ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА
ІМЕНІ ЛЕОНІДА ЮЗЬКОВА

ФАКУЛЬТЕТ ПУБЛІЧНОГО УПРАВЛІННЯ

Кафедра публічного управління та адміністрування

МАГІСТЕРСЬКА РОБОТА

на здобуття освітнього рівня Магістр
на тему:

ПУБЛІЧНО-УПРАВЛІНСЬКІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Виконала: студентка магістратури
за спеціальністю 281 Публічне
управління та адміністрування
Назарова Катерина
Юріївна
(прізвище та ініціали)

Керівник: доктор наук з державного
управління, доцент,
доцент кафедри
публічного управління та
адміністрування
Маланчій Микола
Олександрович
(прізвище та ініціали)

Рецензент:
(прізвище та ініціали)

Хмельницький – 2023 рік

АНОТАЦІЯ

Назарова К. Ю. Публічно-управлінські механізми забезпечення захисту персональних даних. Кваліфікаційна наукова праця на правах рукопису. Магістерська робота на здобуття освітнього ступеня магістра за спеціальністю 281 Публічне управління та адміністрування. Хмельницький університет управління та права імені Леоніда Юзькова, Хмельницький, 2023. 72 с.

Публічно-управлінські механізми забезпечення захисту персональних даних в сучасному світі відіграють важливу роль у забезпеченні прозорості, конфіденційності та безпеки особистої інформації. Одним з ефективних механізмів є створення та вдосконалення законодавчої бази, що регулює обробку та захист персональних даних. Закони та нормативні акти визначають права та обов'язки суб'єктів обробки даних, встановлюють процедури та відповідальність за порушення законодавства. Далі, важливою складовою є створення та діяльність органів з контролю за дотриманням законодавства з питань захисту персональних даних. Ці органи відповідають за моніторинг та реагування на можливі порушення, проведення розслідувань та захист прав громадян у цій сфері. Важливою ініціативою є розробка та впровадження стандартів безпеки та конфіденційності, які регулюють обробку та зберігання персональних даних. Публічно-управлінські механізми також можуть включати проведення освітніх кампаній та тренінгів для громадян та організацій, щоб підвищити їхню свідомість щодо захисту персональних даних та правильного використання інформації. Важливою частиною публічно-управлінських механізмів є також співпраця з приватним сектором та міжнародними партнерами для розробки інноваційних рішень та обміну кращими практиками в сфері захисту персональних даних. Усі ці елементи разом створюють ефективний публічно-управлінський механізм, спрямований на забезпечення надійного та сучасного захисту персональних даних у цифрову епоху.

Ключові слова: війна, персональні дані, військовополонені, комбатанти, некомбатанти, реєстри.

THE SUMMARY

Nazarova K. Yu. Public management mechanisms for ensuring the protection of personal data. Master's degree work for obtaining an open master's degree in the specialty 281 Public management and administration. – Khmelnytskyi Leonid Yuzkov University of Management and Law, Khmelnytskyi, 2023. 72 p.

Public management mechanisms for personal data protection in today's world play an important role in ensuring transparency, confidentiality and security of personal information. These mechanisms are a key element of legal and organizational arrangements aimed at protecting the individual privacy of citizens. One of the effective mechanisms is the creation and improvement of the legal framework regulating the processing and protection of personal data. Laws and regulations determine the rights and obligations of data processing subjects, establish procedures and liability for violations of legislation. Next, an important component is the creation and operation of bodies for monitoring compliance with legislation on personal data protection. These bodies are responsible for monitoring and responding to possible violations, conducting investigations and protecting the rights of citizens in this area.Another important initiative is the development and implementation of security and privacy standards that regulate the processing and storage of personal data. This may include recommendations for encryption, tamper protection, and other technical aspects of information security. Public management mechanisms may also include conducting educational campaigns and trainings for citizens and organizations to raise their awareness of personal data protection and the correct use of information. An important part of public management mechanisms is also cooperation with the private sector and international partners to develop innovative solutions and exchange best practices in the field of personal data protection. All these elements together create an effective public management mechanism aimed at ensuring reliable and modern protection of personal data in the digital age.

Keywords: war, personal data, prisoners of war, combatants, non-combatants, registers.

ЗМІСТ

Зміст

ВСТУП

Актуальність теми. Актуальність цієї теми пов'язана із сучасним етапом всебічного впровадження інформатизації у процеси публічного управління через створення обширних баз даних та розширеного доступу органів влади до особистої інформації. Будівництво демократичної соціально-правової держави, де головною цінністю є людина, її гідність і честь, а також забезпечення недоторканності та безпеки, взаємно пов'язані з необхідністю покращення захисту персональних даних. Наукові відкриття в галузі генної інженерії та застосування комп'ютерної психотехнології, а також транскордонні інформаційні мережі посилюють проблеми щодо правового захисту приватного життя.

З одного боку, в умовах сучасного розвитку цивілізації та всезагального впровадження інформаційно-телекомунікаційних технологій зростає доступ людей до інформації, що об'єктивно сприяє реалізації прав людини на свободу інформації. Автоматизовані бази даних, щодо можливостей зберігання та зручного доступу до неї, значно перевершують ручні архіви (дискові накопичувачі комп'ютерів можуть утримувати обсяги інформації, еквівалентні великим університетським бібліотекам). Комп'ютер дозволяє ефективно поєднувати неосяжні обсяги інформації. Процедури зіставлення даних з різних файлів (наприклад, процедури типу data matching) на комп'ютері дозволяють створювати "біографічні портрети" осіб за допомогою інформації, зібраної з різних баз даних.

З іншого боку, можливість фізичних осіб та колективних утворень отримати доступ до баз персональних даних збільшує ризик порушення сфери приватного життя та недоторканності особистого права. Інформаційно-телекомунікаційні технології (ІТТ) розширили правові виклики, пов'язані з дилемою "розкриття інформації чи захист приватного життя". Таким чином, виникає термінова задача створення ефективного механізму правового захисту приватного життя на національному та міжнародному рівні, зокрема під час транскордонної передачі даних. У розвинених демократичних країнах, здебільшого починаючи з другої половини XX століття, правовий захист сфери

приватного життя у зв'язку із застосуванням інформаційних технологій став одним із пріоритетів у галузі захисту прав людини. Цій темі приділяється велика увага в теоретичних дослідженнях. У національних системах правового захисту приватного життя (які тепер є широко поширеними) розроблено спеціальні засоби правового регулювання для автоматизованої обробки персональних даних. У період розвитку комп'ютерів автоматизована обробка персональних даних стала основним джерелом загроз для сфери приватного життя. Створення глобального інформаційного простору, що розпочалося на базі глобальних комп'ютерно-телекомунікаційних мереж, поставило перед собою важливе завдання розробки єдиної національної та міжнародної правової системи для обробки, використання та передачі персональних даних. Відсутність врахування досвіду ретельного дослідження міжнародних стандартів захисту персональних даних, основних принципів їхнього забезпечення, вивчення особливостей національних регулятивних підходів окремих держав з розвиненим законодавством та довгостроковим досвідом у галузі захисту прав і свобод людини, включаючи право на захист персональних даних, ускладнює розуміння сучасних проблем національного правового регулювання в управлінських відносинах.

У світі, насиченому інформаційними технологіями, особисті дані осіб стали важливою соціальною цінністю та об'єктом єдиного правового регулювання. У рівні правової політики та юридичної доктрини виявляються загальні підходи для більшості країн світу до ставлення до персональних даних.

Інститут персональних даних представляє собою складну структуру, яка охоплює елементи, що відносяться до галузей конституційного, цивільного та адміністративного права. Протягом останнього десятиліття питання забезпечення захисту особистих даних громадян від дій органів публічної влади стали дуже актуальними, викликаючи жваві обговорення як на науково-теоретичному, так і на професійному рівнях.

У той самий час, російська збройна агресія особливо загострила питання про захист основних прав та свобод громадян, зокрема права на життя. В умовах широкомасштабної військової агресії особливу увагу варто приділити питанню

захисту персональних даних військовослужбовців, до яких несанкціонований доступ агресора може становити загрозу їхньому життю.

Стан розробки у вітчизняній та зарубіжній науці. Дослідження особливостей правовідносин, пов'язаних із захистом прав персональних даних громадян від суб'єктів публічної адміністрації, в науковій літературі сьогодні розглядаються обмежено. Ряд вчених, таких як Р.В. Ігонін, Р.А. Калюжний, А.В. Кучеренко, С.Й. Литвин, А.В. Пазюк, В.П. Радкевич, К.М. Рудий, В.О. Серьогін, І.М. Солілко, В.І. Теремецький, А.М. Чвалюк, О.О. Шарибурина, М.Я. Швець, досліджували сутність персональних даних та окремі аспекти їх адміністративно-правового захисту.

На жаль, відсутність наукових публікацій про особливості відносин, що стосуються забезпечення захисту персональних даних громадян від суб'єктів публічної адміністрації, є видимою. Щодо правового захисту персональних даних, Ю.Д. Бєлова, В.М. Брижко, А.М. Новицький, А.В. Пазюк, І.Я. Сенюта, О.М. Селезньова досліджували різні аспекти цього питання.

Важливо відзначити, що більшість сучасних досліджень акцентує увагу на аспектах приватного права, коли йдеться про захист прав персональних даних громадян. Однак, практично всі ці дослідження в основному фокусуються на цивільному праві.

Незважаючи на це, необхідно визнати, що аналіз захисту персональних даних громадян під час воєнного стану вимагає комплексного підходу. З урахуванням поточної геополітичної ситуації та загроз військових конфліктів це питання стає дуже актуальним і потребує ретельного та всебічного наукового вивчення. Зазначається значний дефіцит досліджень, які охоплюють юридичні, етичні та соціокультурні аспекти захисту персональних даних в умовах воєнного стану, що підкреслює важливість подальшого розвитку цього наукового напряму.

