр., третій – з 2010 по 2018 рр., четвертий етап триває з 2018 року до теперішнього часу. Початком формування правового регулювання захисту персональних даних у ЄС слід вважати ухвалення у 1995 р. Директиви 95/46/ЄС – першого загальнообов'язкового правового акта, що заклав основи захисту персональних даних фізичних осіб у Європейському Союзі [87].

Другий етап характеризується прийняттям документів у специфічних сферах, які не підпадали під дію Директиви 95/46/ЄС, зокрема, що встановлюють правила обробки персональних даних та захисту конфіденційності у секторі електронних засобів зв'язку (Директива 2002/58/ЄС); правила обробки персональних даних інституціями, органами та агенціями Союзу та установи на рівні ЄС незалежного Європейського Уповноваженого із захисту даних (Регламент (ЄС) No 45/2001); а також створення Європейського агентства з мережевої та інформаційної безпеки (Регламент (ЄС) No406/2004). Третій етап характеризується закріпленням права на захист персональних даних як фундаментального та невід'ємного права людини на рівні первинного права ЄС – в установчих Договорах, зокрема у статті 16 Договору про функціонування Європейського Союзу, у статті 39 Договору про Європейський Союз та у статті 8 Хартії Основних прав Європейського Союзу. Норми захисту даних, закріплені у цих документах, стали базою для розробки та впровадження в правову систему ЄС Загального Регламенту із захисту даних.

Четвертий - сучасний - етап пов'язаний із набуттям чинності в 2018 р. на території ЄС Загального Регламенту із захисту даних (Регламент (ЄС) 2016/679),

що замінює та скасовує Директиву 95/46/ЄС, та Директиви (ЄС) 2016/680 [87], яка встановлює правила про захист фізичних осіб щодо обробки персональних даних компетентними органами з метою запобігання, розслідування, виявлення або кримінального переслідування за кримінальні злочини або виконання кримінальних покарань, яку кожна держава-член ЄС імплементує в законодавство та зобов'язана застосовувати на своїй території з 6 травня 2018 р. У Європейському Союзі на сучасному етапі відбувається активне формування підгалузі права на захист персональних даних у галузі інформаційного права ЄС.

Встановлено, що право на захист персональних даних має всі необхідні ознаки, які притаманні підгалузі права, а саме: предметна єдність регульованих правом на захист персональних даних суспільних відносин та їх суттєва суспільна значимість; використання комплексу самостійних способів та прийомів правового регулювання захисту персональних даних; наявність власних джерел правового регулювання, що становлять у своїй сукупності право фізичних осіб на захист персональних даних; наявність спеціальних принципів захисту персональних даних, що діють у системі, забезпечуючи цілеспрямоване регулювання суспільних відносин, що утворюють його предмет; власна системна організація, яка відображена в нормах права захисту персональних даних. Відповідно, дане правове явище може бути кваліфіковане як підгалузь права.

Право на захист персональних даних як підгалузь права слід розглядати як сукупність правових норм, що регулюють суспільні відносини, що виникають у процесі збирання, зберігання, обробки, видалення, передачі, розкриття та іншого використання персональних даних, що становлять будь-яку інформацію, за допомогою якої можна однозначно ідентифікувати фізичну особу, і осіб що впливають на такі відносини за допомогою імперативно-диспозитивного методу правового регулювання.

Право на захист персональних даних регулює суспільні відносини, що виникають між їхніми учасниками з приводу збору, обробки та іншого використання персональних даних, у результаті чого вони набувають правову форму, тобто стають правовими відносинами. Суб'єктами таких правовідносин

виступають такі особи: фізичні особи, які надають свої особисті дані для обробки; фізичні чи юридичні особи, які проводять обробку таких даних; інститції, органи, агентства та установи Європейського Союзу (до них застосовується Регламент (ЄС) 2018/1725 та деякі інші правові акти Союзу); уповноважені незалежні органи, що здійснюють регулювання захисту персональних даних у Європейському Союзі та державах-членах; держави-члени ЄС (за винятком провадження ними діяльності, що підпадає під сферу дії Глави 2 Розділу V ДЕС) та їх органи (правила, що стосуються обробки персональних даних правоохоронними та судовими органами держав-членів, встановлює Директива (ЄС) 2016/680) [87].

Під об'єктом права на захист персональних даних, у свою чергу, слід розуміти персональні дані, що означають будь-яку інформацію, що відноситься до ідентифікованої фізичної особи або фізичної особи, що ідентифікується. Така інформація має бути правдивою та повинна позначати унікальну характеристику даної особи (її ідентичність) у конкретний момент часу. До персональних даних може ставитися як загальнодоступна інформація, так і конфіденційного характеру. Анонімна інформація може бути віднесена до персональних даних за дотримання кількох умов. Так, слід розглядати як персональну інформацію про фізичну особу, що ідентифікується, дані, що зазнали анонімізації або псевдонімізації, але які можуть бути приписані такій фізичній особі з використанням додаткової інформації будь-якого роду. Крім того, до персональних даних буде належати лише та анонімна інформація, співвіднесення якої з певною фізичною особою не вимагатиме застосування непропорційних зусиль.

Підгалузь права захисту персональних даних фізичних осіб характеризується наявністю власних принципів, які слід класифікувати як спеціальні принципи права ЄС.

Принципи захисту персональних даних є основними керівними початками, які виражають сутність, основні властивості та загальну спрямованість розвитку правових норм у рамках цієї підгалузі права. Вони знаходять свій відбиток у

найважливіших правових документах Європейського Союзу і є гарантом законності у забезпеченні взаємодії між державами-членами та реалізації норм, створених ними.

До спеціальних (підгалузевих) принципів належать такі: принцип легітимної, справедливої та прозорої обробки; принцип мінімізації даних; принцип обмеження мети обробки; принцип точності даних; принцип обмеження зберігання даних; принцип безпеки даних; принцип застосування особливого режиму для чутливих даних; принцип участі та контролю фізичної особи за використанням персональних даних; принцип відповідальності; принцип обмеження розкриття персональних даних.

Зазначені спеціальні принципи права на захист персональних даних поряд з основними принципами права ЄС та галузевими принципами інформаційного права ЄС застосовуються до всіх операцій з обробки інформації, яку можна визначити як персональні дані фізичних осіб.

Правове регулювання у сфері захисту персональних даних у ЄС спрямоване на захист прав, свобод та законних інтересів усіх без винятку фізичних осіб, які перебувають на території ЄС, персональні дані яких піддаються обробці.

Права та обов'язки базуються на концепції законної, прозорої та контрольованої обробки даних, закладеної у спеціальних принципах та яка відповідає правомірним інтересам фізичних осіб, які надають свої персональні дані (суб'єктів персональних даних).

Порівняно з нормативними актами, що діяли в ЄС, у сучасних правових актах, прийнятих у 2016 р. і пізніше, істотно розширено комплекс суб'єктивних прав фізичних осіб. Деякі з цих прав є новелами не лише на європейському рівні, а й у світовому масштабі.

Комплекс прав, з яких складається фундаментальне право фізичної особи на захист персональних даних, розроблений з урахуванням існуючих ризиків для безпеки особистої інформації, у тому числі в мережі Інтернет, і включає такі права: право на видалення даних (право бути забутим); право на доступ до

інформації; право на виправлення; право на обмеження обробки даних; право на портативність даних; право про заперечення; право на захист персональних даних дітей.

Реалізація особою своїх прав не повинна негативно впливати на права та свободу інших осіб. Для ефективного здійснення правового регулювання кожна фізична особа має деякі обов'язки щодо інших суб'єктів.

Їх можна класифікувати на загальні, які передбачені для всіх ситуацій, пов'язаних з обробкою (обов'язок особи дотримуватись нормативних актів Союзу та держав-членів, що стосуються захисту персональних даних), та факультативні, які передбачені для певних випадків (обов'язок надати додаткову інформацію, необхідну для підтвердження особи суб'єкта даних, або згода законного представника та ін.)

Наразі проводиться реформа уповноважених органів із захисту даних Європейського Союзу та держав-членів.

Зокрема, створено новий орган - незалежну Європейську Раду із захисту даних, скасовано Робочу групу із захисту фізичних осіб щодо обробки персональних даних, яка мала виключно консультативну функцію, нові завдання поставлені перед Європейським Уповноваженим із захисту даних, детально врегульовано діяльність незалежних наглядових органів держав- членів, у тому числі їх взаємодія один з одним та з контролюючими органами Союзу. Зазначені уповноважені органи утворюють цілісну систему на рівні Європейського Союзу, центральним елементом якої стала Європейська Рада із захисту даних.

Ефективне функціонування системи уповноважених органів забезпечується застосуванням дієвих механізмів «Співробітництва» (Cooperation) та «Узгодженості» (Consistency), передбачених у правових актах ЄС.

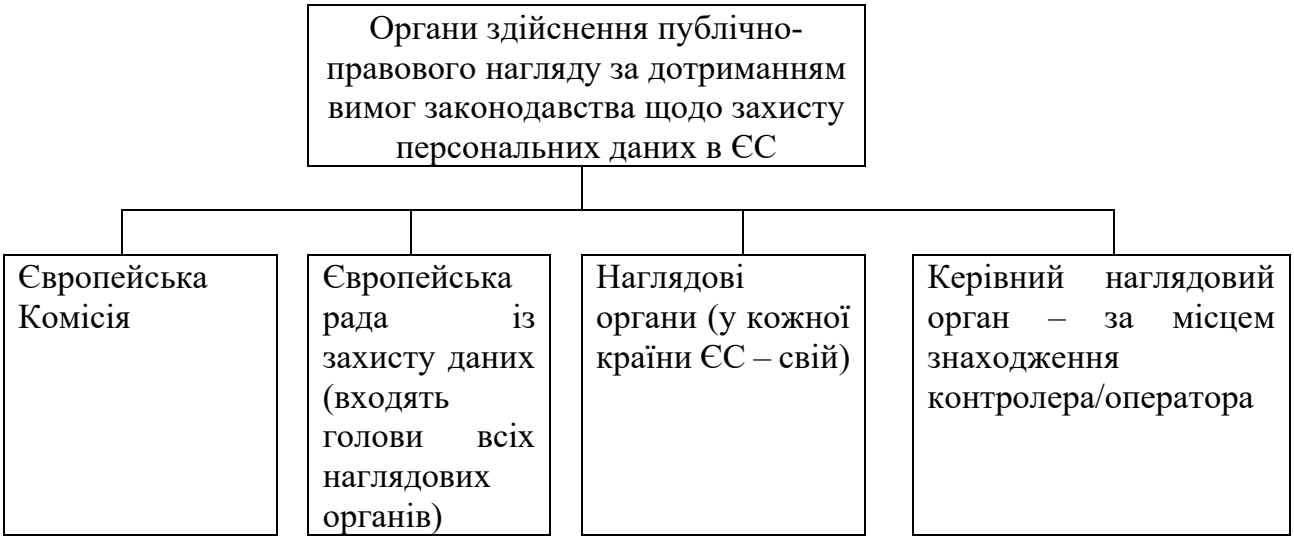

Рисунок - 1.1 Структура органів здійснення публічно-правового нагляду за дотриманням вимог законодавства щодо захисту персональних даних в ЄС

Примітка. Розроблено автором.

Встановлено, що кожен із уповноважених органів має специфічні функції, спрямовані на здійснення єдиної мети - захисту прав, свобод та законних інтересів фізичних осіб при проведенні операцій з обробки їх персональних даних різними суб'єктами.

Європейська Рада із захисту даних виконує контрольну, виконавчу, консультативну функцію, а також функцію з координації та взаємодії. На Європейського Уповноваженого із захисту даних покладено інформаційну, консультативну, організаційну, охоронну та контрольну функції. Національні наглядові органи наділені повноваженнями для здійснення інформаційної, охоронної, виконавчої, контрольної функції та функції з координації та взаємодії. Для цілей реалізації своїх функцій кожен уповноважений орган наділений владними повноваженнями стосовно суб'єктів, які перебувають у його юрисдикції.

Правове регулювання захисту персональних даних у ЄС передбачає застосування компетентними органами спеціальних заходів юридичної відповідальності за порушення правових актів ЄС щодо захисту фізичних осіб

щодо обробки персональних даних, які є передбаченими санкцією правової норми примусовими заходами, що тягнуть за собою певні несприятливі наслідки для правопорушника за вчинене правопорушення.