Метою даного дослідження є глибокий теоретичний аналіз проблем, пов'язаних із забезпеченням захисту персональних даних громадян органами публічної влади під час війни, а також виявлення шляхів їх вирішення. Для досягнення цієї мети ставляться наступні *завдання*:

- визначення поняття «персональні дані громадян» та розгляд їх захисту.

- аналіз особливостей правового режиму обігу персональних даних у системі публічного управління.

- вивчення нормативно-правових засад використання державних інструментів для захисту персональних даних громадян.

- визначення суб'єктів державного управління, які відповідають за захист персональних даних.

- аналіз аспектів захисту персональних даних громадян у контексті державного управління.

- визначення шляхів вдосконалення організаційно-управлінських засад державного управління у сфері захисту персональних даних громадян під час війни.

Об'єктом дослідження є суспільні відносини, що виникають при застосуванні публічних інструментів захисту персональних даних громадян.

Предметом дослідження є теоретико-методичні та практичні аспекти застосування цих інструментів.

Методологічна основа дослідження. Дослідження ґрунтувалося на застосуванні різних методів, як загальнонаукових, так і спеціальних. До загальнонаукових методів належать формально-логічний, аналітичний, історичний, системно-логічний та порівняльно-правовий. Поняття персональних даних було визначено за допомогою формально-логічного та історичного підходів. Аналіз сучасного законодавства щодо особливостей державного управління у сфері захисту персональних даних здійснювався за допомогою аналітичного методу, який використовувався під час розробки пропозицій щодо вдосконалення правової бази для реєстраційних відносин. Системно-логічний метод застосовувався для виявлення ознак механізму державного управління у сфері захисту персональних даних громадян в умовах війни. Використання системного підходу сприяло формулюванню пропозицій з удосконалення організації механізму державного управління у цьому контексті.

Інформаційну основу дослідження створили вітчизняні законодавчі акти, що регулюють дану сферу, а також правові документи іноземних країн, які

містять відомості про особливості механізму державного управління у сфері захисту особистих даних громадян під час воєнних конфліктів. До аналізу були включені наукові публікації, які стосуються вивченої проблематики.

Практичне значення отриманих результатів. Отримані результати та рекомендації, щодо організації механізму державного управління у сфері захисту персональних даних, можуть бути застосовані для удосконалення законодавства, зокрема, при розробці нової редакції Закону України про захист персональних даних.

Структура та обсяг роботи обумовлені метою та завданнями проведеного дослідження. Робота включає в себе вступ, три розділи, шість підрозділів, висновки та список використаних джерел (загалом 89 джерел). Загальний обсяг дослідження становить 72 сторінки.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ГРОМАДЯН У ДІЯЛЬНОСТІ ОРГАНІВ ПУБЛІЧНОЇ ВЛАДИ

1.1 Визначення поняття «персональні дані громадян» та особливості їх публічно-управлінського захисту

Сучасний етап розвитку цивілізації характеризується широкомасштабним впровадженням засобів інформатизації у процеси державного управління, зокрема шляхом створення масивних баз даних та розширеного доступу органів влади до особистої інформації громадян. У той же час, будівництво демократичної соціально-правової держави, де вищою цінністю є людина, її гідність та честь, а також забезпечення безпеки й недоторканності, тісно пов'язані з необхідністю покращення захисту основних прав людини та громадянина. З розвитком інформаційних технологій та створенням баз даних з'явилася нова загроза для цих прав - можливість легкого копіювання та об'єднання особистих даних. Протягом останнього десятиліття багато картотек і баз даних, які раніше були в паперовій формі, перетворилися на електронні. З різних причин ці дані стали доступними третім особам і стали об'єктом купівлі-продажу. Ця обставина призводить до неконтрольованого використання цієї інформації. Тим часом сам факт продажу баз даних або поширення інформації, яка міститься в них, створює підвищену суспільну небезпеку, оскільки конфіденційні дані можуть бути використані на шкоду конкретній особі (суб'єкту персональних даних).

Для захисту конституційних прав громадян від будь-яких порушень необхідно встановлення строгого правового регулювання обігу баз даних, які містять особисті дані. Це включає в себе встановлення юридичної відповідальності для операторів цих баз у випадку порушень правил щодо збирання, зберігання та використання особистих даних. Такий підхід сприятиме забезпеченню ефективного юридичного захисту інтересів окремих громадян і

суспільства в цілому. Ці та інші обставини актуалізують цю тему та підкреслюють необхідність розробки відповідних теоретико-правових засад. З'явлення категорії персональних даних в інформаційному праві та загальному праві тісно пов'язане з концепцією захисту приватного життя, яке, у зростаючому інформаційному суспільстві, стає все більше піддається різноманітним загрозам. Бажання забезпечити належний рівень захисту особистості від інформаційних загроз викликало ідею регулювання обігу інформації про особу - персональних даних, виокремлюючи їх як особливий вид інформації, що вимагає особливого захисту.

Персональні дані – це інформація, що стосується конкретної фізичної особи (суб'єкта персональних даних), або дані, які можуть бути визначені відносно неї, прямо чи опосередковано. Така інформація включає прізвище, ім'я, по батькові, рік, місяць, дата та місце народження, адресу, сімейний, соціальний, майновий стан, освіту, професію, доходи та інші відомості, які зазвичай представлені у формалізованій формі, що дозволяє їх обробку в інформаційних системах, переважно автоматизованими засобами, повністю або частково. Для відрізнення персональних даних від іншої інформації використовується як основний критерій наявність взаємозв'язку між суб'єктом та змістом відповідної інформації про нього. Цей зв'язок може бути очевидним, коли ідентифікуюча інформація прямо вказує на суб'єкта даних, або він може бути потенційно визначений. Як додатковий ознаку персональних даних слід враховувати їх формалізований характер, тобто набір відомостей та їх зв'язок з інформаційною системою, який обумовлений цілями та завданнями обробки в цій системі.

Аналіз міжнародної практики та досвіду окремих країн у сфері правового захисту персональних даних підтверджує наявність сталої тенденції до універсалізації в цьому напрямі. Ці стандарти виступають важливим правовим орієнтиром для розвитку законодавства, яке визначає правові механізми захисту персональних даних та його правозастосовної практики. У сучасних умовах створилися передумови для виділення самостійного нормативного комплексу в системі права. Цей комплекс об'єднує різноманітні за своєю природою правові

норми, які регулюють суспільні відносини, пов'язані із захистом персональних даних фізичних осіб.

У системі права цей інститут слід розглядати як комплексний правовий механізм, а саме як "інститут захисту персональних даних". Його основу становлять норми міжнародного публічного та приватного права, а також правові положення конституційного, адміністративного, цивільного, кримінального, трудового, інформаційного та інших сфер національного права. З урахуванням комплексного характеру даного інституту і предмету його регулювання недоречно визначати його як багатогалузевий інститут, що входить до складу галузі інформаційного права. Унікальність суспільних відносин, які регулюються цим інститутом, разом із галузевою природою його юридичних норм, вимагає міжгалузевого (комплексного) регулювання.

Пропонуємо визначати поняття персональних даних як інформацію або сукупність відомостей, що безпосередньо чи опосередковано стосуються конкретної фізичної особи, незалежно від її громадянства, місця постійного проживання чи іншого юридичного зв'язку з державою, що є їхнім носієм. Ці відомості дозволяють ідентифікувати особу "прямо" або "опосередковано", при умові, що вони оброблялися через збирання, реєстрацію, накопичення, зберігання, адаптацію, зміну, оновлення, використання, поширення, анонімізацію, знищення, включаючи використання інформаційних (автоматизованих) систем.

Ураховуючи високий темп розвитку цього інституту, його кількісні та якісні характеристики, важко визнати його самостійною галуззю права на сучасному етапі. Тому твердження про галузеву самостійність цього нормативного комплексу, на даний момент, в юридичній науці вважається помилковим і не має об'єктивних підстав.

Поняття персональних даних включає в себе інформацію або сукупність відомостей, які прямо чи опосередковано стосуються конкретної фізичної особи. Незалежно від громадянства, постійного місця проживання чи інших правових зв’язків з державою, ці відомості дозволяють ідентифікувати особу. Обробка персональних даних може включати збирання, реєстрацію, накопичення,

зберігання, адаптацію, зміну, оновлення, використання, поширення та анонімізацію, а також знищення, в тому числі з використанням інформаційних (автоматизованих) систем.

У сучасних умовах визначається потреба в комплексному правовому захисті персональних даних. Міжнародна практика підтверджує тенденцію до універсалізації у цьому напрямі, розвиваючи загальні (наднаціональні) підходи до правового регулювання відносин, пов'язаних із захистом персональних даних.