Юридична відповідальність в даний час здійснюється на підставі чинних правових актів ЄС, кожен з яких передбачає застосування санкцій за порушення у певній сфері для конкретних суб'єктів: контролерів та процесорів (які обробляють персональні дані); компетентних органів держав-членів (що обробляють особисті дані фізичних осіб з метою запобігання, розслідування, виявлення кримінальних злочинів або виконання покарань за скоєння злочинів); наглядових органів держав-членів; інституцій, органів та установ Союзу, у тому числі Європейського Уповноваженого із захисту даних. Крім того, застосування заходів відповідальності (зокрема дисциплінарних) регулюється спеціальними актами інституцій, органів та установ ЄС.

Усі заходи спрямовані на запобігання та мінімізацію наслідків порушень, що стосуються персональних даних фізичних осіб, а також на покарання порушників, яке виражається в обов'язку винної особи зазнати передбачених санкцією відповідної правової норми несприятливих наслідків за скоєне правопорушення. Ці заходи можуть бути дисциплінарного, адміністративного та іншого характеру. Правові акти ЄС також не забороняють державам-членам включати до свого законодавства заходи кримінальної відповідальності.

Визначено три основні напрямки, за якими прогнозується розвиток правового регулювання захисту персональних даних у Європейському Союзі. Перший напрямок: прийняття нових правових актів на рівні ЄС, а також внесення змін та доповнень до чинних, зокрема, Регламенту (ЄС) 2016/679, Директиви (ЄС) 2016/680, Регламенту (ЄС) 2018/1725 та інших [87].

Інституції та органи Союзу продовжують активно працювати, аналізуючи практику застосування суб'єктами правил зазначених правових актів, для внесення у майбутньому доповнень та змін до них чи їхнього можливого перегляду. Крім того, протягом найближчих кількох років планується прийняття

нових правових актів на рівні ЄС, деякі з них вже перебувають на стадії обговорення, проекти інших - у розробці.

Серед пріоритетних напрямків – захист оперативних даних, що обробляються правоохоронними органами ЄС (розглядається питання застосування Глави IX Регламенту (ЄС) 2018/1725 до Європолу та Європейської прокуратури), а також захист даних у сфері електронних комунікацій (у розробці знаходяться проекти Регламенту «ePrivacy» та Директиви "EECC").

Другий напрямок: прийняття спеціальних актів інституціями та уповноваженими органами ЄС, а також реалізація ними різних ініціатив, зокрема довгострокових стратегій.

Для уточнення положень чинних правових актів Комісія ЄС має право приймати делеговані акти, а також виконавчі акти на підставі повноважень, наданих їй Європейським парламентом та Радою ЄС. Акти з питань процедурного характеру, такі як керівні принципи та передова практика, у межах своєї компетенції уповноважені приймати Європейську Раду із захисту даних та Європейську Уповноважену із захисту даних.

Акти рекомендаційного та консультаційного характеру приймаються ними як за своєю ініціативою, так і за запитами Комісії та інших інституцій ЄС. Серед стратегій інституцій та органів ЄС, спрямованих на перспективу, можна виділити Стратегію з розвитку Єдиного цифрового ринку, Стратегію «подаючи приклад» на 2015-2019 рр., Програму з прав, рівності та громадянства на 2014-2020 рр., Стратегію «Horizon 2020 " та ін..

Третій напрямок: прийняття всіма державами-членами нових (або внесення змін до чинних) національних законів, які уточнюють певні положення регламентів та імплементують у законодавство директиви. У ході дослідження встановлено, що держави-члени імплементують положення правових актів ЄС у свої закони із затримками та іншими численними порушеннями. У зв'язку з цим Комісія ЄС винесла зауваження деяким державам, і за невиконання її вимог має намір ініціювати позови в Суді ЄС.

Інша проблема полягає в тому, що при імплементації не вдалося уникнути колізій, оскільки кожна держава може інтерпретувати ті самі положення правових актів ЄС по-різному. У цих умовах особливе значення матиме судова практика Суду ЄС, яка продовжує відігравати важливу роль у правозастосуванні та правотворчості, сприяючи подальшому розвитку та вдосконаленню права на захист персональних даних у ЄС.

РОЗДІЛ 2. АНАЛІЗ ДЕРЖАВНОГО УПРАВЛІННЯ У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

2.1 Нормативно-правові засади державного управління у сфері захисту персональних даних

Інститут персональних даних – це відносно «молодий» за своєю правовою природою інститут суспільних відносин. Сучасним «взірцем» правового регулювання та забезпечення захисту персональних даних є «Загальний регламент про захист даних» або «General Data Protection Regulation – GDPR») [87].

Зрозуміло, що поява цього визначного нормативно-правового документу є результатом тривалого історичного процесу становлення нормативно-правового забезпечення захисту персональних даних. У цьому процесі можливо побачити результати та історичні надбання розвитку глобальної правової доктрини. При цьому наголосимо, що Україна не залишається поза цього процесу, а навпаки стає його органічною частиною.

З моменту вступу у дію 25 травня 2018 року Європейського регламенту щодо захисту персональних даних минуло уже більше двох років, що також дає можливість об’єктивно оцінити його ефективність та вплив на суспільні відносини.

Підкреслимо, що дія цього нормативно-правового акту поширюється, крім іншого, і на територію України, однак, лише опосередковано.

Із цієї, й не лише, причини, питанням захисту персональних даних у нашій країні приділено значну увагу з боку представників юридичного середовища та громадськості. Сьогодні у наукових та публіцистичних публікаціях часто можна зустріти думку, що GDPR – це у першу чергу приватно-правове явище, цивілістичне нововведення європейських законодавців. Насправді ж, цей Регламент є результатом тривалого розвитку концепції фундаментальних прав і свобод людини, котра виникла задовго до 25 травня 2018 року.

Сфера захисту персональних даних охоплює відносини комплексного правового характеру і має як публічно-правові так і приватно-правові прояви. Водночас, на нашу думку, приватно-правові відносини та засоби правового впливу на регулювання та приватно-правовий захист персональних даних носять додатковий (субсидіарний) характер у порівнянні з публічно-правовими. Це обумовлено тим, що історично захист персональних даних сформувався, як елемент конституційно-правового та адміністративно-правового захисту права на недоторканість (концепція «прайвесі»).

Найвиразніше ця ідея відображена у правових догмах загального права. Охорона приватного життя громадян, свободи людини від неправомірного та надмірного втручання (докучання) держави у сфері приватного життя була об'єднана у американській юриспруденції у концепцію «прайвесі». У ній знайшли адекватне відображення принципи індивідуалізму та інші загальнодемократичні ідеали.

Перше чітке формулювання змісту поняття «прайвесі» було зроблено ще в 1890 р., яке визначило його як «право дати людині спокій». Англійською мовою усі аспекти особистого життя позначаються єдиним терміном «privacy», котрий не має буквального еквівалента в українській мові. Цей термін увійшов у політико-правовий лексикон і визначає всі аспекти приватного життя: інтимний світ, сферу особистих стосунків, недоторканність приватного листування, щоденників, свободу думки та релігійних переконань [53].

Саме у 1890 році два американських юриста С.Д. Уоррен та Л.Д. Брендайс опублікували в Harvard Law Review статтю «The Right to Privacy» (Право на особисте життя), де описували згадане «право бути залишеним наодинці» («the right to be let alone»).

У своїй статті «Право на приватність» у Гарвардському правовому журналі вони стверджували, що приватності загрожує небезпека у зв'язку із новими винаходами та методами ведення бізнесу, й обґрунтовували необхідність створення спеціального «права приватності».

На тлі подальшого розвитку наукового і технічного прогресу ми дедалі більше переконуємося в справедливості даних міркувань. Практично одразу, а точніше у першій половині XX ст., сформульоване право на особисте життя знаходить своє відображення в американській судовій практиці [83]. Ця ідея доволі блискавично поширюється і за межами США.

Паралельно історичні передумови визнання права на недоторканість особистого життя формуються у «неофіційній» правовій доктрині на теренах України. Історичні витоки сучасного національного праворозуміння цінностей забезпечення особистісної сфери людини, у тому числі її приватності від будь-яких форм зовнішнього втручання ми можемо співвіднести з працями відомого діяча громадівського руху Михайла Драгоманова. Мова йде про його Проект основ статуту українського товариства «Вільна Спілка»- «Вольный союз». У частині першій, присвяченій головним завданням «Вільної Спілки» в Росії (Російській Імперії) виголошується завдання спрямоване на «перетворення цієї держави на засадах політичної свободи».

Під словами політичні свободи М. Драгоманов пропонує розуміти: недоторканість тіла для принизливих покарань та смертної кари; недоторканість особи і житла для поліції без судової постанови; недоторканість приватних листів та телеграм тощо» [14]. Саме це і дає поштовх численним та, нажаль, також і не реалізовані спробам вироблення нових правових засад забезпечення недоторканості приватного життя людини, які не витримали випробувань жорстокою реальністю XX століття.

У XX столітті значну роль у становленні та формулюванні права на особисте життя, як і у попередньому, також відіграла діяльність американських судів. Так, у 1965 році у справі Griswold v. Connecticut суддя Верховного Суду США Дуглас вивів право на особисте життя із перших п’яти поправок до Конституції США, визнавши, що ці поправки «охороняють різні аспекти недоторканості особистого життя» [83].

Широко відомі слова, котрі він промовив, резюмуючи рішення суду: «Йдеться про право на недоторканість особистого життя, котре старше, ніж Білль про права».

Сформована у США концепція «privacy» суттєво вплинула на становлення сучасної системи прав і свобод людини. У 1948 році право на особисте життя фіксується разом із іншими фундаментальними правами і свободами у Загальній декларації прав людини (ст. 12) [18], а в 1950 році – У Європейській конвенції з прав людини (ст. 8) [16].

10 грудня 1948 року на Генеральній Асамблеї ООН була затверджена Загальна Декларація прав людини, у ст. 12 котрої встановлювалось, що ніхто не може бути об’єктом свавільного втручання в його особисте та сімейне життя, свавільного посягання на недоторканість.

Як відомо, перший у світі спеціальний Закон про захист персональних даних був прийнятий німецькою землею Гессен у 1970 році [35]. До цього подібних законів не було ніде у світі. А за сім років з'явився перший федеральний закон, що захищає персональні дані німців [8].

Упродовж останніх 30 років більш, ніж у 20 європейських країнах були прийняті нормативні акти щодо захисту персональних даних. У них були закріплені чинні механізми правового регулювання обігу персональних даних. Варто зауважити, що створення нормативних актів у даній сфері відбувалося паралельно із розвитком законодавства про захист права на недоторканість особистого життя.

На теренах Російської Імперії окремі елементи права на недоторканість особистого життя законодавчо закріплювались та аналізувалися ще в дореволюційний період.

Через відсутність традицій конституалізму, як правового явища, саме адміністративні та кримінально-процесуальні норми в той історичний період стають джерелами закріплення перших «елементів» будови захисту особистої недоторканості. Так, Поштовий Устав 1857 року та Телеграфний Устав 1876 року регламентували таємницю кореспонденції. Кримінально-правова охорона

названої таємниці здійснювалася на основі норм «Уложення про покарання кримінальні та виправні 1845 року», «Кримінального Уложення 1903 року». Так, в останньому (ст. 162-170) встановлювалася заборона на втручання посадових осіб при здійсненні ними правосуддя в особисте та сімейне життя людини [3].

Пізніше питання піднесення важливості «людиноцентризму» у питаннях правового регулювання ми бачимо у період після завершення Другої Світової війни. Належна увага до прав людини на той час пояснюється, перш за все, руйнівними наслідками Другої Світової війни. Це знайшло своє відображення й у визначенні права на особисте життя.

Головним пріоритетом того часу були найбільш значимі соціальні питання повоєнного періоду: недоторканість особистого і сімейного життя, таємниця листування. Водночас, на власне проблему захисту персональних даних, котра, здавалося б, є логічним продовженням права на особисте життя, не звертали належної уваги.

В США у 1947 році прийнято Privacy Act, у котрому американський Конгрес вперше встановлює зв'язок між правом на приватне життя і персональні дані. Даний закон встановлює, що особисте життя людини може бути безпосередньо зачеплене внаслідок збору, використання та поширення персональної інформації органами державної влади. Проте, цей та інші правові акти не можна назвати повноцінним законом, що регулює обробку персональної інформації. Разом із тим, право на захист персональних даних починає виходити із тіні права на особисте життя.

На початку другої половини XX ст. починають розвиватися інформаційні технології, котрі дозволяли значно швидше опрацьовувати більшу кількість інформації. У 60-ті роки ці технології стають усе більш доступними, що викликало певне занепокоєння Ради Європи.

Так, у 1968 році Парламентська Асамблея публікує рекомендацію №509. У ній висловлюється стурбованість щодо можливих загроз праву на особисте життя, котрі виникають внаслідок використання нових технологій обробки даних. У результаті, Асамблея доручила Комітету з прав людини дослідити дане

питання. Багато хто вважає, що саме цей момент став відправною точкою для Data Privacy [81].

Головним піонером у сфері Data Privacy стала саме Німеччина: перший національний закон про персональні дані (Bundesdatenschutzgesetz) з'являється у 1977 році у ФРН [85]. Особливе ставлення німецької громадськості до даного питання обумовлюється, перш за все, локальними історичними подіями: в середині XX ст. німці пережили два політичних режими – Третій Рейх та НДР. Обидва режими базувалися, крім іншого, на масовому стеженні за населенням. Такі потрясіння привели до надзвичайної витребуваності конфіденційності. Саме тому Німеччина досі вважається одним зі світових лідерів у захисті особистого життя та персональних даних.

Іншою значимою для Data Privacy країною є Франція, котра «відстала» від Німеччини лише на рік. Прийняття у 1978 році Закону про інформатику та громадянські свободи також було пов'язано із локальними подіями. На початку 70-х років французький уряд розробив проект SAFARI, сутність котрого полягала у створенні єдиного реєстру даних із використанням номеру соціального страхування, що дозволяло би ідентифікувати будь-якого громадянина. Обробку всієї інформації планувалося здійснювати завдяки передовим на той час обчислювальним технологіям.

У 1974 році газета Le Monde публікує про це статтю із назвою «SAFARI ou la chasse aux Français» (САФАРІ або полювання на французів) та провокує гучний скандал на тему масового стеження. Під тиском громадськості уряд був вимушений відступити, що привело до прийняття вище згаданого закону і створенню Комісії з інформатики та громадянських свобод. Попри те, уникнути реалізації проекту не вдалось, але нова Комісія змогла встановити певні обмеження щодо обробки персональних даних [76].

Німецький і французький закони стають наріжним каменем для персональних даних та дають відчутний імпульс для розвитку цієї сфери. На проблему починають звертати увагу усе більше й більше країн, а також міжнародних організацій.

У цей період у Конституції СРСР 1977 року громадянам декларативно гарантувалася недоторканість особистості, житла, а також охорона законом особистого життя, таємниці листування, телефонних розмов і телеграфних повідомлень. У ст. 57 Конституції 1977 року передбачалося, що повага особистості, охорона прав і свобод громадян – зобов'язання всіх державних органів, громадських організацій та посадових осіб.

Водночас в УРРС у 1978 році у зв'язку із ратифікацією Міжнародного пакту про громадянські та політичні права від 16 грудня 1966 року було прийнято нову Конституцію УРСР. Конституція УРСР 1978 року стала першою і єдиною за увесь період існування СРСР конституцією, котра містила окремий, стандартний для розвинутих європейських країн, розділ щодо комплексу громадянських, політичних, економічних, соціальних і культурних прав [29].

Зрозуміло, що жодним чином про захист персональних даних у цих соціалістичних конституціях не йшлося, хоча самі по собі вони стають справжнім юридичним «проривом» у контексті демократизації життя радянських громадян.

У 1980 році організація економічної співпраці та розвитку публікує Гайдлайни щодо захисту персональних даних із урахуванням розвитку комп'ютерних технологій, що триває, та їх використання для комерційних трансакцій. За рік по тому було укладено перший міжнародний договір у сфері Data Privacy.

Принципи, закладені у Європейській конвенції про захист прав і основних свобод, набули розвитку в спеціальних нормах Конвенції Ради Європи про захист прав фізичних осіб щодо автоматичної обробки персональних даних 1981 року. У цій Конвенції захист даних розглядається як захист основних прав і свобод індивідів, зокрема, їх права на недоторканість особистого життя щодо обробки персональних даних.

Після цього розпочинається сучасний етап становлення нормативно-правового забезпечення захисту персональних даних в Європейському Союзі. Як наголошують сучасні дослідники, у процесі формування та розвитку правове

регулювання захисту персональних даних у Європейському Союзі пройшло чотири етапи.

Нормативно-правові засади державного управління у сфері захисту персональних даних представлені спеціальним законодавчим актом та окремими нормами включеними до інших законів. Мова йде про Закон України «Про захист персональних даних», який по факту є національною імплементацією стандартів «Загального регламенту про захист даних». 21 липня 2000 р. у відповідь на Директиву 95/46/ЄС Міністерство торгівлі США прийняло Принципи відповідності вимогам інформаційної безпеки ЄС (International Safe Harbor Privacy Principles), запропонувавши компаніям дотримуватися їх [89].

У рішенні Європейської Комісії 2000/520/ЄС визнається, що ці принципи забезпечують необхідний захист [78]. Крім того, в цілях гармонізації був створений механізм затвердження міжнародними корпораціями спеціальних, єдиних корпоративних правил обробки персональних даних [23, с. 67].

Сучасні вимоги щодо обробки персональних даних передбачають необхідність дотримання наступних вимог:

1. Обробка персональних даних має здійснюватися на законній та справедливій основі.

2. Обробка персональних даних має обмежуватися досягненням конкретних, заздалегідь визначених та законних цілей. Не допускається обробка персональних даних, несумісна з метою збору персональних даних.

3. Не допускається об'єднання баз даних, що містять персональні дані, обробка яких здійснюється в цілях, несумісних між собою.

4. Обробці підлягають лише персональні дані, що відповідають цілям їхньої обробки.

5. Зміст і обсяг персональних даних, що обробляються, повинні відповідати заявленим цілям обробки. Персональні дані, що обробляються, не повинні бути надмірними по відношенню до заявлених цілей їх обробки.

6. При обробці персональних даних повинні бути забезпечені точність персональних даних, їх достатність, а в необхідних випадках та актуальність

щодо цілей обробки персональних даних. Оператор повинен вживати необхідних заходів або забезпечувати їх прийняття за видаленням або уточненням неповних або неточних даних.

7. Зберігання персональних даних має здійснюватися у формі, що дозволяє визначити суб'єкта персональних даних, не довше, ніж цього вимагають мети обробки персональних даних, якщо термін зберігання персональних даних не встановлений законом, договором, стороною якого вигодонабувачем або поручителем за яким є суб'єкт персональних даних.

Оброблювані персональні дані підлягають знищенню чи знеособлення по досягненні цілей обробки чи разі втрати необхідності у досягненні цих цілей, якщо інше не передбачено законом.

У нормативно-правовій сфері проблема в тому, що Закон України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності» від 05.04.2007 р. № 877-V на здійснення заходів щодо контролю у сфері захисту персональних даних навряд чи можна поширити, оскільки ця сфера відносин не є видом господарської діяльності.

На сьогодні законодавче регулювання порядку проведення перевірок у сфері захисту персональних даних обмежується однією статтею Закону про захист персональних даних (згідно зі ст. 22 контроль за дотриманням законодавства про захист персональних даних у межах повноважень, передбачених законом, здійснює уповноважений державний орган з питань захисту персональних даних). Держнагляд та контроль за дотриманням законодавства про захист персональних даних, мала б робити окрема державна служба, яка розробляє та затверджує плани перевірок власників баз персональних даних, проводить у межах своїх повноважень виїзні та невиїзні перевірки, видає обов'язкові для виконання приписи щодо усунення порушень законодавства про захист персональних даних, що складає адмінпротоколи про виявлені порушення законодавства.

Слід звернути увагу, що законодавство вказують на необхідність встановлення наглядових повноважень на рівні закону. Поки що порядку

проведення перевірок немає не лише в законі, а й у підзаконних нормативних актах

Правові аспекти регулювання управлінням у сфері захисту персональних даних наведено у таблиці 2.1.

Таблиця 2.1 Правове регулювання управлінням у сфері захисту персональних даних

Вид нормативно-правового акту	Зміст правового регулювання
Конституція України	Ст. 32 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.
Закон України «Про захист персональних даних» від 01 червня 2010 року	Закон регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних.
Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних, підписана в Страсбурзі 28 січня 1981 року	Конвенція поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів
Наказ Уповноваженого Верховної Ради України з прав людини №1/02-14 від 08 січня 2014 року “Про затвердження документів у сфері захисту персональних даних”	Порядком обробки персональних даних (далі - Порядок) визначено загальні вимоги до обробки та захисту персональних даних суб’єктів персональних даних, що обробляються повністю чи частково із застосуванням автоматизованих засобів, а також персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів.

Примітка. Складено автором.

Таким чином, сьогодні, як мінімум необхідно здійснити приведення змісту Закону України «Про захист персональних даних» у відповідність до Загального регламенту про захист даних Європейського Парламенту та Ради, який застосовується з 25 травня 2018 р.;

2.2 Суб'єкти державного управління у сфері захисту персональних даних

Ключовим суб'єктом відносин, що виникають з приводу персональних даних, є їх суб'єкт. Легальне визначення поняття «суб'єкт персональних даних» дано в ч. 1 ст. 2 Закону України «Про захист персональних даних» [53],

Основні публічно-правові суб'єкти управлінням у сфері захисту персональних даних відображено у табл.2.2.

Комплаєнс-проект – це насамперед дослідження бізнес-процесів у компанії на предмет «залучення» до них персональних даних, виконання юридичних, організаційних та технічних заходів захисту, включаючи підготовку необхідної документації для забезпечення відповідності вимогам законодавства, а також проведення тренінгу з роботи з персональними даними. Це комплексна та досить популярна послуга, яка зараз має запит серед клієнтів .

Таблиця 2.2 Основні публічно-правові суб'єкти управлінням у сфері захисту персональних даних

Вид нормативно-правового акту	Зміст правового регулювання
«Контролер даних» (Data Controller)	фізична чи юридична особа, орган публічної влади, агентство чи інший орган, який самостійно чи спільно з іншими визначає цілі та засоби опрацювання персональних даних
«Оператор даних» (Data Processor)	фізична чи юридична особа, орган публічної влади, агентство чи інший орган, який опрацьовує персональні дані від імені контролера

Примітка: Розроблено автором

Займає друге місце за запитом, одразу після загального юридичного консалтингу. При виконанні комплаєнс-проектів досліджують та оцінюють всі бізнес-процеси компанії, з'ясовують, за якими «каналами» вона отримує та передає персональні дані у групі компаній, наприклад, на користь контрагентів.

Основні типи персональних даних – це дані працівників та дані клієнтів (контрагентів). Бувають також різні цілі, способи, терміни та правові підстави для обробки даних. Для всіх категорій суб'єктів персональних даних ми малюємо матрицю, на основі якої формуємо необхідний комплект документів.

Як правило, компанія вже має 5–10 документів і вона думає, що цього достатньо, щоб відповідати закону. Доводиться розчаровувати клієнта і пояснювати, що цього недостатньо. Часто, наприклад, у компаніях немає положення про відеоспостереження, положення про архів, положення про пропускний режим. Необхідно підготувати повноцінний комплект документів, який відповідає всім вимогам законодавства. Деякі компанії вважають, що вони можуть не подавати таке повідомлення. Але на практиці під виняток із цього правила майже ніхто не підпадає.

Структура діяльності з «Опрацювання даних», яка означає будь-яку операцію або низку операцій з такими персональними даними відображена на рисунку 2.1

Рисунок 2.1. - Структура діяльності з «Опрацювання даних», яка означає будь-яку операцію або низку операцій з такими персональними даними

Примітка. Розроблено автором.

У комплаєнс-проектах є не лише правова, а й технічна складова, про яку я згадав. Пов'язана вона з кількома перевіреними та досвідченими субпідрядниками – спеціалізованими ІТ-компаніями, які мають потрібні ліцензії для такої роботи. Ці організації допомагають нашим клієнтам реалізувати технічні заходи щодо безпеки персональних даних при їх обробці в інформаційних системах. Наприклад, проводять аудит інформаційних систем персональних даних, допомагають вибрати рівень захищеності персональних даних у ІТ-системах, готують модель загроз, консультують із різних питань інформаційної безпеки.

Якщо обробка персональних даних здійснюється державним органом, органом місцевого самоврядування, які діють виключно в межах повноважень, визначених законом, то зазвичай обсяг та мета обробки вже сформульовані відповідними актами законодавства, що регламентують діяльність таких володільців.

Термін «контролер файлу» означає фізичну або юридичну особу, державний орган, установу чи будь-який інший орган, що уповноважений відповідно до національного законодавства вирішувати, яким повинно бути призначення файлу даних для автоматизованої обробки, які категорії персональних даних повинні зберігатися та які операції повинні здійснюватися з ними.