Таблиця 1.1 Види персональних даних

№	Види персональних даних	Характеристика	Особливості обробки
1	загальнодоступні персональні дані	Це інформація, яка може бути визначена як особиста та входить до групи даних, отриманих з відкритих джерел, таких як адресні книги та довідники. До цих даних включаються прізвище, ім'я, по батькові, місце та дата народження, а також інформація про освіту та підвищення кваліфікації, а також трудова діяльність. Крім того, деякі з цих відомостей можуть стосуватися інтернет-простору, зокрема користувачів мережі Інтернет. Це може включати мережевий псевдонім, ідентифікатор облікового запису користувача та електронну пошту. Такі дані, як мережевий псевдонім чи ідентифікатор користувача, можуть бути використані для ідентифікації користувачів в онлайн-середовищі та дозволяють збирати і аналізувати інформацію про їхню активність в мережі. Отже, включаючи інформацію з різних джерел, таких як традиційні адресні книги та інтернет-платформи, ми отримуємо різноманітні дані, які можуть служити для ідентифікації та створення повної картини про особу, її взаємодію та активність як у офлайн, так і в онлайн середовищах.	Обробка загальнодоступних персональних даних, які містяться у відкритих джерелах, реалізується відповідно до побажань та вимог особи, що стосується цих даних. Такий підхід до обробки визначається уваженням до прав та побажань суб'єкта персональних даних, що є важливою особливістю цього процесу. У випадках, коли персональні дані стають доступними широкій громадськості, їх обробка регулюється узгоджено з волею особи, яка є суб'єктом цих даних. Це включає в себе право особи визначати, як її персональні дані будуть використовуватися та оброблятися згідно з вимогами та нормами приватності. Отже, особливості обробки загальнодоступних персональних даних здійснюються у відповідності до волі та побажань самої особи,

			яка стосується цих даних, покладаючи акцент на захист її приватності та дотримання встановлених норм. ;
2	особливі персональні дані	інформація, що розташована в закритих базах державних органів і включає в себе серію та номер паспорта, дані про військову службу, військовий квиток, наявність водійського посвідчення, страховий номер індивідуального особового рахунку, обов'язкове медичне страхування, індивідуальний номер платника податків та інші ідентифікаційні дані, які були надані державними органами.	Спеціальні персональні дані можуть бути оброблені у випадках отримання різних видів послуг, таких як державні, муніципальні та інші сервіси. Це відкриває можливість для обробки конфіденційних інформаційних даних в рамках надання різноманітних послуг громадянам та організаціям. Визначаючи особливості обробки спеціальних персональних даних, слід зазначити, що це відбувається у контексті отримання різних форм громадських, соціальних чи адміністративних послуг. При цьому можуть здійснюватися операції із збору, зберігання, обробки та передачі інформації, яка має особливий характер та стосується, наприклад, медичного стану, віросповідання чи інших конфіденційних аспектів особистого життя. Такий механізм обробки спеціальних персональних даних відкриває можливості для забезпечення необхідної конфіденційності та збереження прав та інтересів осіб, що звертаються за різними видами публічних та приватних послуг. ;
3	спеціальні персональні дані	До цієї інформації входять такі дані, як національність, расова приналежність, віровчення,	Обробка особливих персональних даних може мати місце лише у

		філософські переконання, політичні переконання, аспекти інтимного життя та стан здоров'я	випадках і за умов, які є об'єктивно необхідними для здійснення такої обробки. У таких ситуаціях визначається конкретний контекст і необхідність проведення обробки особливих персональних даних з урахуванням вагомості і обґрунтованості такого втручання у права та свободи осіб, які стосуються цих даних. Це підкреслює важливість встановлення чітких та обґрунтованих умов для обробки особливих персональних даних, що враховує потреби та права суб'єктів даних. Обмеження використання цих даних лише тоді, коли це дійсно необхідно, служить ключовим принципом, який забезпечує баланс між необхідністю обробки та захистом приватності та прав осіб.

Примітка. Складено автором

Розгляд поняття та різновидів персональних даних є ключовим кроком для визначення ефективних заходів їхнього захисту. Інститут захисту персональних даних виступає важливою юридичною гарантією, що визначає конституційні права особи на недоторканність приватного життя, особисту та сімейну таємницю. Цей інститут взаємодіє із правовими обов'язками інших суб'єктів, спрямованими на збереження цієї таємниці та забезпечення конфіденційності персональних даних.

Вищезгадані конституційні права людини та область їх реалізації становлять ключові елементи цього нормативного комплексу. Очевидно, що різні правові режими, включаючи режим воєнного стану, можуть визначати специфічні аспекти захисту прав громадян. У цих умовах важливо узгоджувати

заходи забезпечення безпеки та правил захисту особистої інформації з особливостями кожного контексту, забезпечуючи врегульованість та відповідність стандартам прав людини.

Під поняттям «захист персональних даних» розуміється ряд дій, які вживаються суб'єктами відповідних правовідносин з метою забезпечення високого рівня безпеки особистої інформації та персональних даних. Ці заходи спрямовані на досягнення таких цілей:

- передбачення витоків, розкрадань, втрат, спотворень та підробок персональних даних;

- захист від несанкціонованого доступу та дій, спрямованих на знищення, модифікацію, спотворення, копіювання та блокування інформації, пов'язаної з персональними даними. Також запобігання іншим формам незаконного втручання в інформаційні ресурси;

- гарантування захисту конституційних прав громадян на збереження особистої таємниці та конфіденційності персональних даних, що зберігаються в інформаційних системах;

- дотримання прав суб'єктів персональних даних у процесі розробки, виробництва та використання інформаційних систем, технологій та засобів їх забезпечення;

- запобігання завданню можливої шкоди суб'єкту персональних даних, такої як шкода для здоров'я, незаплановані фінансові чи матеріальні витрати, втрата свободи дій внаслідок шантажу чи погроз, що використовуються на основі персональних даних. Також, запобігання порушенню конституційних прав суб'єкта внаслідок втручання у його особисте життя шляхом контактування з ним з різних приводів без його згоди.

Право на захист персональних даних визначається комплексом заходів, які забороняють третім особам виконувати будь-які операції з особистими даними без виразної згоди власника цих даних. Крім того, воно наділяє суб'єктів персональних даних повноваженням контролювати дії операторів, які обробляють ці дані.

Визначення правового статусу захисту персональних даних базується на кількох ключових принципах, які грають важливу роль у правовому регулюванні цього питання:

Таблиця 1.2 Принципи захисту персональних даних громадян

Принцип захисту персональних даних	**Опис принципу**
1. Законність та справедливість	Обробка персональних даних повинна ґрунтуватися на законі та здійснюватися в справедливий спосіб.
2. Обмеження цілей обробки	Персональні дані можуть збиратися лише для визначених, законних і конкретних цілей та не можуть бути оброблені способом, несумісним із цими цілями.
3. Мінімізація обробки	Обробка повинна обмежуватися лише тими персональними даними, які необхідні для визначених цілей обробки.
4. Точність персональних даних	Забезпечення точності та актуальності персональних даних, а також їх виправлення у випадку неправильності.
5. Обмеження зберігання	Персональні дані повинні зберігатися лише протягом того періоду, який необхідний для досягнення цілей обробки.
6. Конфіденційність	Забезпечення належного рівня захисту та запобігання несанкціонованому доступу чи розголошенню персональних даних.
7. Відповідальність	Визначення відповідальних осіб та організацій за забезпечення відповідності з принципами захисту персональних даних.
8. Право суб'єкта на доступ і контроль	Забезпечення можливості суб'єкта персональних даних контролювати доступ, корегувати та видаляти свої дані.
9. Захист від автоматизованого прийняття рішень	Гарантування права суб'єкта на людський втручання при прийнятті рішень, що базуються на автоматизованій обробці його персональних даних.

Примітка: Складено автором.

Конфіденційність - забезпечення конфіденційності отримуваних персональних даних та обмеження доступу до них інших осіб є одним з важливих аспектів правового регулювання.

Достовірність та повнота - персональна інформація повинна бути достовірною та повною, виключаючи будь-які недостовірні або неповні дані.

Цільовий Характер обробки - обробка та зберігання персональної інформації повинні відбуватися тільки з визначеними законними цілями.

Законність Збирання та обробки - збирання та обробка персональної інформації повинні відповідати законним цілям та методам.

Сумлінність оператора - оператор повинен вести себе сумлінно та дотримуватися визначених норм та стандартів.

Право на інформацію - суб'єкт персональних даних повинен мати вільний доступ до своїх даних та право на повну інформацію про них.

Неприпустимість об'єднання Баз Даних - забороняється об'єднання баз даних, створених для несумісних між собою цілей.

Обмеження створення закритих інформаційних ресурсів - забороняється створення інформаційних ресурсів персонального характеру, які обмежені чи закриті для суб'єкта персональних даних, за винятком випадків, передбачених законом.

Гарантованість державою прав суб'єкта - держава гарантує суб'єктивні права особи, пов'язані із захистом її персональних даних.

Ці принципи становлять основу для розвитку ефективних та справедливих механізмів захисту персональних даних.

Загальний висновок, таким чином, може бути сформульований так: поняття «персональні дані» можна визначити як інформацію в машинно-орієнтованій формі, що включає дані про приватне життя живого індивіда (суб'єкта даних), який може бути ідентифікований на підставі цієї інформації або співставлення її з іншою інформацією. При цьому, якщо суб'єкт даних може розумно вважати цю інформацію конфіденційною та має право контролювати її розголошення, то ці дані можна вважати персональними. При цьому критерії «ідентифікованості суб'єкта даних» та «чутливості» враховуються, щоб визначити ступінь, на яку індивід може бути ідентифікований на основі цих даних та наскільки ця інформація може впливати на його приватне життя.

1.2 Організаційно-управлінські особливості обігу інформації, що містить персональні дані

Закон України «Про захист персональних даних» від 01.06.2010 р. № 2297–VI. встановлює правила збору, зберігання, використання та передачі персональних даних, а також встановлює права суб'єктів персональних даних [7]. Персональні дані громадян в першу чергу це інформація, що стосується конкретної особи, яка ідентифікується або може бути ідентифікована з використанням цієї інформації. Персональні дані громадян є важливим інформаційним ресурсом для багатьох сфер суспільної діяльності, включаючи державне управління, господарської діяльності, науки, медицини, військової справи тощо. Однак, збір, обробка та зберігання цих даних повинні здійснюватися відповідно до вимог законодавства щодо захисту персональних даних, щоб запобігти можливим порушенням прав та свобод суб'єктів персональних даних. Отже, персональні дані громадян можна розглядати як інформацію, що потребує особливої уваги та захисту з боку органів управління, корпоративних структур та інших сторін, які працюють з цими даними.