Стаття 22 Закону України «Про захист персональних даних» говорить, що **к**онтроль за додержанням законодавства про захист персональних даних у межах повноважень, передбачених законом, здійснюють такі органи:

1) Уповноважений (Уповноважений Верховної Ради України з прав людини включає до своєї щорічної доповіді про стан додержання та захисту прав і свобод людини і громадянина в Україні звіт про стан додержання законодавства у сфері захисту персональних даних);

2) суди.

Нажаль інших органів наділених публічно-правовими повноваженнями там не передбачено.

Водночас, законодавство вимагає, аби володільці, розпорядники персональних даних та треті особи зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.

В органах державної влади, органах місцевого самоврядування, а також у володільцях чи розпорядниках персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до цього Закону, створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних при їх обробці.

Таким чином, контролерам персональних даних докласти зусиль для визначення та призначення відповідального за захист персональних даних, оскільки це може бути сильним союзником для контролера персональних даних/обробника у процесі забезпечення відповідності обробки персональних даних.

Володільцем персональних даних можуть бути підприємства, установи і організації усіх форм власності, органи державної влади чи органи місцевого самоврядування, фізичні особи-підприємці, які обробляють персональні дані на законних підставах.

Якщо персональні дані щодо однієї й тієї ж особи, на достатній правовій підставі обробляються (зберігаються) різними суб'єктами (фізичними чи юридичними особами), кожна така особа є самостійним володільцем персональних даних.

Якщо право приймати рішення щодо обробки однієї бази персональних даних мають декілька суб'єктів, то вони виступають співволодільцями цієї бази. Проте, якщо той чи інший співволоділець має право самостійно приймати рішення щодо обробки окремої частини бази персональних даних, то він в повній мірі є володільцем цього об'єму даних.

Володілець має право здійснювати обробку персональних даних тільки на законних підставах і виключно тих даних, які відповідають законній меті обробки.

Державно-владні суб’єкти (державні органи, органи місцевого самоврядування) мають право обробляти персональні дані тільки в тому випадку, коли це необхідно для виконання ними своїх повноважень, визначених законом.

Залежно від ролі, яку виконують усі суб’єкти відносин, пов’язаних з персональними даними, їх можна поділити на дві групи:

– основні, участь яких є обов’язковою. До цієї групи належать суб’єкт персональних даних, володілець персональних даних та Уповноважений з прав людини. Їх участь є невід’ємним елементом захисту персональних даних;

– факультативні, тобто суб’єкти, які можуть не брати участь у вказаних правовідносинах, що не вплине на їх хід та результати, а в разі такої участі їх становище значно обмежене. До них слід віднести розпорядника та третю особу.

Окремо наголосимо, що суб’єкти персональних даних наділені рядом важливих прав.

До найбільш важливих повноважень суб’єктів прав персональних даних:

1. Суб'єкт має право отримання інформації, що стосується обробки його персональних даних, у тому числі що містить:

- підтвердження факту обробки персональних даних оператором;

- правові підстави та цілі обробки персональних даних;

- цілі та застосовувані оператором способи обробки персональних даних;

- найменування та місце знаходження оператора, відомості про осіб (за винятком працівників оператора), які мають доступ до персональних даних або яким можуть бути розкриті персональні дані на підставі договору з оператором або на підставі закону;

- оброблювані персональні дані, які стосуються відповідного суб'єкту персональних даних, джерело їх отримання, якщо інший порядок подання таких даних не передбачено національним законом;

- терміни обробки персональних даних, зокрема терміни їх зберігання; порядок здійснення суб'єктом персональних даних прав, передбачених законодавством;

- інформацію про здійснену або про передбачувану транскордонну передачу даних;

- найменування або прізвище, ім'я, по батькові та адресу особи, яка здійснює обробку персональних даних за дорученням оператора, якщо обробка доручена або буде доручена такій особі.

2. Суб'єкт персональних даних має право вимагати від оператора уточнення його персональних даних, їх блокування або знищення у разі, якщо персональні дані є неповними, застарілими, неточними, незаконно отриманими або не є необхідними для заявленої мети обробки, а також вживати передбачених законом заходів щодо захисту своїх прав .

Відомості повинні бути надані суб'єкту персональних даних оператором у доступній формі, і в них не повинні утримуватись персональні дані, що належать до інших суб'єктів персональних даних, за винятком випадків, якщо є законні підстави для розкриття таких персональних даних.

3. Відомості надаються суб'єкту персональних даних або його представнику оператором при зверненні або отриманні запиту суб'єкта персональних даних або його представника.

Запит повинен містити номер основного документа, що засвідчує особу суб'єкта персональних даних або його представника, відомості про дату видачі зазначеного документа та орган, що видав його, відомості, що підтверджують участь суб'єкта персональних даних у відносинах з оператором (номер договору, дата укладання договору, умовне словесне позначення та (або) інші відомості), або відомості, що іншим чином підтверджують факт обробки персональних даних оператором, підпис суб'єкта персональних даних або його представника. Запит може бути направлений у формі електронного документа та підписаний електронним підписом відповідно до законодавства України.

У разі, якщо відомості, а також оброблювані персональні дані були надані для ознайомлення суб'єкту персональних даних на його запит, суб'єкт персональних даних має право звернутися повторно до оператора або направити йому повторний запит з метою отримання відомостей та ознайомлення з такими персональними даними не раніше ніж через тридцять. днів після початкового звернення чи направлення первинного запиту, якщо коротший термін встановлено законом, прийнятим відповідно до ним нормативним правовим актом чи договором, стороною якого або вигодонабувачем або поручителем яким є суб'єкт персональних даних.

4. Суб'єкт персональних даних має право звернутися повторно до оператора або направити йому повторний запит з метою отримання відомостей, а також для ознайомлення з оброблюваними персональними даними до закінчення терміну, зазначеного в законодавстві, у разі, якщо такі відомості та (або) оброблювані персональні дані були надані йому для ознайомлення повному обсязі за результатами розгляду первинного звернення..

5. Оператор має право відмовити суб'єкту персональних даних у виконанні повторного запиту, що не відповідає умовам, передбаченим законодавством. Така відмова має бути мотивованою. Обов'язок подання доказів обґрунтованості відмови у виконанні повторного запиту лежить на операторі.

Окремо наголосимо, що до суб’єктів управління (та захисту прав персональних даних) також необхідно віднести окремі установи та організації. Законодавства про захист персональних даних передбачає як окрему підставу для використання персональних даних дозвіл на обробку персональних даних, наданий власнику бази персональних даних згідно із законом виключно для здійснення своїх повноважень.

Тому, скажімо, роботодавець цілком міг би послатися на це положення Закону для обґрунтування відсутності необхідності отримання згоди працівників на використання їх персональних даних, тим більше, що реалізовувати вимоги трудового законодавства без таких даних у принципі неможливо.

І якщо, наприклад, працівник відповість роботодавцю відмовою, то, по суті, така відмова має стати окремою підставою для розірвання трудового договору, оскільки роботодавець просто опиняється у безвихідній ситуації.

На наш погляд, розумніше не стільки вимагати згоду працівників на використання їх персональних даних у необхідному для роботи обсязі, скільки ознайомити їх із наданими ним законодавчими гарантіями щодо захисту персональних даних.

РОЗДІЛ 3. УДОСКОНАЛЕНЯ ОРГАНІЗАЦІЙНО-УПРАВЛІНСЬКИХ ЗАСАД УПРАВЛІННЯ У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

3.1 Удосконалення сфери публічного контролю та юридичної відповідальності у контексті державного управління у сфері захисту персональних даних

У контексті побудови національної системи захисту персональних даних суб'єктами публічного управління на особливу увагу заслуговують нормативно-правові акти ЄС.

Європейська рада щодо захисту персональних даних — це незалежний орган ЄС, який сприяє послідовному застосуванню правил захисту даних у всьому Європейському союзі, а також сприяє співпраці між органами захисту даних ЄС.

Європейська рада щодо захисту персональних даних складається з керівників одного наглядового органу від кожної держави-члена ЄС, а також Європейського інспектора захисту персональних даних або з їх представників.

У випадку, коли в державі-члені більше одного наглядового органу, які є відповідальними за моніторинг застосування положень щодо персональних даних, призначається єдиний представник відповідно до права такої держави-члена.

Водночас, Європейська Комісія має право брати участь у діяльності та засіданнях Європейської ради щодо захисту персональних даних без права голосу. Для цього Європейська Комісія призначає свого представника. Голова Європейської ради щодо захисту персональних даних інформує Європейську Комісію про діяльність Європейської ради захисту персональних даних.

Крім того у випадках, передбачених у Статті 65 GDPR Європейський інспектор із захисту персональних даних має право голосу лише за рішеннями, що стосуються принципів та норм, що застосовуються до установ, органів, відомств та агентств Союзу, які відповідають змісту цього Регламенту [86].

Таким чином, Європейська рада щодо захисту персональних даних складається з представників національних органів захисту даних та окремих представників інших органів ЄС. Європейська рада щодо захисту персональних даних має власний секретаріат, що відповідає за організацію її діяльності.

Відповідно до концепції *європейського консенсусу* Європейська рада щодо захисту персональних даних прагне забезпечити узгоджене застосування на рівні Регламенту 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 р. «Про захист фізичних осіб щодо обробки персональних даних та про вільне переміщення таких даних».

При цьому наголосимо, що європейський консенсус насамперед визначається на двох рівнях. По-перше, його можна визначити на рівні правил, під якими мають на увазі конкретні імплементаційні заходи, які вживаються для реалізації правового принципу в конкретній системі.

По-друге, консенсус може діяти на рівні власне принципів, під якими мають на увазі ті загальні концепції, які лежать в основі національних правових стандартів [84, С.13]. Європейський консенсус – це концепція, яка використовується органами влади ЄС та ЄСПЛ, і випливає з еволюційного характеру тлумачення Європейської конвенції про права людини.

Європейська рада щодо захисту персональних даних може приймати загальні керівні принципи для роз'яснення конкретних умов європейського законодавства про захист даних, надаючи зацікавленим сторонам послідовне тлумачення їхніх прав та обов'язків.

Загальний регламент про захист даних також дає право Європейській раді щодо захисту персональних даних приймати обов'язкові рішення, адресовані національним органам нагляду, для забезпечення послідовного виконання його положень.

Коло завдань та повноважень Європейської ради щодо захисту персональних даних, окреслено у ст. 70 GDPR, в якій виділяються наступні завдання:

- надавати загальні керівні роз’яснення (включаючи посібники, рекомендації та практичний досвід) для роз'яснення законодавства про захист персональних даних;

- консультувати Європейську Комісію з будь-яких питань, що стосуються захисту персональних даних, та щодо будь-якого нового запропонованого законодавства, на рівні Європейського Союзу;

- приймати висновки щодо механізму забезпечення узгодженості у транскордонних справах, пов'язаних із захистом персональних даних;

- сприяти співпраці та ефективному обміну інформацією та передовим досвідом між національними наглядовими органами [86].

Європейської ради щодо захисту персональних даних має складати річний звіт про свою діяльність щодо захисту прав персональний даних фізичних осіб щодо їх обробки в ЄС, та, якщо необхідно, у третіх країнах та міжнародних організаціях.

Важливим елементом входження України у європейський простір захисту персональних даних є отримання статусу спостерігача при Європейській раді щодо захисту персональних даних. Серед наших держав-сусідів такий статус з 2018 року має Республіка Молдова

Наприклад, прийняття Республіки Молдова в якості члена зі статусом спостерігача до Європейської ради щодо захисту персональних даних є першим і великим досягненням у Східному регіоні Європи, і в даний час Республіка Молдова є єдиною державою з таким статусом в Європейській Раді з питань захисту даних. Подібне досягнення для України також буде сприяти досягненню взаємовідносин між Україною та Європейським Союзом як в економічному, так і політичному плані.

Сучасний етап розвитку суспільства характеризується зростаючою роллю інформаційної сфери та інтенсивним розвитком автоматизованих технологій у сфері обробки та передачі даних. Впровадження їх у всі соціальні сфери підвищує уразливість приватного життя дитини, створює загрози незаконного обігу персональних даних неповнолітніх.

У сьогоднішньому світі вже важко уникнути ідентифікації, але заборонити зберігати інформацію персонального характеру, обробляти її та використовувати з метою, не узгодженою з її суб'єктом, можливо і, безумовно, необхідно, тому громадянам варто звернути увагу на правове регулювання цього питання.

У разі недієздатності суб'єкта персональних даних згоду на обробку його персональних даних дає законний представник суб'єкта персональних даних.

Діти - неповнолітні громадяни, тому їх права захищають батьки та законні представники.

Таким чином, правом надавати згоду на використання особистих відомостей про неповнолітнього наділені його батьки (або інші представники). Свою згоду на роботу з особистою інформацією вони мають висловити письмово з обов'язковим власноручним підписом.

Більшість громадян вже звикли до того, що регулярно підписують згоду на обробку своїх персональних даних або персональних даних своїх неповнолітніх дітей при зверненні до медичних установ, освітніх організацій, держорганів та інших ситуацій.

Законодавство застерігає від зловживання свободою масової інформації: забороняється поширення в засобах масової інформації, а також в інформаційно-телекомунікаційних мережах інформації про неповнолітнього, постраждалого в результаті протиправних дій (бездіяльності), включаючи прізвища, імена, по батькові, фото- та відеозображення такого неповнолітнього батьків та інших законних представників, дату народження такого неповнолітнього, аудіозапис його голосу, місце його проживання або місце тимчасового перебування, місце його навчання або роботи, іншу інформацію, що дозволяє прямо чи опосередковано встановити особу такого неповнолітнього, за винятком випадків, передбачених законом.

Винятком є ситуації, коли поширення такої інформації здійснюється з метою захисту прав та законних інтересів неповнолітнього, який постраждав у результаті протиправних дій (бездіяльності). У таких випадках така інформація може поширюватися:

1) за згодою неповнолітнього, який досяг чотирнадцятирічного віку та постраждалого внаслідок протиправних дій (бездіяльності), та його законного представника;

2) за згодою законного представника неповнолітнього, який не досяг чотирнадцятирічного віку та потерпілого внаслідок протиправних дій (бездіяльності);

3) без згоди неповнолітнього, який досяг чотирнадцятирічного віку та постраждалого внаслідок протиправних дій (бездіяльності), та (або) законного представника такого неповнолітнього, якщо отримати цю згоду неможливо або якщо законний представник такого неповнолітнього є підозрюваним або обвинуваченим у вчиненні даних протиправних дій.

При цьому до поширення інформації, що стосується неповнолітнього потерпілого від злочину проти статевої недоторканності та статевої свободи особи, встановлено додаткові вимоги.

Така інформація може бути поширена у ЗМІ лише з метою розслідування злочину, встановлення осіб, причетних до скоєння злочину, розшуку зниклих неповнолітніх у обсязі, необхідному для досягнення зазначених цілей, та з дотриманням вимог.

Дані попереднього розслідування можуть бути оприлюднені лише з дозволу слідчого, дізнавача і лише в тому обсязі, в якому ними буде визнано це допустимим, якщо розголошення не суперечить інтересам попереднього розслідування та не пов'язане з порушенням прав та законних інтересів учасників кримінального судочинства.

Варто зазначити, що зображення людини також відноситься до її персональних даних, а отже, використання фотографій усіх громадян (у тому числі неповнолітніх) регулюється нормами закону. Охорона зображення громадянина захищена Цивільним кодексом України, яка свідчить, що оприлюднення та подальше використання зображення громадянина (у тому числі його фотографії, а також відеозаписи або твори образотворчого

мистецтва, в яких його зображено) допускаються лише за згодою цього громадянина.

Після смерті громадянина його зображення може використовуватися тільки за згодою дітей та чоловіка або жінки померлого, а за їх відсутності - за згодою батьків. Така згода не потрібна у випадках:

1. Використання зображення здійснюється у державних, суспільних чи інших громадських інтересах;

2. Зображення громадянина отримано під час зйомки, яка проводиться у місцях, відкритих для вільного відвідування, або на публічних заходах (зборах, з'їздах, конференціях, концертах, виставах, спортивних змаганнях та подібних заходах), за винятком випадків, коли таке зображення є основним об'єктом використання;

3. Громадянин позував за плату.

За публікацію фотографій дітей в інтернеті без згоди їхніх батьків має бути передбачена відповідальність.

Батькам, які нерідко викладають фотографії улюблених дітей у соціальних мережах, слід розуміти, що публікуючи щось в інтернеті, вони публікують це назавжди. І дитина навіть через багато років може мати наслідки від публікації фотографії, зробленої, коли вона була в дитячому садку. Без крайньої необхідності не публікуйте в мережі ПІБ дітей, відомості про них (а це персональні дані) та їх фотографії. І не забувайте про можливі наслідки, коли даєте свою згоду на використання зображення своєї дитини (підопічного) у ЗМІ.

Таким чином, у контексті захисту дітей у кіберпросторі «правильніше буде говорити про дані взагалі, тобто про особисту інформацію, яку сама дитина, її родичі та друзі можуть залишати в інтернеті», – пояснює експерт.

«На відміну від використання персональних даних дорослих, метою якого найчастіше є саме кіберзлочин, тобто кримінальні дії для отримання певної вигоди (зазвичай фінансової – наприклад, крадіжка грошей з рахунку), що здійснюються з використанням інтернету, метою використання даних про дитину в 99% випадків є шантаж батьків в офлайні. Чинним кримінальним

законодавством (ст. 163) це сприймається як звичайний злочин. Інформацію про дитину обов'язково слід тримати в таємниці».

Потраплення персональних даних до рук зловмисників однозначно матиме вкрай негативні наслідки. У зв'язку з цим він наводить кілька ситуацій.

Саме по собі розкриття паспортних даних нічим не загрожує підлітку – історії про кредити на чужий паспорт залишилися в минулому, оскільки банки навчилися ретельно перевіряти інформацію від того, хто подає заявку на кредит. Ризик може виходити тільки від мікрокредитних організацій, які можуть дати позику за чужим паспортом, але це рідкісний випадок. Незаконність подібних дій легко можна буде довести.

По прізвищу та імені дитини зловмисник може знайти її в соціальних мережах та розпочати спілкування. Цілі такого спілкування можуть бути різними – від отримання інформації про дохід сім'ї з метою подальших злочинів проти власності (квартирна крадіжка, пограбування) і до особистої зустрічі з дитиною з метою викрадення, наприклад. Крім того, всі пам'ятають бурхливі обговорення діяльності зловмисників, які давали дітям різні завдання у соціальних мережах, супроводжуючи ці вказівки погрозами нашкодити сім'ї у разі відмови підкорятися.

Деякі батьки використовують ім'я дитини як кодове слово для банку, чим також можуть скористатися шахраї.

Дата народження може бути використана для входження в довіру до дитини – адже лише добрі люди знають цю дату та готові зробити подарунок. Варіантів безліч - обіцянки перевести гроші як подарунок на батьківську картку, для чого "дарувальнику" потрібно знати всі дані картки. Незнайомець може також підійти «з подарунком» на вулиці та запропонувати сходити у кафе відсвяткувати(відзначити свято). Дату народження дітей батьки також часто використовують як кодовий набір символів для проведення фінансових операцій.

За допомогою фотографій, які викладає дитина, можна отримати повне уявлення як про дитину, так і про її сім'ю: рівень доходу, коли вони збираються у відпустку, коли вони вже були у відпустці, де відпочиває сім'я. Зловмисник

дізнається найціннішу для себе інформацію – коли будинок буде пустувати. Багато чого можна дізнатися і про саму дитину: в якій школі вчиться, з ким дружить, якими вулицями ходить, в яких секціях займається. Все це може бути використане як для налагодження безпосереднього контакту з дитиною, так і для шантажу батьків, для яких зловмисники справляють враження, що знають про дитину дуже багато.

Номер телефону та e-mail.

Щодо номера телефону, то, по-перше, це небажані дзвінки від незнайомих людей. По-друге, SMS-розсилка з фішинговими посиланнями. Ну і, звичайно, саме знання номера телефону дитини шахраєм змусить батьків хвилюватися ще більше (коли вони, наприклад, отримають SMS із проханням перевести 5000 рублів, тому що їхній син розбив вікно в будинку, підтверджене номером телефону дитини).

Знання адреси електронної пошти є ще одним каналом прямого контакту з дитиною. А також канал для спам-розсилок, які можуть містити фішингові посилання. Загалом чим більше інформації про дітей має зловмисник, тим більше він зможе отримати від батьків.

Витік персональних даних може статися з об'єктивних причин, наприклад, через технічний збій, або по суб'єктивних, до яких належать недбалість співробітників, атаки хакерів або корисливі цілі персоналу.

У будь-якому разі, якщо паспортні або інші персональні дані в результаті опиняться в руках зловмисників, вони можуть використовуватись у злочинних цілях.

Використовуючи ПДН, можна отримати доступ до коштів на банківських картках жертви, а також взяти кредити у кількох банках на ім'я потерпілого. Надалі стягувати борг за зловмисниками колектори будуть саме з тієї особи, на яку оформлено позику, доки особа не доб'ється свого визнання жертвою шахрайства.

Отримавши доступ до персональних даних, можна здійснювати й інші юридичні дії: незаконні маніпуляції з нерухомістю інших осіб, переведення боргів, відкриття так званих фірм-одноденок.

Структура системи контролю та управління ризиками, які можуть виникнути через недотримання умов GDPR наведено у табл.3.1.

У сукупності юридична відповідальність за порушення норм персональних даних далека від своєї досконалості, однак, вже достатньо багато зроблено в рамках Кодексу про працю, Цивільного кодексу, Кодексу про адміністративні правопорушення, Кримінального кодексу та інших нормативно-правових актів.

Основним недоліком існуючої юридичної відповідальності за порушення норм персональних даних є відсутність взаємопов'язаності між різними сферами обороту персональних даних.

Таблиця 3.1 Структура системи контролю та управління ризиками, які можуть виникнути через недотримання умов GDPR

Складова	Сутність
GDPR compliance як система контролю та управління ризиками, які можуть виникнути через недотримання умов GDPR	Відповідно до умов GDPR, компанії, установи, організації не тільки повинні забезпечити, щоб персональні дані були зібрані на законних підставах і під жорсткими умовами, а й зобов'язані захищати їх від зловживання та експлуатації, а також поважати права власників даних – або їм загрожує покарання за це.
Data Protection Officer (DPO) - це особа, яка повинна призначатися контролером та/або оператором даних з метою забезпечення відповідності їхньої діяльності положенням GDPR у наступних випадках:	опрацювання здійснює публічний орган або установа, за винятком судів, що діють як судові інстанції; основні види діяльності контролера або оператора становлять операції опрацювання, які, в силу їхньої специфіки, обсягів та/чи цілей, вимагають регулярного, систематичного і широкомасштабного моніторингу суб’єктів даних; або основні види діяльності контролера або оператора становлять широкомасштабне опрацювання спеціальних категорій даних та персональних даних про судимості і кримінальні злочини

Примітка: Складено автором

Серед інших недоліків слід виділити, по-перше, відсутність комплексності у забезпеченні юридичної відповідальності за порушення норм про персональні дані, а цілий ряд норм взагалі є окремими фрагментами зазначеної діяльності, системно між собою не пов'язані, по-друге, у нормативно-правових актах відсутній системний підхід у регулюванні відносин, пов'язаних із захистом персональних даних за допомогою юридичних санкцій; по-третє, наявність суттєвих недоліків у юридико-технічному конструюванні самих складів правопорушень, що стосуються досліджуваних відносин.

Слід констатувати(зазначити), що недоліки в юридико-технічному конструюванні самих складів правопорушень, які стосуються досліджуваних відносин, часом істотно знижують ефективність їх застосування. В інших випадках їх зміст виявляється вужчим або взагалі відрізняється від назви відповідних статей.

У державі ще не сформувалася сучасна інфраструктура загальної інформатизації і, зокрема, сфери персональних даних, які здатні задовольнити потреби зацікавлених суб'єктів інформаційно-обчислювального обслуговування на необхідному рівні, не організовані інформаційні ресурси персональних даних у системі баз даних. У недержавному секторі, хоча інформаційні технології і широко використовуються в різних сферах, це поки що не позначилося на забезпеченні правомірного накопичення та зберігання персональних даних з використанням інформаційних технологій. Для вирішення існуючої проблеми держава має визначити ступінь своєї участі у регулюванні процесів створення та функціонування закритих недержавних (корпоративних) систем, а також відкритих систем насамперед на користь захисту прав громадян.

Ключові повноваження державного наглядового органу у сфері захисту персональних даних відображено у табл.3.2.