Закон України «Про захист персональних даних» від 01.06.2010 р. № 2297–VI. не використовує категорію «обіг персональних даних», а натомість вживає численні поняття «обробка персональних даних», «знеособлення персональних даних», «використання персональних даних», «збирання», «накопичення», «зберігання», «поширення», «видалення та знищення персональних даних» [7].

У цьому контексті О.С. Дяковський наголошує. що «обіг персональних даних» це – відносини зі збирання, реєстрації, зберігання, використання та поширення інформації, що містять персональні дані з використанням інформаційних (автоматизованих) систем, в результаті яких ці дані не змінюються [8]. Як бачимо категорії знеособлення персональних даних», «видалення та знищення персональних даних», автор до числа елементів обігу персональних даних не відносить.

Позбавлений Закон України «Про захист персональних даних» від 01.06.2010 р. № 2297–VI також прямих відсилок до певної групи процесуальних відносин, лише у загальному вигляді описуючи можливості здійснення «забезпечення захисту персональних даних» (ст. 24 Закон України «Про захист персональних даних» від 01.06.2010 р. № 2297–VI) [7].

Відповідно до положень теорії права у правовій системі існують два ключових компоненти: матеріальне та процесуальне право. Матеріальне право визначає сутність прав і обов'язків учасників правовідносин, дає відповідь на питання «що?». Процесуальне право, своєю чергою, регулює процес реалізації цих прав та обов'язків, відповідаючи на питання «як?». Процесуальні норми встановлюють правила діяльності органів влади, місцевого самоврядування та посадових осіб у правовому процесі. Процесуальне право також визначає права та обов'язки всіх учасників цього процесу. Стан правової системи неможливо оцінити, спираючись лише на матеріальне право. Процесуальне право допомагає забезпечити законність і досягнення результатів ефективного правового регулювання. Таким чином, процесуальні норми права – це норми, що забезпечують процедуру (порядок), форми реалізації або захисту норм матеріального права. Вони мають вторинний, похідний характер по відношенню до норм матеріального права. Функціональне призначення процесуальних норм полягає, передусім, в тому що вони закріплюють процедуру, форми реалізації або захисту (охорони) матеріальних норм, здійснення правового регулювання організаційних відносин. Водночас, коли ми ведемо мову про процесуальні норми та їх особливості то варто пам’ятати, що ми ведемо таку мову про норми процесуального характеру властиві певній правовій сукупності, - галузі права.

У сучасній адміністративно-правовій теорії поняття адміністративного процесу включає широке та вузьке розуміння. Так, В. О. Тімашов наголошує, що перший підхід, відомий як "юрисдикційний", передбачає його детальне та широке тлумачення. У вузькому розумінні адміністративний процес визначається як регульований нормами адміністративно-процесуального права порядок застосування заходів адміністративного примусу, в основному - адміністративних стягнень. Іншими словами, адміністративний процес

обмежується веденням справ щодо адміністративних правопорушень. У цьому розумінні адміністративний процес виявляє виключно юрисдикційний (правоохоронний) характер. Згідно з другим підходом, відомим як «управлінський», також називають «широким розумінням адміністративного процесу». В цьому випадку адміністративний процес розглядається як регульований нормами адміністративно-процесуального права порядок розгляду індивідуально-конкретних справ у сфері виконавчої діяльності органів державного управління. Іншими словами, в широкому розумінні адміністративний процес охоплює всю сукупність адміністративних проваджень [9, с.177].

Зазначений теоретичний підхід відображено у перспективному законодавстві, зокрема у Законі України «Про адміністративну процедуру» від 17 лютого 2022 року № 2073-IX (набере чинність 01.01.2024 року), наголошено, що він регулює взаємовідносини між органами виконавчої влади, органами місцевого самоврядування, їхніми посадовими особами та іншими суб'єктами, які мають визначені законом повноваження у сфері публічної адміністрації. Цей документ встановлює стосунки з фізичними та юридичними особами щодо розгляду та вирішення адміністративних справ шляхом прийняття та виконання адміністративних актів. В ньому також чітко вказано, що "адміністративна процедура" є законодавчо визначеним порядком розгляду та вирішення конкретних справ (п.5 ст. 2 Законі України «Про адміністративну процедуру» від 17 лютого 2022 року № 2073-IX) [10].

Таким чином, якщо ми будемо послуговуватися винятково теоретичним або нормативно-правовим тлумаченням процесуального впливу на відносини у сфері обігу інформації, що містить персональні дані з позицій адміністративного права то це не дасть нам можливості охопити такі відносини ефективним правовим регулюванням.

Зовсім іншим та набагато перспективнішим виглядає тлумачення нормативно-правового регулювання обігу персональних даних з позицій комплексного правового впливу, охоплюючи при цьому елементи властиві для предмету правового регулювання галузі конституційного, цивільного та

адміністративного права. Комплексне регулювання суспільних відносин у сфері персональних даних передбачає застосування низки законодавчих та нормативно-правових актів, які визначають права та обов'язки суб'єктів відносин у цій сфері. В Україні існують законодавчі акти, які стосуються захисту персональних даних та регламентують їх обіг, зокрема Закон України «Про захист персональних даних», Закон України «Про інформацію», Закон України «Про державну реєстрацію актів цивільного стану», Закон України «Про публічні електронні реєстри» тощо. Крім того, існують різноманітні нормативно-правові акти, які визначають правила обробки персональних даних у певних сферах, наприклад, медичній, соціальній, фінансовій тощо.

Комплексність процесуального правового регламентування обігу інформації, що містить персональні дані доводить і європейський правовий досвід. Справжнім «зразком», для української правової системи, правового регулювання та забезпечення захисту персональних даних є Регламент (Євросоюзу) 2016/679 [12].

Це обумовлено з одного боку тим, що хоч Україна і не є членом ЄС, але з іншого General Data Protection Regulation поширюються на осіб, що працюють у сфері робіт чи послуг, де бере участь суб'єкт (фізична особа), яка проживає в ЄС. На цьому етапі необхідно переглянути Privacy Policy, правила користування сайтом, додатки, сервіси [13]. Зазначені документи мають бути в злагодженій взаємодії між собою й General Data Protection Regulation.

Саме у Регламент (Євросоюзу) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 р. серед інших процедур йдеться про «псевдонімізацію» персональних даних – тобто, обробку персональних даних фізичної особи таким чином, щоб їх більше неможливо було віднести до конкретного суб'єкта даних без використання додаткової інформації, за умови, що така додаткова інформація зберігається окремо, і щодо неї вжито технічних та організаційних заходів, що запобігають її віднесенню ідентифікованій фізичній особі [12].

Застосування псевдонімізації до особистих даних може зменшити ризики для відповідних суб'єктів даних і допомогти «контролерам» і «процесорам» даних виконувати свої обов'язки з захисту даних. «Псевдонімізація» в Регламенті

(Євросоюзу) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 р. не означає відмову від інших заходів захисту даних. Щоб заохотити використання псевдонімізації при обробці даних, мають бути передбачені міри псевдонімізації у контролера, коли цей контролер прийняв необхідні технічні і організаційні заходи, а також щоб додаткова інформація, яка дозволяє віднести дані до конкретного суб'єкта, зберігалася окремо [12].

Таким чином, особисті дані, що пройшли псевдонімізацію, і можуть бути віднесені до фізичної особи за наявності додаткової інформації, мають розглядатися як інформація про ідентифіковану особу. Для встановлення можливості ідентифікації фізичної особи слід враховувати всі методи, щодо яких є реальна ймовірність їх використання для прямої або опосередкованої ідентифікації особи. При визначенні можливості використання такого методу слід враховувати всі об'єктивні фактори, такі як витрати і час, потрібні для ідентифікації, а також технології, доступні на момент обробки даних, і технологічний прогрес.

У підсумку наголосимо, що з нашої точки зору варто на доктринальному та нормативно-правовому півні визначити категорію «обіг персональних даних», що має охоплювати суспільні відносини не лише зі збирання, реєстрації, зберігання, використання та поширення інформації, що містять персональні дані, але й включати видалення персональних даних їх знищення та псевдонімізацію.

Під псевдонімізацією необхідно розуміти глибоке (істотне) знеособлення персональних даних, шляхом обробки персональних даних фізичної особи таким чином, що їх більше неможливо було віднести до конкретного суб'єкта даних без використання додаткової інформації, і за умови, що така додаткова інформація зберігається окремо, та щодо неї вжито технічних та організаційних заходів, що запобігають її віднесенню ідентифікованій фізичній особі. Також, зважаючи на комплексне регулювання суспільних відносин у сфері персональних даних необхідно вести мову про процесуальні особливості обігу інформації, що містить персональні дані. Такі особливості відзначаються тим, що визначені у законодавстві про захист персональних даних принципи правового регулювання цих відносин мають бути відображені у процесуальних приписах окремих

галузей права та міжгалузевих інститутах. До числа таких можна віднести процесуальні вимоги захисту персональних даних у адміністративно-управлінських, фінансово-податкових, митних, господарсько-цивільних, кримінально-процесуальних, трудових відносинах, відносинах у сфері соціального захисту, медичного забезпечення. проходження військової служби, оперативно-розшукової та контррозвідувальної діяльності. Їх головна особливість полягає у необхідності забезпечення захисту чутливої інформації фізичної особи на основі балансу суспільних інтересів та інтересів особи шляхом неухильного дотримання законності, адекватності, точності, обмеженості та цілісності і конфіденційності персональних даних. Таким чином у кожній сфері суспільних відносин мають бути розроблені відповідні процесуальні вимоги щодо обігу інформації яка містить персональні дані на основі базових правових вимог визначених у спеціальному законі та регламенті.