Таблиця 3.2 Ключові повноваження державного Наглядового органу у сфері захисту персональних даних

Види повноважень	Зміст діяльності
1) «Слідчі» повноваження	• видавати розпорядження надати будь-яку інформацію, яку він вимагає для виконання своїх завдань; • проводити розслідування в формі перевірок захисту даних; • здійснювати перегляд сертифікацій; • повідомляти про передбачуване порушення Регламенту; • доступ до всіх персональних даних і до всієї інформації, необхідної для виконання його завдань; • доступ до будь-яких приміщень та/або будь-якого обладнання і засобів опрацювання даних контролера і оператора.
2) Контрольно-виправні повноваження	• надсилати попередження контролеру або оператору про те, що призначені операції опрацювання ймовірно порушать положення Регламенту; • виносити догану контролеру або оператору, якщо операції опрацювання порушують положення Регламенту; • накладати тимчасове чи остаточне обмеження, в тому числі, заборону, на опрацювання; • накладати адміністративні штрафи, залежно від обставин кожної індивідуальної справи; • наказувати призупинення потоків даних до одержувача в третій країні чи до міжнародної організації.

Примітка. Складено автором.

Виходячи з того, що поширення конфіденційної інформації персонального характеру становить більш істотну суспільну небезпеку для конкретних громадян, ніж інші відносини, властиві інформаційним процесам, вирішення питання про врегулювання порядку розповсюдження персональних даних більш ніж актуально в даний час і потребує уважного та якнайшвидшого розгляду.

Враховуючи прогалини правового регулювання Інтернету, вони мають бути усунені у новому інформаційному законодавстві.

Поряд із законом, що регулює державну політику в Мережі, слід ухвалити рамковий закон про Інтернет. У ньому, як вважає автор, необхідно:

1) відпрацювати понятійний апарат із залученням відповідних експертів у галузі технічних знань для вироблення чітких законодавчих понять;

2) закріпити найважливіші принципи «мережевих відносин»;

3) відобразити специфіку суб'єктного складу мережевих відносин;

4) встановити правила інформаційного обміну у мережі Інтернет;

5) сформулювати відповідальність учасників мережевих відносин за порушення закріплених норм, а також передбачити способи доведення та особливості розгляду «мережевих суперечок»; встановити межі відповідальності кожного учасника мережевих відносин.

Запропоновані норми мають стимулювати операторів персональних даних відповідати за дії підрядників, щоб ті не порушували законодавство. Але ці заходи можуть не спрацювати, оскільки штрафи незначні: щоб законопроекти принесли результат, сплата штрафу повинна коштувати дорожче, ніж запровадження системи захисту інформації.

Такого підходу дотримувалися в Євросоюзі при розробці Загального регламенту захисту даних (GDPR), який набув чинності у травні 2018 року. Його виконання є обов'язковим для всіх організацій, у тому числі російських, при обробці персональної інформації громадян, які перебувають на території ЄС.

Насамперед GDPR стосується компаній, які мають представництва у країнах ЄС.

Крім того, потурбуватися про відповідність вимогам GDPR також мають російські компанії, сайти яких перекладені мовою хоча б однієї країни — члена Євросоюзу або приймають через сайт платежі у валюті країн ЄС.

Максимальний штраф за порушення положень GDPR становить 20 мільйонів євро або 4% від обороту компанії (залежно від того, яка сума більша).

Крім того, серйозним стимулом для операторів ЄС забезпечувати безпеку персональних даних не на папері, а насправді є обов'язок повідомляти наглядовий орган про витік персональних даних.

3.2 Напрями удосконалення організаційно-управлінських засад державного управління у сфері захисту персональних даних (на прикладі митно-податкових відносин)

Отже, стаття 67 Конституції України передбачає обов’язок кожної особи сплачувати податки і збори у порядку і розмірах, встановлених законом [26]. Податки є основою формування державних доходів, що їх одержує держава на підставі своїх владних повноважень для виконання властивих їй функцій. Відповідно охорона податкової системи залишається одним із основних напрямів внутрішньої діяльності держави.

Протиправне невиконання платником податків своїх відповідальність, грубо ігнорує вказаний конституційний обов’язок, у якому втілено публічний інтерес усіх членів суспільства і сумлінне виконання якого справедливо визнається однією з необхідних умов існування соціуму.

Податкове право це система фінансово-правових відносин, що регулює податкові відносини державних органів і платників податків щодо встановлення, зміни та стягнення з платників податків частини їхніх доходів до відповідного бюджету [10, с.11]. Податкове право перебуває на стику з адміністративним правом або навіть входить до нього як самостійний інститут [34. с.105], а також пов’язане з кримінальним правом у частині відповідальності за ухилення від сплати податків.

Методологія податкових перевірок виступає засобом здійснення контролю, результати якого можуть впливати на прийняття рішень щодо притягнення особи до різного роду юридичної відповідальності. Ст. 41 ПК України органи державної фіскальної служби віднесено до переліку контролюючих органів, що здійснюють від імені держави функції контролю за своєчасністю і правильністю сплати суб'єктами господарювання податків і

зборів, зокрема, шляхом проведення документальних невиїзних перевірок платників податків відповідно до ст. 78 ПК України [43].

Положеннями ст. 46 ПК України на платників податків покладено обов'язок з подання податкових декларацій контролюючому органу у строки, встановлені законом, на підставі яких здійснюється нарахування (сплата) податкового зобов'язання.

У разі невиконання платником податків обов'язку щодо подання податкової звітності контролюючий орган в силу ч. 102.1. ст. 102 ПК України має право провести податкову перевірку та самостійно визначити суму грошових зобов'язань платника податків у випадках, визначених ПК України, не пізніше закінчення 1095 дня, що настає за останнім днем граничного строку подання податкової декларації [43].

Під час аналізу неоподаткованих активів потрібно розрізняти незаконні доходи та доходи, які не були задекларовані (або не підлягали декларуванню). Різні країни вирішують це питання по-різному.

Відповідно до податкового законодавства з активів, які не були належним чином оподатковані, податок сплачується шляхом внесення самостійних коригувань до фінансової звітності або донарахування під час проведення податкового контролю. У цьому контексті в обох випадках сплачуються штрафні санкції. Нажаль у вітчизняній практиці використання непрямих методів контролю майнового становища особи не передбачено. Непрямі методи податкового контролю набувають широкого розповсюдження у багатьох державах. Їх використання передбачене податковим законодавством Австралії, Данії, Фінляндії, Греції, Швеції, Великій Британії та ін.

Прийнятий Верховною радою України 15.06.2021 року Закон України, який передбачає податкову амністію та нульове декларування одночасно, має на меті на певний час усунути невизначеність між оподаткованими та неоподаткованими активами, що належать фізичним особам-платникам податків в Україні (резиденти та нерезиденти, які на момент отримання активу були податковими резидентами в Україні).

Проте залишаються відкритими питання порядку проведення перевірок задекларованих у ході податкової амністії активів і посилення заходів податкового контролю після неї, що є чинником, який визначить успішність цієї деклараційної кампанії. Одним із таких заходів має стати запровадження непрямих методів контролю майнового становища платника податку на доходи фізичних осіб. Сьогодні актуалізуються питання, щодо яких є досить високі очікування завдяки потенціалу розвитку міждержавного обміну податковою інформацією, значній цифровізації податкових відносин та розвитку концепції вини платника податку, яку потрібно доводити, використовуючи такі методи доказування.

Непрямі методи застосовуються переважно до фізичних осіб, оскільки, як свідчить досвід, гроші, які не були оподатковані, завжди потрапляють до однієї чи кількох осіб. Зазвичай методи контролю засновані на перевірці доходів і витрат в обов'язкових фінансових книгах та документах, що ведуться платником податків та переносяться до їхніх податкових декларацій. Переоцінка податку базується на різницях, які виникають щодо цих книг та податкових декларацій. У свою чергу непрямі методи визначають податкове зобов'язання шляхом аналізу фінансових операцій, використовуючи інформацію з інших джерел, крім податкових декларацій та офіційних документів фінансової звітності. Як правило, податкова оцінка ґрунтується на детальній інформації, яка вказує на розумне визначення правильного податкового зобов'язання.

Очевидно, що серед держав, які вже запровадили методологію непрямого податкового контролю багато країн-членів ЄС. Відповідно на публічно-правові відносини щодо доступу та використання персональних даних має вплив система встановлених у ЄС нормативних вимог. Правове регулювання відносин з приводу персональних даних має тривалу історію, упродовж котрої було вироблено систему стандартів, які, на наш погляд, найбільш повно розкриваються в джерелах права Ради Європи та ЄС.

Так само достатньо багато країн бувшого пострадянського простору встали на шлях істотних соціально-політичних реформ орієнтиром для яких є

європейські правові та соціальні цінності. Серед таких держав-сусідів України є Республіка Молдова у якій достатньо давно та успішно започатковане використання непрямих методів податкового контролю.

Наприклад, у Податковому кодексі Республіки Молдова питанням застосування непрямих методів контролю присвячено положення окремої Глави 11 і торкаються лише платників-податків – фізичних осіб. Глава 11 була введена в 13.01.2012 року. Власне, у 2012 році у Республіки Молдова було запущено програму податкової амністії.

Податковий орган Республіки Молдова має право використовувати такі непрямі методи оцінки оподатковуваного доходу: a) метод витрат; b) метод грошового потоку; c) метод власності; d) інші використовувані в міжнародній практиці методи. Одразу наголосимо, що остання відсилочна норма відкриває широкі можливості до здійснення заходів податкового контролю, і водночас сферою ймовірних предметів судового оскарження [38].

Непрямі методи використовуються окремо або в сукупності в залежності від складності, труднощі (конкретної ситуації), джерел інформації, що перевіряється. При визначенні оціненого оподатковуваного доходу враховуються кошти, задекларовані платником податку відповідно до податкового законодавства,

З метою визначення оціненого оподатковуваного доходу можуть використовуватися такі непрямі джерела:

інформація від фінансових установ (їх відділень або філій), осіб, які здійснюють нотаріальну діяльність, митних органів, правоохоронних органів, фондових бірж та / або інших публічних органів про здійснені фізичною особою угодах і операціях і даних по ним, а також про аналогічні угоди і операціях, здійснених іншими фізичними особами в аналогічних умовах;

наявна у фізичних і юридичних осіб інформація про продані та / або безоплатно передані майно, роботи, послуги та грошових коштах, про кошти або матеріальні цінності, придбані та / або отриманих фізичною особою щодо якої здійснюється перевірка;

інформація, наявна в інформаційній системі Державної податкової служби;

інформація або інші докази, отримані податковим органом шляхом використання спеціальних засобів, проведення аналізів, вимірювань, зіставлень, досліджень;

інші документи, інформації, пояснення і / або інші докази, отримані як від третіх осіб, так і від перевіряється фізичної особи [38].

На виконання положень Податкового кодексу Республіки Молдова фізичні та / або юридичні особи подають Головної державної податкової інспекції наступну інформацію:

1) Центр державних інформаційних ресурсів «Registru»:

інформацію про персональні дані;

інформацію про документування транспортних засобів, в тому числі переданих власниками в користування за плату або безоплатно;

2) фінансові установи - інформацію про всі види рахунків, активних протягом податкового року, в тому числі оборот (рух) за цими рахунками;

3) Прикордонна поліція - інформацію про перетин державного кордону Республіки Молдова;

4) туристичні компанії - інформацію про надані туристичні послуги;

5) страхові компанії - інформацію за договорами страхування;

6) власники регістрів власників цінних паперів - інформацію про операції з цінними паперами, скоєних в період податкового року;

7) Національний банк Молдови - інформацію про осіб, які згідно з валютним законодавством отримали дозвіл на відкриття рахунків за кордоном, а також звіти за відкритими за кордоном рахунках, подані відповідно до законодавства їх власниками;

8) нотаріуси та інші особи, які здійснюють нотаріальну діяльність:

інформацію про договори купівлі-продажу, міни, оренди нерухомості та цінних паперів;

інформацію про договори позики та дарування;

інформацію про інші договори по капітальних активів;

9) судові виконавці - інформацію про реалізацію прав кредиторів, визнаних виконавчим документом, представленим для виконання [38].

Така інформація надається безкоштовно в порядку та строки, встановлені Головною державною податковою інспекцією.

Порядок подання та структура інформації визначаються Головною державною податковою інспекцією.