РОЗДІЛ 2. МЕХАНІЗМИ ПУБЛІЧНО-ПРАВОВОГО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ГРОМАДЯН

2.1 Законодавчі елементи механізму захисту персональних даних фізичних осіб органами публічної адміністрації

Правове регулювання захисту сфери приватного життя громадян є важливим аспектом сучасного правового середовища, оскільки забезпечує необхідний баланс між інтересами особистої свободи та колективної безпеки. Це поле права визначає обсяг і межі того, як інформація про особу може збиратися, зберігатися, оброблятися та розголошуватися.

Одним із основоположних аспектів правового регулювання є визнання сфери приватного життя як основного правового принципу. Це включає в себе захист від недозволених втручань у особисте життя, а також забезпечення конфіденційності особистих даних. Нормативно-правові акти про захист персональних даних, конституційні норми та рішення судів спрямовані на забезпечення цього захисту.

Важливою складовою правового регулювання є визначення обов'язків та відповідальності суб'єктів обробки персональних даних. Оператори та інші учасники, які мають доступ до особистої інформації, повинні дотримуватися встановлених норм щодо безпеки, зберігання та обробки даних.

Додатково, правове регулювання враховує виняткові обставини, такі як ситуації екстреної необхідності чи випадки, пов'язані з національною безпекою. Однак в таких випадках також передбачаються обмеження та гарантії, щоб уникнути надмірного втручання в особисту приватність.

Правове регулювання захисту сфери приватного життя громадян постійно вдосконалюється відповідно до технологічного розвитку та зміни суспільних потреб. Це сприяє створенню ефективної правової рамки, яка забезпечує надійний захист особистих даних та зберігає баланс між індивідуальними правами та загальними інтересами суспільства.

Утворення загального розуміння сфери приватного життя визначається як область особистих відносин індивіда, де йому надана свобода від втручання з боку держави, суспільства та інших осіб. Цей процес входить у рамки загального розвитку прав людини, ідеї правової держави і громадянського суспільства. Поняття сфери приватного життя, враховуючи його динаміку, не може бути універсальним і визначається різним чином в різних країнах. Це залежить від рівня суспільного розвитку, приналежності до конкретної цивілізації та особливостей історичного та культурного розвитку національного співтовариства.

Концепція права на недоторканість приватного життя у контексті сучасної системи прав людини визначає його важливе положення. Це право, визнане основоположним, має комплексний характер, охоплюючи всі особисті цивільні права людини, які визначають зміст сфери приватного життя, його недоторканність, а також забезпечення та захист цієї сфери. Одночасно воно впливає на соціальні, економічні та культурні права людини, сприяючи підвищенню якості приватного життя.

Ураховуючи те, що право на недоторканість приватного життя не є абсолютним, важливим є формулювання принципу дуалізму цілей правового регулювання сфери приватного життя. Цей принцип можна узагальнити, визначивши його так: метою правового регулювання сфери приватного життя є не тільки абсолютний захист права індивіда на недоторканість його приватного життя, але й забезпечення оптимального балансу інтересів між індивідом і суспільством в конкретних умовах.

Такий підхід визнає необхідність врахування різноманітних факторів і реалій, що визначаються сучасним суспільством, і наголошує на важливості збереження рівноваги між захистом особистих прав і загальними інтересами громади.

В світі визначальною концепцією щодо правового захисту сфери приватного життя є «прайвесі», яка виникла в межах європейської цивілізації як територіально-просторова концепція. Ця концепція виникла на тлі західної культурно-історичної традиції, яка розглядає наявність фізичного анклаву,

належать індивіду або займаного ним, як необхідну умову забезпечення приватності сфери приватного життя. Цей фізичний анклав вважається "персональним життєвим простором" індивіда.

Проектування територіально-просторового характеру концепції «прайвесі» виражається у панівному формулюванні права на недоторканість приватного життя як права індивіда "залишатися наодинці із собою" (to be let alone) протягом існування цієї концепції.

Протягом подальшого еволюційного розвитку концепція «прайвесі» зазнає перетворень, перейшовши з територіально-просторової форми в інформаційно-просторову. Домінуючим у формулюванні права на недоторканість приватного життя в рамках цієї концепції стає право індивіда на «контроль за циркуляцією інформації про себе (особистої інформації)».

У другій половині XX століття виникли і розвивалися інформаційні технології, що дозволили значно швидше обробляти великий обсяг інформації. У 60-ті роки ці технології стали все більш доступними, викликаючи певне занепокоєння Ради Європи [79]. Запропонована концепція техногенної еволюції інституту «прайвесі». Згідно з цією концепцією, ключовим фактором еволюції інституту є розвиток інформаційних технологій під час НТР.

Виділяються три виразно виражених етапи еволюції «прайвесі», коли виникають нові форми інституту, що характеризуються взаємопов'язаною сукупністю нових видів посягань на право на недоторканість приватного життя, нових принципів і засобів юридичного захисту сфери приватного життя. Ці етапи співпадають за часом з періодами домінування певних засобів збору, обробки та поширення особистої інформації в суспільстві (далі – «основні носії інформації»).

Проблему конфіденційності даних першою почала висвітлювати Німеччина, що у 1977 році прийняла свій перший закон про персональні дані (Bundesdatenschutzgesetz) [83]. У 1974 році газета Le Monde викликала резонанс статтею "SAFARI ou la chasse aux Français" (САФАРІ або полювання на французів), що стосувалася масового стеження. Під тиском громадськості уряд відступив, що призвело до утворення Комісії з інформатики та громадянських

свобод та прийняття згаданого вище закону [73]. У 1981 році була укладена перша міжнародна угода про конфіденційність даних - Конвенція про захист фізичних осіб при автоматизованій обробці персональних даних. Ця Конвенція стала значущим досягненням у цій галузі після Конвенції про захист прав людини і основних свобод від 04.11.1950 [33].

Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року [32] послужила основою для розробки Директиви 95/46/ЄС Європейського Парламенту і Ради ЄС "Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних", прийнятої 24 жовтня 1995 року [54]. Зараз ця директива заміщена Регламентом (Євросоюзу) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних та вільного переміщення таких даних [85].

Принципи, визначені в Європейській конвенції про захист прав і основних свобод, знайшли свій розвиток у 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 осіб, зокрема, їх права на недоторканість особистого життя у зв'язку з обробкою персональних даних. Причини прийняття пояснюються конфліктом, що виник наприкінці 1970-х років між інтенсивним впровадженням засобів автоматизованої обробки даних та їх поширенням у телекомунікаційних мережах, зловживанням при використанні персональних даних та потребою в упорядкуванні міжнародних операцій [6].

Україна затвердила цю Конвенцію лише 6 липня 2010 року [59]. Значення цього міжнародного документа для уніфікації правового регулювання відносин, пов'язаних з обробкою персональних даних, можна розкрити через наступні тези.

Приближення українського законодавства до стандартів Європейського Союзу, які визначають права фізичної особи у контексті обробки персональних даних, визвало прийняття важливого правового акта в Україні - Закону України «Про захист персональних даних» [53]. Цей закон, ухвалений Верховною Радою України 1 червня 2010 року під номером 2273-VI, позначив значний прогрес в

регулюванні обробки персональних даних в країні. Його сутність полягає у національній імплементації стандартів, визначених у Директиві 95/46/ЄС.

Зазначений закон визначає ключові аспекти захисту персональних даних та їх обробки, і може розглядатися як узгодження національного законодавства з європейськими стандартами. У своїй суті, цей правовий акт є національною реалізацією вимог, які містяться у відповідних нормах Директиви 95/46/ЄС. Такий підхід до інтерпретації закону надає можливість використовувати відповідні положення Європейської Директиви при тлумаченні його положень.

Ще однією важливою аспектом в контексті нормативно-правового регулювання є Закон України «Про інформацію». У цьому законі термін «персональні дані» визначається як «інформація про фізичну особу» (див. ст. 11 Закону України «Про інформацію» [56]). В Україні також впроваджено електронну систему охорони здоров'я, яка описана в Законі України «Про державні фінансові гарантії медичного обслуговування населення» [48]. Ця інформаційно-телекомунікаційна система автоматизує облік медичних послуг. При цьому функціонування електронної системи охорони здоров'я має дотримуватися вимог законодавства про захист персональних даних [66].

Специфіка захисту персональних даних в трудових правовідносинах передбачена передусім цілями обробки цих даних і регламентується Кодексом законів про працю України [30]. З іншого боку, роботодавець може обробляти персональні дані працівника, але лише в межах, необхідних для прийняття його на роботу та виконання ним трудової функції (див. ч. 2 ст. 24 Кодексу законів про працю України [30]).

Деякі положення Цивільного кодексу України також присвячені правам на особисте життя та його конфіденційність. Ці норми взаємодіють із іншими суб'єктивними немайновими правами, що на практиці виступають юридичними гарантіями для забезпечення таємниці особистого життя [72].

У той же час, швидкий розвиток інформаційних технологій вносить нові виклики у сферу приватності та особистого життя. Однією з основних проблем стало поширення Інтернету та його стрімкий прогрес. Першою потенційною загрозою цьому стало питання, яке виявив Європейський Союз, що вирішив

створити нормативну базу для адаптації до нових загроз та уніфікації законодавства щодо персональних даних в країнах-членах ЄС. З цією метою були вдосконалені механізми, передбачені міжнародною Конвенцією 1981 року, і введені нові зобов'язання для операторів персональних даних та нові права для громадян ЄС.