Інформація повинна містити відомості:

про зарахування і / або списання протягом одного податкового року коштів на кожен банківський рахунок / с кожного банківського рахунку та / або на банківські рахунки / с банківських рахунків фізичної особи якщо сукупний дебетовий або кредитовий оборот відповідних рахунків за податковий рік перевищує 300 тисяч леїв;

про туристичні послуги, придбаних фізичною особою протягом одного податкового року, сукупний обсяг яких перевищує суму в 100 тисяч леїв;

про страхові внески, внесених фізичною особою протягом одного податкового року, сукупна величина яких перевищує суму в 100 тисяч леїв;

про операції з цінними паперами, що мали місце протягом одного податкового року, сукупний обсяг яких перевищує суму в 100 тисяч леїв на одну фізичну особу

про нотаріально завірених протягом одного податкового року договорах сукупний обсяг яких перевищує суму в 300 тисяч леїв на ім'я однієї фізичної особи

про реалізацію прав кредиторів, здійснених протягом одного податкового року, сукупний обсяг яких перевищує суму в 300 тисяч леїв на одну фізичну особу

Етапи застосування непрямих методів оцінки також визначені у Податкового кодексу Республіки Молдова. Процедура перевірки фізичної особи із застосуванням непрямих методів оцінки складається з наступних етапів:

аналіз і відбір фізичних осіб, які підлягають перевірці;

попередня податкова перевірка фізичних осіб;

податковий контроль [38].

Разом з широким запровадженням зазначених методів податкових перевірок виникли певні ускладнення практика вирішення яких судовими органами у частині забезпечення прав суб’єктів персональних даних привертає нашу увагу. Яскравим прикладом цього є Постанова Конституційного Суду Республіки Молдова від 6 серпня 2020 року №22 «Про винятковий випадок неконституційності деяких положень статті 226-16 ч. (11) Податкового кодексу, ухваленого Законом №1163 від 24 квітня 1997 року (надання податкової інформації судовим інстанціям та органам кримінального переслідування як засобу доказування) (звернення №18g/20» [47].

В межах розгляду скарги у цій справі Конституційний Суд Республіки Молдова наголосив, що «на думку Парламенту, механізм декларування та забезпечення конфіденційності податкової інформації є частиною норм, що належать до регулювання процесу управління та легалізації капіталу. В той саме час відповідно до бюджетно-податкової політики було вирішено надати суб'єктам оподаткування можливість добровільно задекларувати доходи та майно, які підпадають під положення глави 11 Податкового кодексу [Непрямі методи оцінки оподатковуваного доходу фізичних осіб].

Глава 11 Податкового кодексу визначає, що застосування непрямих методів оцінки оподатковуваного доходу фізичних осіб відбувається із дотриманням гарантій конфіденційності, передбаченої статтею 226-16 Податкового кодексу республіки Молдова. Відповідно аби забезпечити зазначеним у статті 226-3 Податкового кодексу суб'єктам захисту інформації, законодавець передбачив, що будь-яка інформація, отримана Державною податковою службою, що розглядається як податкова таємниця та надається органам кримінального переслідування та судовим інстанціям лише з метою розгляду справ про ухилення від сплати податків. Таким чином, Конституційний Суд зазначає, що інформація про доходи та майно платників податків, одержана податковими органами, розглядається як податкова таємниця та може містити персональні дані цих осіб. Конституційний суд зазначає, що обмеження права

доступу до певної категорії інформації застосовується для захисту іншого основного права - права на приватне життя, передбаченого статтею 28 Конституції. Отже, це обмеження переслідує як мінімум одну законну мету (захист прав, свобод та гідності інших осіб), на яку посилається частина друга Статті 54 Конституції Республіки Молдова [47].

Тобто зазначена Постанова Конституційного Суду Республіки Молдова прямо відповідає встановленим у європейських нормативних актах принципах легітимної мети обробки персональних даних.

Підсумовуючи наголосимо, що непрямі методи визначення доходу податкові органи застосовують тоді, коли реальний дохід не можна визначити через відсутність інформації (втрачені або не надаються відповідні документи від декларанта безпосередньо) або якщо інформація явно необ'єктивна.

Непрямі методи податкового контролю це такий спосіб визначення податкового зобов’язання при якому використовуються дані відмінні від інформації з офіційної звітності платника податків. При цьому коло таких даних не є чітко визначеним, і сюди може входити інформація як з відкритих джерел так із офіційних ресурсів що дозволяє реконструювати реальну картину доходів та витрат платника податків.

Відповідно, запроваджуючи в Україні інструментарій непрямих методів контролю доходів платників податків необхідно одночасно гарантувати забезпечення захисту прав суб’єктів прав персональних даних, які виступають відповідними платниками податків (декларантами). Хоча податкове законодавство містить окремі норми щодо забезпечення обмеженого доступу до інформації отриманої податковими органами в процесі декларування та використання методів податкового контролю, зазначені норми не є достатніми у контексті їх співвідношення з практикою розповсюдженою в ЄС.

Це дозволяє запропонувати ведення у податкове законодавство положень, які б визначали поняття «*податкова таємниця*», що комплексно включало б відомості вся сукупність яких відповідала б вимогам щодо поводження з

персональними даними на основі принципів напрацьованих у директивних актах ЄС.

Удосконалюючи податкове законодавство України у частині використання досвіду Республіки Молдови необхідно акцентувати увагу на можливості запозичення, як нормативного регулювання самої методології здійснення перевірок так і щодо гарантування захисту прав суб'єктів персональних даних в процесі здійснення такого контролю.

ВИСНОВКИ

У магістерському дослідженні розглянуто теоретичні та практичні аспекти формування та реалізації державної політики у сфері забезпечення захисту персональних даних. За результатами дослідження зроблено такі висновки:

1. Поняття персональних даних пропонуємо визначати, як відомості або сукупність відомостей, що торкаються інформації щодо громадянина, яка є їх власником, та дозволяють здійснити її ідентифікацію.

2. Перелік ознак персональних даних 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..

3. Аналіз європейських стандартів охорони персональних даних дозволив ствекрджувати, що найбільш повно вони відображені в Загальному регламенті про захист даних. Практика ЄСПЛ виробила критерії правомірного обмеження прав на персональні дані, що відповідають загальним принципам правомірного втручання в приватне життя: втручання відповідає закону; втручання здійснюється із легітимною метою; втручання є необхідним у демократичному суспільстві.

4. Поняття «суб’єкт персональних даних» є загальним, визначаємо суб’єкта персональних даних як особу (без уточнення фізична чи юридична) і не виключає застосовування в окремому порядку її положень «до інформації, яка стосується груп осіб, асоціацій, фондів, компаній, корпорацій та будь-яких інших організацій, що безпосередньо чи опосередковано складаються з окремих осіб, незалежно від того, мають чи не мають такі установи статус юридичної особи…». Таким чином, припускається можливість поширення правового регулювання захисту персональних даних деякою мірою і на організації, зокрема юридичних осіб, якщо це передбачатиме національне законодавство.

5. Важливим елементом входження України у європейський простір захисту персональних даних є отримання статусу спостерігача при Європейській раді щодо захисту персональних даних. Серед наших держав-сусідів такий статус з 2018 року має Республіка Молдова

Враховуючи прогалини правового регулювання Інтернету, вони мають бути усунені у новому інформаційному законодавстві. Поряд із законом, що регулює державну політику в Мережі, слід ухвалити рамковий закон про Інтернет. У ньому, як вважає автор, необхідно: відпрацювати понятійний апарат із залученням відповідних експертів у галузі технічних знань для вироблення чітких законодавчих понять; закріпити найважливіші принципи «мережевих відносин»; відобразити специфіку суб'єктного складу мережевих відносин; встановити правила інформаційного обміну у мережі Інтернет; сформулювати відповідальність учасників мережевих відносин за порушення закріплених норм, а також передбачити способи доведення та особливості розгляду «мережевих суперечок»; встановити межі відповідальності кожного учасника мережевих відносин.

Необхідно запропонувати ведення у податкове законодавство положень, які б визначали поняття «податкова таємниця», що комплексно включало б відомості вся сукупність яких відповідала б вимогам щодо поводження з персональними даними на основі принципів напрацьованих у директивних актах ЄС.

6. Право на захист персональних даних має всі необхідні ознаки, які притаманні підгалузі права, а саме: предметна єдність регульованих правом на захист персональних даних суспільних відносин та їх суттєва суспільна значимість; використання комплексу самостійних способів та прийомів правового регулювання захисту персональних даних; наявність власних джерел правового регулювання; наявність спеціальних принципів захисту персональних даних, що діють у системі, забезпечуючи цілеспрямоване регулювання суспільних відносин, що утворюють його предмет; власна системна організація, яка відображена в нормах щодо захисту персональних даних.

Таким чином, перші норми щодо захисту персональних даних розглядалися у контексті права на недоторканість особистого життя. Однак, на тлі переходу до інформаційного суспільства, для котрого характерне широке використання інформаційних технологій, активний збір та обробка інформації, включно із персональною інформацією, виникла потреба у правовому регулюванні обробки персональних даних. Поширення «доби Інтернету» лише прискорює потребу нормативно-правового регулювання захисту персональних даних.

Передовими країнами у цьому сенсі стали країни Західної Європи, у котрих були прийняті спеціальні закони про захист персональних даних. Однак, законодавство щодо персональних даних в європейських країнах продовжує розвиватися. У практиці європейських держав сьогодні також виникають нові проблеми, що потребують правового регулювання (наприклад, транскордонна передача персональних даних, використання біометричних персональних даних, даних медико-генетичного характеру, тощо).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Агарков М. М. Предмет и система советского гражданского права. *Избранные труды. Т. П. М*, 2002. С. 269-317.
2. Аномалії в цивільному праві України : навч.-практ. посіб. / відп. ред. Р. А. Майданик. Київ : Юстініан, 2007. 912 с.
3. Балашкина И.В. Особенности конституционного регулирования права на неприкосновенность частной жизни в Российской Федерации. *Право и политика*. 2007. №7. С. 92–105.
4. Бєлова Ю.Д. Стандарти захисту права на персональні дані відповідно до Директиви 95/46/ЕС. *Часопис «Університетські наукові записки» Хмельницького університету управління та права*. 2017. № 3 (63). С. 130-139.
5. Брижко В. М. Захист персональних даних: реалії та практика сучасності. *Інформація і право*. 2013. № 3. С. 31-48.
6. Булеца С. Б. Персональні дані пацієнта. *Науковий вісник Ужгородського національного університету*: Серія ПРАВО. Випуск 22. Частина 2. Том 1, 2014. С. 186-191.
7. Великий тлумачний словник сучасної української мови (з дод. і допов.) / Уклад, і голов, ред. В. Т. Бусел. Київ; Ірпінь: ВТФ «Перун», 2005. 1728 с.
8. Власко С. Захист персональних даних: чий досвід може стати в нагоді Україні. URL:https://www.eurointegration.com.ua/experts/2018/01/16/7076152/
9. Волкова Н. В. Засоби індивідуалізації фізичних осіб (окремі аспекти). *Актуальні питання держави і права*. 2008. № 39.С. 238-243.
10. Гега П.Т. Основи податкового права : навчальний посібник. Київ : Т-во «Знання», КОО. 2003. 318 с.
11. Гражданское право: актуальные проблемы теории и практики /Под общ. ред. В.А. Белова. М.: Юрайт-Издат, 2007. 993 с.

12. Дмитренко О. А. Право фізичної особина власні персональні дані в цивільному праві. України : автореф. дис. ... канд. юрид. наук :12.00.03. Київ, 2010. 19 с.

13. Долінська А.М. Право на свободу інтернет-користувачів, як фізичних осіб. *Visegrad journal on Human rights*. 2020. № 4. С. 30-35. URL: http://vjhr-journal.sk/wp-content/uploads/2020/12/VJHR_4_2020.pdf;

14. Драгомановський збірник. „Вільна Спілка" та сучасний український конституціоналізм / За редакцією Т.Г.Андрусяка. Львів: Світ, 1996. – С.9-10 (256 с.)

15. Еннан Р. Є. IT право: проблеми і перспективи розвитку в Україні URL: http://aphd.ua/publication-173/.Інтернет-відносин.

16. Європейської конвенції про захист прав людини і основних свобод від 04.11.1950. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

17. Жилінкова І.В. Правове регулювання відносин у мережі Інтернет. *Право України*. 2003. №5. С. 124-127.

18. Загальна декларація прав людини: від 10.12.1948 URL: https://zakon.rada.gov.ua/laws/show/995_015#Text

19. 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. 219 с.

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

21. Кардаш А. В. Інформація про особу та персональні дані: окремі аспекти співвідношення. *Форум права*. 2017. № 4. С. 87-92.

22. Каретник О. С. До питання про правову природу персональних даних фізичної особи : цивілістичні аспекти. *Право України: Юридичний журнал*. 2014. № 9. С. 192-200.