Питання необхідності «переосмислення» інструментів правового регулювання для інтернет-середовища акцентують вітчизняні дослідники [16], існуючий Кодекс України про адміністративні правопорушення вже включає відповідні юридичні положення. Наприклад, відповідальність за порушення умов і надання недостовірної інформації, що визначає порядок протидії порушенням авторських прав та (або) суміжних прав у мережі Інтернет, прописана в статтях 164-17 та 164-18 Кодексу України про адміністративні правопорушення [31].

Отже, Загальний регламент з питань захисту персональних даних (GDPR) та інші нормативні акти, які стосуються конфіденційності даних, не представляють собою нововведення в європейському законодавстві. Регламентація з питань захисту персональних даних, разом із всім комплексом реформ у сфері приватності, є результатом еволюції юридичної думки, що виникла на основі потреби захисту особистого життя будь-якого громадянина.

У національному контексті розвитку системи захисту персональних даних вирішальне значення мають нормативно-правові акти, спрямовані на врахування публічно-правових вимог щодо утворення ефективної системи захисту персональних даних та їх баз у різних інформаційних сферах та «середовищах». Це особливо актуально в контексті активності Міністерства цифрової політики України щодо впровадження застосунку «Дія».

Застосунок «Дія», впроваджений Міністерством цифрової трансформації України, представляє сучасний інструмент для надання громадянам доступу до публічних послуг та оптимізації їхнього використання. Цей інноваційний застосунок призначений для спрощення взаємодії громадян з державними органами та покращення якості надання адміністративних послуг.

Однією з ключових особливостей «Дії» є можливість централізованого доступу до різноманітних громадських послуг. Громадяни можуть використовувати застосунок для подання документів, запитань чи скарг, а також для взаємодії з державними інстанціями на відстані, що важливо, особливо в умовах сучасної цифрової епохи.

Ефективність «Дії» проявляється в широкому спектрі можливостей, доступних громадянам. Вона спрощує процеси отримання документів, надає оперативну зворотню зв'язок щодо статусу заявок, а також дозволяє громадянам ефективно взаємодіяти з різними рівнями влади.

Додатковою перевагою є впровадження елементів цифрової ідентифікації, які підвищують безпеку та забезпечують конфіденційність особистої інформації громадян. Це робить процес взаємодії з державними службами не лише зручним, але й високо надійним.

«Дія» також є важливим кроком у напрямку створення "єдиного вікна" для громадян у відносинах з державою. Цей застосунок покликаний об'єднати різні послуги в єдиному просторі, забезпечуючи громадянам швидкий та ефективний доступ до ресурсів держави.

Усе це дозволяє говорити про високий потенціал застосунку «Дія» в удосконаленні взаємодії громадян із державними службами та підвищенні якості надання публічних послуг. За допомогою цього інструменту, Україна визначається як країна, що активно використовує інновації для сприяння розвитку та зручності своїх громадян.

Підкреслимо, що право на захист персональних даних проявляє всі необхідні риси, що є характерними для підгалузі права. Це включає предметну єдність регульованих правом суспільних відносин, а також їх значимість для суспільства. Право на захист персональних даних реалізується через використання комплексу самостійних засобів та методів правового регулювання. Воно має свої власні джерела та спеціальні принципи, що діють в системі, спрямовані на цілеспрямоване регулювання суспільних відносин, що становлять предмет цього права. Забезпечено власну системну організацію, яка відображена в нормах щодо захисту персональних даних.

Перші норми щодо захисту персональних даних були розглянуті в контексті права на недоторканність особистого життя. Однак, в умовах переходу до інформаційного суспільства, де активно використовуються інформаційні технології та проводиться широкий збір і обробка інформації, виникла необхідність в правовому регулюванні обробки персональних даних. З поширенням "доби Інтернету" ця потреба стала тимчасовою і вимагає нормативно-правового регулювання захисту персональних даних.

Це включає облік операторів обробки у державному реєстрі, контроль за безпекою при обробці персональних даних в автоматизованих інформаційних системах, ліцензування та контроль за дотриманням ліцензіатами вимог та умов технічного захисту персональних даних, призупинення дії ліцензії у випадку порушення конфіденційності персональних даних. Також визначено процедури адміністративного припинення обробки персональних даних при порушенні законодавства, притягнення винних до відповідальності та опублікування звітів про стан захисту персональних даних у засобах масової інформації.

2.2 Визначення суб'єктів державного управління, які відповідають за захист персональних даних

Розглядаючи особливості персональних даних, можна виокремити різні суб'єкти інформаційних відносин, які підлягають регулюванню у сфері збору, обробки, використання та передачі цих даних. Один із ключових суб'єктів у цьому контексті - суб'єкт персональних даних, тобто фізична особа, що може бути ідентифікована на підставі цих даних чи за допомогою цих даних та іншої інформації, яка перебуває у володінні чи під контролем користувача даних.

Важливо враховувати, що ці дані, з точки зору пересічної людини або відповідно до вимог законодавства, можуть справедливо вважатися особистими, інтимними або конфіденційними. Такий підхід визначається ступенем чутливості і приватності інформації, а також конкретним контекстом обробки.

Таким чином, в сфері регулювання персональних даних слід враховувати різні відтінки чутливості цих даних, забезпечуючи належний захист прав та конфіденційність фізичних осіб. При цьому важливо дотримуватися принципів прозорості, справедливості та дотримання вимог законодавства для забезпечення справедливого та ефективного регулювання сфери обігу персональних даних.

Утримувач персональних даних, також відомий як контролер чи адміністратор файлів, представляє собою фізичну або юридичну особу, яка має право приймати рішення в рамках чинного законодавства щодо збору, обробки та передачі комп'ютеризованих чи інших технологічно заснованих персональних даних. Це може включати власників або ліцензованих операторів відповідних інформаційних ресурсів, а також осіб, які отримали спеціальне уповноваження від компетентних державних органів.

Користувач персональних даних – це фізична або юридична особа, яка відповідно до встановлених законом правил використовує зібрані та оброблені персональні дані, проте не є «власником даних» або «контролером файлів».

Оброблювач персональних даних, що їх обробляє, представляє собою фізичну або юридичну особу, яка має необхідні комп'ютерні або інші ресурси,

ліцензовані для здійснення обробки персональних даних. Оператори виконують автоматизовану чи ручну обробку даних, отриманих від комерційних замовників або інших осіб, які є «власниками» цих даних.

Збирач персональних даних – це особа, яка виконує первинний збір персональних даних відповідно до власних законних повноважень або за дорученням особи, що має такі повноваження.

Органи виконавчої влади утворюють систему, що об'єднує взаємопов'язані та взаємозалежні державні органи для здійснення виконавчої влади на території України [25, С.91]. Згідно з конституційно-правовою моделлю в Україні, існує три рівні органів виконавчої влади: вищі, центральні та місцеві [18, С.91]. Правовий статус Кабінету Міністрів України детально розкривається у Законі України від 27 лютого 2014 р. №794-VII "Про Кабінет Міністрів України". Згідно зі статтею 1 Закону України "Про центральні органи виконавчої влади" від 17 березня 2011 року № 3166-VI, систему центральних органів виконавчої влади складають міністерства України та інші центральні органи виконавчої влади.

Система центральних органів виконавчої влади включає міністерства, державні служби, державні агентства, державні інспекції, а також центральні органи виконавчої влади із спеціальним статусом [12, С.94]. Ця система є невід'ємною частиною загальної структури органів виконавчої влади, де вищим органом є Кабінет Міністрів України.

Відповідно до пункту 2 статті 1 Закону України «Про центральні органи виконавчої влади» від 17 березня 2011 року № 3166-VI, міністерства формують та втілюють державну політику у одній чи кількох сферах, тоді як інші центральні органи виконавчої влади виконують конкретні функції щодо реалізації державної політики. За словами В. Галунька, інші центральні органи виконавчої влади здійснюють реалізацію державної політики в певній сфері і, додатково, надають адміністративні послуги, ведуть державний нагляд (контроль), управляють об’єктами державної власності, систематизують практику застосування законодавства у справах, що входять до їхньої компетенції, і виконують інші повноваження, передбачені законодавством [13, С.96-97].

Зокрема, важливо відзначити, що у нашому дослідженні доцільно враховувати не лише класифікацію органів публічного адміністрування, визначену у нормативно-правових актах, а й підхід до визначення суб'єктів відносин, пов'язаних із персональними даними, який закріплений у статті 4 Закону України "Про захист персональних даних" від 01.06.2010 року № 2297–VI. Згідно з цим законом, органи публічної адміністрації виступають як володільці, розпорядники та треті особи персональних даних. Підкреслюється, що володільцем чи розпорядником персональних даних можуть бути також підприємства, установи і організації різних форм власності, органи державної влади чи місцевого самоврядування, фізичні особи - підприємці, які обробляють персональні дані відповідно до закону. Розпорядником персональних даних, володільцем яких є орган державної влади чи орган місцевого самоврядування, крім цих органів, може бути лише підприємство державної або комунальної форми власності.

Підкреслюється, що володільцем або розпорядником персональних даних можуть стати різноманітні юридичні та фізичні особи, що включає в себе не лише підприємства, установи і організації різних форм власності, а й органи державної влади та місцевого самоврядування. Фізичні особи, в тому числі підприємці, також можуть виступати як володільці та розпорядники персональних даних відповідно до чинного законодавства.

Важливо відзначити, що розпорядником персональних даних, якщо їх власником є орган державної влади чи місцевого самоврядування, може бути лише підприємство, яке має державну або комунальну форму власності. Це визначення обмежує можливість переходу контролю над персональними даними виключно на суб'єкти, які відповідають визначеним правовим стандартам та нормативам.