23. Кирилюк О. Становление универсального международно-правового регулирования в сфере защиты персональных данных. *Legea si Viata*. 2015. № 11. С. 75-86

24. Кодекс законів про працю України: Закон України від 10.12.1971 № 322-VIII. URL : https://zakon.rada.gov.ua/laws/show/322-08#Text

25. Кодекс України про адміністративні правопорушення: Закон України від 07.12.1984 р. № 8073-X. Дата оновлення: 24.11.2021 р. URL: https://zakon.rada.gov.ua/laws/show/80731-10

26. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року. *Офіційний вісник України*. 2011. № 1. Ст. 85.

27. Конвенція про захист прав людини і основоположних свобод від 04.11.1950. База даних «Законодавство України» / ВР України. URL: http://zakon3.rada.gov.ua/ laws/show/995_004

28. Конституція України : Закон України від 28 червня 1996 р. № 254к/96-ВР / *Верховна Рада України*. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141. URL: http:// zakon5.rada.gov.ua/laws/show/254%D0%B (дата звернення: 15.01.2021).

29. Конституція Української Радянської Соціалістичної Республіки. Прийнята на позачерговій сьомій сесії Верховної Ради Української РСР дев'ятого скликання 20 квітня 1978 року. URL: http://static.rada.gov.ua/site/const/istoriya/1978.html

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

31. Кохановська О. В. Цивільно-правові проблеми інформаційних відносин в України : автореферат дис. ... д-ра юрид. наук : 12.00.03 Цивільне право, сімейне право, цивільний процес, міжнародне приватне право. Київ : Б. в., 2006. - 34 с.

32. Кравчук М. М. Конституційно-правові аспекти захисту персональних даних у мережі Інтернет. *Наукові записки Інституту законодавства Верховної Ради України.* 2013. №2. С. 40-45.

33. Красавчикова Л. О. Личная жизнь граждан под охраной закона. Москва : Юрид. лит., 1983. 160 с.

34. Кучерявенко М.П. Поняття складного інституту податкового права. *Вісник Академії правових наук України.*1998. № 4. С. 105-107.

35. Лушников А.М. Защита персональных данных работника: сравнительно-правовой комментарий. *Трудовое право*. 2009. № 9. С. 93–101.

36. Махов В.Н., Пешков М.А. Уголовный процесс США (досудебные стадии). М.: ЗАО Бизнес-школа «Интел-Синтез», 1998. 208 с.

37. Мельник К. С. Теоретико-правовий зміст терміна «персональні дані». *Інформація і право*. 2013. № 3. С. 49-57.

38. Налоговый кодекс Республики Молдова. URL: https://wipolex-res.wipo.int/edocs/lexdocs/laws/ru/md/md102ru.pdf

39. Народний Рух України. Документи і матеріали. К.: Софія, 1993.- С.9 (64)

40. Основи законодавства України про охорону здоров'я від 19 листопада 1992 року № 2801-XII. *Відомості Верховної Ради України*. 1993. № 4. Ст. 19.

41. Пазюк А. В. Міжнародно-правове регулювання інформаційної сфери (теоретичні і практичні аспекти) : дис. ... д-ра юрид. наук : 12.00.11.; Київ. нац. ун-т ім. Т. Шевченка. Київ, 2016. 567 с.

42. Пазюк А. В. Міжнародно-правове регулювання інформаційної сфери (теоретичні і практичні аспекти) : дис. ... д-ра юрид. наук : 12.00.11.; Київ. нац. ун-т ім. Т. Шевченка. Київ, 2016. 567 с.(с.55)

43. Податковий кодекс України : Закон України від 02.12.2010 р. з змінами та доповненнями від 20. 10. 2019 р., підстава № 129-IX. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2755-. (дата звернення: 15.01.2021).

44. Положення про Єдину державну електронну базу з питань освіти, в редакції постанови Кабінету Міністрів України від 12 липня 2017 р. № 550. База даних «Законодавство України» / ВР України. URL: http://zakon2.rada.gov.ua/laws/show/752-2011-%D0%BF

45. Посикалюк О. О. До питання про об'єкт особистих немайнових прав фізичних осіб. *Юридична Україна*. 2009. № 5. С. 65-71.

46. Посикалюк О. О. Особисті немайнові права фізичних осіб в романській, германській, англо-американській системах приватного права. Київ: Науково-дослідний інститут приватного права і підприємництва НАПрН України. 2011. 205 с.

47. Постанова Конституційного Суду Республіки Молдова від 6 серпня 2020 року №22 «Про винятковий випадок неконституційності деяких положень статті 226-16 ч. (11) Податкового кодексу, ухваленого Законом №1163 від 24 квітня 1997 року (надання податкової інформації судовим інстанціям та органам кримінального переслідування як засобу доказування) (звернення №18g/20». URL: http://base.spinform.ru/show_doc.fwx?rgn=127177

48. Про авторське право і суміжні права: Закон України В редакції Закону № 2627-III від 11.07.2001. *Відомості Верховної Ради України*. 2001. № 43. Ст. 214.

49. Про державні фінансові гарантії медичного обслуговування населення: Закон України від 19 жовтня 2017 року № 2168-VIII. *Офіційний вісник України.* 2018. № 4.

50. Про державну реєстрацію актів цивільного стану: Закон України від 1 липня 2010 року № 2398-VI. *Відомості Верховної Ради України*. 2010. № 38. Ст. 509.

51. Про доступ до публічної інформації: Закон України від 13 січня 2011 року № 2939-VI. *Офіційний вісник України*. 2011. № 10. Ст. 446.

52. Про доступ до судових рішень: Закон України від 22 грудня 2005 року № 3262-IV. *Відомості Верховної Ради України*. 2006. № 15. Ст. 128.

53. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297–VI. *Офіційний вісник України*. 2010. № 49. Ст. 1604.

54. Про захист персональних даних : проект Закону України від 25.03.2008, № 2273. База даних «Законодавство України» / ВР України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=32124

55. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних: Директива 95/46/ЄС Європейського Парламенту і Ради від 24 жовтня 1995 року. База даних «Законодавство України» / ВР України. URL: http://zakon5.rada.gov.ua/laws/show/994_242.

56. Про звернення громадян: Закон України від 2 жовтня 1996 року № 393/96-ВР. *Відомості Верховної Ради України*. 1996. № 47. Ст. 256.

57. Про інформацію : Закон України в редакції Закону № 2938-VI від 13.01.2011. *Відомості Верховної Ради України*. 2011. № 32. Ст. 313.

58. Про організацію формування та обігу кредитних історій: Закон України від 23 червня 2005 року № 2704-IV. *Відомості Верховної Ради України*. 2005. № 32. Ст. 421.

59. Про правовий захист баз даних: Директива 96/9/ЄС Європейського Парламенту та Ради від 11 березня 1996 року. База даних «Законодавство України» / ВР України. URL: http://zakon3.rada.gov.ua/laws/show/994_241.

60. Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних : Закон України від 06.07.2010 р. № 2438–VI. *Офіційний вісник України*. 2010. № 58. Ст. 1994.

61. Про телебачення і радіомовлення: Закон України в редакції Закону № 3317-IV від 12.01.2006. *Відомості Верховної Ради України*. 2006. № 18. Ст. 155.

62. Різак М. В. Класифікація персональних даних як необхідний елемент введення ефективної комунікації в суспільстві. *Науковий вісник Міжнародного гуманітарного університету*. 2013. Вип. 6-3(1). С. 90-94.

63. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20 січня 2012 року № 2-рп/2012 . *Офіційний вісник України*. 2012. № 9. Ст. 332.

64. Романюк І. І. До поняття суб'єктивного права на власні персональні дані, його ознак і місця в системі особистих немайнових прав в Україні. *Науковий вісник Ужгородського національного університету : Серія: Право*. 2012. Вип. 20. Ч. 2. Т. 1. С. 233–237.

65. Романюк І. І. Законодавчі та теоретичні підходи до визначення поняття персональних даних та відмежування його від суміжних понять. *Актуальні питання публічного та приватного права*. 2014. № 1. С. 82-90.

66. Сенюта І. Я. Захист персональних даних у сфері охорони здоров'я: алгоритм змін. *Науковий вісник Херсонського державного університету. Серія «Юридичні науки»*. Випуск 6-1/2014. 2014. С. 216–221.

67. Серебряник О. О. Інформація про особу як об'єкт цивільних прав : автореф. дис. ... канд. юрид. наук : 12.00.03; Івано-Франків. ун-т права ім. короля Данила Галицького. Івано-Франківськ, 2016. 20 с.

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

69. Сліпченко С. О. Місце об'єктів особистих немайнових правовідносин у системі об'єктів цивільного права. *Право і суспільство*. 2013. № 6.2. С. 92-97.

70. Сопілко І. М. Механізм захисту персональних даних: проблеми та перспективи. *Юридичний вісник. Повітряне і космічне право*. 2013. № 2. С. 66-70.

71. Стефанчук М. О. Цивільно-правові наслідки зміни соціально-індивідуалізуючих ознак фізичної особи. *Jurnalul juridicnaţional: teorie şipractică.* 2015. № 6. С. 153-156.

72. Теремецький В. І. Суб'єкти відносин, пов'язаних з персональними даними. *Право і Безпека*. 2015. № 2. С. 171-176.

73. Хартія Основних прав Європейського Союзу від 7 грудня 2000 року. URL: https://zakon.rada.gov.ua/laws/show/994_524#Text

74. Цивільний кодекс України : Закон України від 16 січня 2003 року № 435-IV. База даних «Законодавство України» / ВР України. URL: http://zakon5.rada.gov.ua/laws/show/435-15.

75. Чанишев Р. І. Міжнародні стандарти захисту персональних даних працівника і законодавство України. *Актуальні проблеми держави і права*. 2011. Вип. 57. С. 275-281.

76. Шатська У. Право на приватне життя: історія, розвиток, українські реалії. URL: https://zmina.info/columns/pravo-na-pryvatne-zhyttya-istoriya-rozvytok-ukrayinski-realiyi/

77. Шишка Р. Б. До проблеми індивідуалізації фізичної особи. *Еволюція цивільного законодавства: проблеми теорії і практики. Матеріали міжнародної науково-практичної конференції*. 29-30квітня 2004 р., м. Харків. Київ : Академія правових наук України, НДІ приватного права і підприємництва, НДІ інтелектуальної власності, Національна юридична академія ім. Я. Мудрого, 2004. С.153-162.

78. 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.): URL: http://eur-lex.europa.eu/eli/dec/2000/520/oj

79. Case of Amann v. Switzerland, App. No.27798/95 URL: http://hudoc.echr.coe.int/eng?i=001-58497

80. Case of Rotaru v. Romania, App. No.28341/95 URL: http://hudoc.echr.coe.int/eng?i=001-58586

81. Human rights and modern scientific and technological developments. Recommendation 509 (1968). URL: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=14546&lang=en

82. Information privacy law: Textbook / D. J. Solove, M. Rotenberg. N. Y., 2003. 795 p.

83. Judith DeCew Privacy. *Stanford Encyclopedia of Philosophy*. URL: https://plato.stanford.edu/entries/privacy/

84. Kanstantsin Dzehtsiarou. European Consensus and the Legitimacy of the European Court of Human Rights. Cambridge University Press. 2015. 230 p.

85. Malte Kröger: *Datenschutz und Prüfungsrecht Was das Nowak-Urteil für das Prüfungswesen bedeutet*. In: *Junge Wissenschaft im Öffentlichen Recht*. URL: *https://www.juwiss.de/8-2018/*

86. Proposal for a Regulation on Privacy and Electronic Communications. URL:https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-privacy-and-electronic-communications

87. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: http://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=ENм

88. Richard A. Posner. The Right of Privac. *Georgia Law Review*. 1978. Vol. 12. № 3. P. 393-422.

89. Safe Harbor Privacy Principles, issued by the U.S. Department of commerce on July 21, 2000. URL: https://rm.coe.int/16806af271.

Виконав: студент магістратури спеціальності 281 Публічне управління та адміністрування заочної форми навчання		Фіярська С. І.
«____» грудня 2021 р.	Підпис	Ініціали, прізвище
Науковий керівник кандидат наук з державного управління, доцент, доцент кафедри публічного управління та адміністрування		М.О. Маланчій
«____» грудня 2021 р.	Підпис	Ініціали, прізвище
Робота допущена до захисту: Завідувач кафедри публічного управління та адміністрування, доктор наук з держ. управління, доцент		Е.В. Щепанський
«____» грудня 2021 р.	Підпис	Ініціали, прізвище