Такий розподіл володіння та управління персональними даними підкреслює важливість відповідності законодавчим вимогам у сфері захисту особистої інформації, а також наголошує на важливості прозорості та відповідальності при обробці особистих даних у різних секторах суспільства.

У контексті забезпечення безпеки персональних даних у державних органах, органах місцевого самоврядування та серед володільців чи розпорядників персональних даних, які проводять обробку інформації, що підлягає обов'язковому повідомленню згідно із чинним законодавством, встановлюється (визначається) структурний підрозділ або відповідальна особа. Ця структура чи особа координує діяльність, пов'язану із захистом персональних даних під час їх обробки.

Наприклад, національні поліцейські органи в Україні взяли на себе важливу місію забезпечення захисту персональних даних громадян у сучасному цифровому середовищі. За допомогою передових технологій та ефективних правових засад, Національна поліція виконує численні функції для забезпечення конфіденційності та безпеки особистої інформації громадян.

Однією з ключових обов'язків Національної поліції України є боротьба з кіберзлочинністю та незаконним доступом до персональних даних. Спеціальні підрозділи з кібербезпеки та кіберполіції вдосконалюють методи виявлення, запобігання та розслідування кіберзлочинів, спрямованих на порушення конфіденційності особистої інформації.

Національна поліція активно співпрацює з органами державної влади, міжнародними партнерами та власниками інформаційних систем для розробки та впровадження ефективних стратегій захисту персональних даних. Це включає в себе постійне оновлення систем безпеки, вдосконалення процедур обробки даних та розробку нових методів виявлення та запобігання кіберзлочинам.

Національна поліція також виконує роль освітнього партнера для громадян, надаючи їм інформацію про те, як ефективно захищати свої персональні дані в онлайн-середовищі. Це може включати в себе навчання про безпеку в Інтернеті, попередження щодо шахрайства та ідентифікацію потенційних загроз для конфіденційності особистих даних.

Національна поліція України розуміє важливість справедливого та етичного оброблення персональної інформації та активно застосовує всі необхідні заходи для забезпечення високого ступеня захисту персональних даних громадян в сучасному цифровому світі.

Пропонуємо розширити повноваження Уповноваженого органу захисту прав суб'єктів персональних даних за допомогою таких ініціатив:

- внесення до повноважень Уповноваженого органу обов'язку вести реєстр баз персональних даних.

- регулювання контролю за відповідністю транскордонної передачі персональних даних щодо невизначеного кола осіб, неповнолітніх та інших соціально незахищених верств населення до вимог законодавства.

- уповноважений орган може здійснювати аналіз законопроектів, які порушують конституційне право на недоторканість приватного життя, особисту та сімейну таємницю в контексті обробки персональних даних, та готувати висновки до їх набуття чинності відповідними законами. Подальше включення Уповноваженого органу у законотворчий процес дозволить оперативно реагувати на недоліки у законодавстві, виявлені в ході діяльності з захисту прав суб'єктів персональних даних.

- визначення Уповноваженим органом керівних принципів уніфікації заходів, спрямованих на дотримання законодавства щодо захисту приватного життя та персональних даних в умовах швидкого розвитку технологій. Розробка єдиних критеріїв та підходів в сфері захисту конституційного права на недоторканність приватного життя при обробці персональних даних.

Проведений аналіз вмісту інституту захисту персональних даних та практики його реалізації в діяльності органів виконавчої влади вказує на те, що правова основа захисту персональних даних в Україні не утворює стійкої та однорідної системи норм. Нормативні акти, які закріплюють відповідні правові положення, містять низку неточностей як теоретичного, так і практичного характеру. Присутні виразні прогалини та колізії в правовому врегулюванні розглянутих суспільних відносин.

РОЗДІЛ 3. УДОСКОНАЛЕНЯ ПУБЛІЧНО-УПРАВЛІНСЬКИХ МЕХАНІЗМІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ФІЗИЧНИХ ОСІБ

3.1 Захист персональних даних громадян у контексті державного управління

На сьогоднішній день, практика здійснення державної інформаційної політики потребує нового теоретичного підходу. Цей процес прямо пов'язаний з науковою обґрунтованістю та ефективністю впровадження інформаційної політики країни та її світоглядним забезпеченням. Застосування інформаційних технологій на основі цифрових каналів зв'язку трансформує існуючі методи виробництва та споживання, сприяючи виникненню нових інформаційних об'єктів у віртуальному середовищі. Віртуалізація відносин стає можливою завдяки різноманітним інформаційним системам.

До того моменту, поки правова система не розробить або не визначить спеціальний легальний режим для цих об'єктів, існуюча система правового регулювання є лише однією з форм вияву та втілення цифрової інформації. Важливо відзначити, що правове регулювання не визначає цінність нових явищ та категорій для обігу та забезпечення інформаційної безпеки. Значущість набуває інтерес суб'єктів правових відносин та можливості їх реалізації.

Цінність інформаційних об'єктів у віртуальному середовищі прямо формується та визначається користувачем інформаційної системи, який є учасником інформаційних відносин. Важливо відзначити, що ці питання не отримали достатньої уваги в адміністративно-правовій та управлінській науці, а також в інформаційній сфері, де державна інформаційна політика, як правило, розглядається як допоміжна для обслуговування корпоративних інтересів державної влади, а засоби масової інформації (як офіційні, так і незалежні) розглядаються як певний зв'язок між державою та громадянським суспільством.

Наукові дослідження природи публічної інформації є важливою сферою пізнання для адміністративно-правової науки, оскільки вони спрямовані на розуміння суспільних процесів та взаємодії між інститутами громадянського

суспільства, окремими особами та публічно-владними структурами. Дослідження в цій області включають в себе вивчення впливу інформації на суспільство, зокрема, як публічна інформація впливає на різні соціальні групи та як вона використовується для формування переконань та психологічних стимулів поведінки людей. Аналіз доступності публічної інформації дозволяє оцінити ефективність органів влади у забезпеченні доступу до інформації та визначити якість інформаційних послуг, які гарантуються законодавством.

Одночасно, дослідження технологій обробки та зберігання публічної інформації мають на меті покращення технологій зберігання, пошуку та обробки цієї інформації. В конечному підсумку, дослідження етичних аспектів використання публічної інформації надає можливість оцінити етичні вимоги до використання цієї інформації, особливо у відношенні до приватності та конфіденційності особистої інформації (персональних даних громадян).

У сучасній юридичній науці можна виділити загальне (широке) та спеціальне визначення поняття публічної інформації. Широке розуміння публічної інформації означає, що це інформація, яка є доступною для загального використання та розповсюдження. Це може бути інформація, опублікована у засобах масової інформації, на сайтах урядових органів, відкритих базах даних, наукових досліджень тощо. Зазвичай, публічна інформація вважається такою інформацією, яка не містить конфіденційних даних та є доступною для всіх, хто бажає отримати її. Вона може включати в себе такі види інформації, як законодавство, документи проектів, фінансову інформацію компаній, статистичні дані, наукові дослідження та інші види даних.

Одним із основних принципів публічної інформації є її відкритість та доступність для всіх, хто бажає її використовувати. Це допомагає забезпечити прозорість управління та демократію в суспільстві, а також забезпечує можливість використання цієї інформації для розвитку науки, бізнесу та інших галузей діяльності.

Закон України «Про доступ до публічної інформації» визначає публічну інформацію як інформацію, яка знаходиться у володінні або під контролем органів державної влади, органів місцевого самоврядування, підприємств,

установ, організацій, які здійснюють завдання публічного характеру, та є відкритою для використання і розповсюдження за умови дотримання вимог законодавства [8].

Закон України «Про доступ до публічної інформації» встановлює, що кожен має право на доступ до публічної інформації, яка знаходиться у володінні або під контролем органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, які здійснюють завдання публічного характеру. Це право може бути обмежене лише з тих мотивів, які передбачені законом, такі як захист державної таємниці, конфіденційності особистих даних, комерційної таємниці тощо.

Закон України «Про доступ до публічної інформації» також встановлює обов'язок органів державної влади, органів місцевого самоврядування та інших суб'єктів, які здійснюють завдання публічного характеру, забезпечити доступ до публічної інформації та надати її у відповідності до вимог законодавства. Вони повинні надавати цю інформацію безплатно або за символічну плату та незволікати з її наданням. Також зазначений нормативно правовий акт передбачає можливість звернення до суду в разі відмови в доступі до публічної інформації або ненадання її у повному обсязі.

Отже, можна виокремити кілька ключових ознак публічної інформації, на які вказує дане визначення: вона повинна віднесені до сфери відання та компетенції суб’єкта владних повноважень, існувати у конкретній матеріалізованій формі, і перебувати у володінні суб'єкта владних повноважень або іншого розпорядника публічної інформації [9].

З метою забезпечення уніфікованого застосування положень законодавства про доступ до публічної інформації, Пленум Вищого адміністративного суду України у своїй постанові № 10 від 29.09.2016 «Про практику застосування адміністративними судами законодавства про доступ до публічної інформації» вніс відповідні уточнення.

Отже, визначальним критерієм для публічної інформації є те, що вона має бути заздалегідь зафіксована будь-якими засобами та на будь-яких носіях і перебувати у володінні суб'єктів владних повноважень або інших розпорядників

публічної інформації. Також, важливо відмітити, що звернення, для відповіді на яке необхідно створити інформацію, не є інформаційним запитом, за винятком випадків, коли розпорядник інформації не володіє необхідною інформацією, але зобов'язаний нею володіти (пункт 1 частини першої статті 22 Закону № 2939-VI). Це важливий аспект, який допомагає відрізнити інформаційний запит від звернення, яке, як правило, передбачає створення нової інформації (наприклад, підготовку роз'яснень) [10].

Щодо інформації, що становить суспільний інтерес, Вищий адміністративний суд України, керуючись практикою Європейського суду з прав людини, включає до цього поняття:

- дані про втручання представників влади в кримінальне розслідування та тиск на суддів;

- інформацію про дипломатичні переговори з питань актуального інтересу та позицію уряду;

- зміст звернення депутата до Конституційного Суду щодо конституційності закону;

- дані про використання природних ресурсів та отримання дозволів на відчуження земельних ділянок;

- інформацію про можливі порушення громадських осіб у сфері приватного життя;

- дані про будівництво житла для депутатів за державний рахунок та оплату праці керівника великої приватної компанії;

- інформацію про можливі загрози здоров'ю та негативні умови догляду за пацієнтами [11].

Таким чином, публічна інформація повинна перебувати у володінні або під контролем органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, які здійснюють реалізацію завдань та функцій публічного характеру. Така інформація повинна бути відкритою для використання та розповсюдження, що означає, що вона повинна бути доступною для громадян з врахуванням особливостей процедур доступу до неї. Право доступу до публічної інформації нерозривно пов'язані з інститутом

адміністративних процедур, який наділяє має інформаційну природу декларація про специфічну адміністративно-процесуальну форму. Без зазначеної форми аналізоване право неспроможна реалізовуватися ефективно. Ідеальний підхід, згідно з яким право на доступ до публічної інформації може бути врегульовано за допомогою єдиної (загальної) процедури, не відповідає поточному рівню розвитку суспільних відносин у даній сфері. Поряд із зазначеною «загальною» процедурою необхідна система спеціальних процедур, які є формою найбільш поширених і (або) затребуваних відносин у сфері, що розглядається. До таких віднесено: процедура усного запиту; процедура запиту інформації з облікових систем (реєстрів); виняткова процедура (прискорений доступ до інформації, необхідної для запобігання суттєвим для суб'єкта запиту загрозам або здійсненням заходів з самозахисту прав чи запобігання правопорушень); процедура доступу до інформації з обмеженим доступом; процедура доступу до персональних даних Інформація повинна розповсюджуватися відповідно до вимог спеціального законодавства, що включає в себе забезпечення її точності, повноти та актуальності.

Вона повинна стосуватися питань публічного (загального) інтересу, таких як діяльність органів влади, розвиток економіки, соціальної сфери, охорони здоров'я, екології, оборони тощо. Інформація не повинна містити спеціальних обмежень щодо її використання, за винятком обмежень, передбачених законом, наприклад, захист державної таємниці, конфіденційності особистих даних, комерційної таємниці тощо. Така інформація повинна бути зберігатися у відповідних системах документообігу та веденні обліку.

Також існують особливі аспекти використання Інтернету, як для певних категорій населення в нормальних умовах, так і в умовах ведення бойових дій. Наприклад, важливою частиною реалізації свободи доступу до онлайн-середовища є доступ для певних груп осіб, таких як працівники правоохоронних органів, військовослужбовці, особи, які перебувають під воєнними зобов'язаннями під час проведення військових зборів, або особи, що відбувають різні види кримінальних покарань, пов'язаних із обмеженням або позбавленням волі. В Україні це питання стало особливо актуальним у зв'язку з проведенням

операції Антитерористична операція на сході країни, і обумовлено необхідністю захисту життя і здоров'я цієї спеціальної групи інтернет-користувачів, а також за мотивами збереження державної, військової таємниці.

Ми вважаємо, що можна взяти на увагу європейський досвід, як прикладом якого служить справа Калда проти Естонії (рішення від 19 січня 2016 року). Це рішення вирішує питання щодо прав в'язнів на доступ до Інтернету і може мати серйозні наслідки, оскільки воно встановлює перший прецедент для потенційного широкого розширення права на доступ до Інтернету для ув'язнених.

У цьому випадку, позивачем є громадянин Естонії, який перебуває під довічним покаранням у в’язниці міста Пярну. У 2005 році він звернувся до керівника в’язниці з проханням надати йому доступ до трьох веб-сайтів: онлайн версії Державної Газети; рішень Верховного Суду та адміністративних судів, які доступні в Інтернеті; бази даних HUDOC із рішеннями ЄСПЛ [89]. Відмовлено у наданні доступу, і Верховний Суд Естонії визначив, що така відмова є неправомірною. Однак позивача було переміщено до іншої в’язниці у місто Тарту, де він стикнувся із аналогічною проблемою. Вказуючи на конфлікти з адміністрацією в’язниці, Калда вимагав надати йому доступ до інших трьох веб-сайтів: Інформаційного офісу Ради Європи у Таллінні; Канцлера юстиції; Естонського парламенту [89].

Хоча в’язниця вже забезпечила ув’язнених доступом до деяких веб-сайтів, включаючи сайт ЄСПЛ, інформація на ньому була представлена лише англійською та французькою мовами. Адміністративний Суд вирішив, що Калді слід надати доступ до веб-сайту Інформаційного офісу Ради Європи, де є переклади рішень ЄСПЛ на естонську, проте вказав, що законом не передбачено доступу ув’язнених до двох інших веб-сайтів. Це рішення не влаштувало жодну зі сторін і призвело до подальшого оскарження. У своєму рішенні Верховний Суд відмовив позивачеві в праві на доступ до будь-якого з перерахованих веб-сайтів, пояснюючи це обґрунтуванням захисту правопорядку, збільшенням витрат на контроль за використанням Інтернету та наявністю альтернативних засобів для отримання офіційної інформації (бібліотека та пошта) [89].

Європейський Суд з прав людини (ЄСПЛ) розглядав дану справу у контексті порушення права на інформацію, визначеного в статті 10 Європейської конвенції з прав людини. Суд підкреслив, що суспільство має право на отримання інформації, що становить загальний інтерес, і держави повинні утримуватись від утруднення доступу особи до такої інформації. Однак Суд зауважив, що це право не можна трактувати як загальний обов'язок забезпечення доступу ув'язнених до Інтернету або конкретних сайтів, оскільки ув'язнення призводить до обмежень.

Суд визнав, що втручання було законним, оскільки воно передбачалося Актом про ув'язнення, який обмежував доступ до певних сайтів і ставив перед собою легітимні цілі захисту прав інших осіб та запобігання порушенням і злочинам. Суд також врахував необхідність у демократичному суспільстві таких свобод.

Суд зазначив, що інформація на сайтах, до яких прагнув отримати доступ позивач, мала переважно правовий характер та стосувалася основних прав людини, зокрема прав в'язнів, необхідної для захисту своїх прав в суді. Він вказав на різницю між самостійним пошуком інформації та можливістю звертатися до відповідного органу, що може займати додаткові кошти. Також була наголошена затримка у наданні перекладів рішень ЄСПЛ на доступних позивачеві сайтах порівняно із сайтом Ради Європи.

Суд визначив, що національні суди, посилаючись на загрозу безпеки, не провели детального оцінювання ризиків, пов'язаних з доступом до ще трьох конкретних сайтів. З урахуванням того, що ув'язнені мають доступ до Інтернету через спеціально обладнані комп'ютери, надання доступу до цих сайтів не повинно призвести до значних додаткових витрат. Отже, на підставі таких розсуджень ЄСПЛ визнав, що стаття 10 Конвенції була порушена. Це рішення підтримує необхідність врахування позиції ЄСПЛ при впровадженні прав засуджених на доступ до Інтернету в Україні.

Особливу увагу привертають аспекти свободи доступу до Інтернету для військовослужбовців під час виконання своїх обов'язків у зоні проведення операцій на сході країни. Згідно з рекомендаціями інформаційної та

кібернетичної безпеки в цій зоні, слід дотримуватися таких правил: уникати включення геолокації на особистих пристроях військовослужбовців, щоб уникнути визначення їх місцеперебування; використовувати паролі та якісне антивірусне обладнання; утримуватися від використання WiFi-роутерів та інтернет-модемів; дотримуватися безпечної поведінки в мережі; оберігати використання соціальних мереж, щоб уникнути розповсюдження інформації, що може викликати військовий інтерес або бути об'єктом розвідки.

Важливо враховувати, що виконання військовими завдань в зоні конфлікту підвищує ризик втрати чи конфіскації особистих пристроїв, таких як мобільні телефони, флеш-картки чи ноутбуки. На цих пристроях може міститися важлива інформація, така як копії паспортів, ідентифікаційних кодів, адреси, номери карток, телефонні номери близьких, доступи до електронної пошти, соціальних мереж та інша цінна інформація. Тому в рамках проекту "Інтернет-свобода в Україні: підтримуючи засади свободи слова та безпеки в часи конфлікту", що здійснюється за підтримки програми MATPA від уряду Нідерландів і впроваджується ГО "Інтерньюз-Україна", були розроблені рекомендації з метою покращення комунікації під час конфлікту, визначення викликів для свободи Інтернету та підвищення цифрової безпеки як на рівні інститутів, так і серед інтернет-користувачів.

У рекомендаціях для військовослужбовців пропонується вживати такі заходи як блокування пристроїв при віддаленні від них, встановлення повного шифрування для всіх дисків комп'ютера, використання надійного пароля для входу в соціальні мережі. Рекомендується утримуватися від входу в акаунти соцмереж з неповідомих чи незахищених пристроїв, розміщення часткової або неправдивої інформації про себе (наприклад, обмеження точності вказання місця навчання у військовій інституції та приналежності до конкретної військової частини для уникнення точного визначення місця служби). Також рекомендується обмежити доступ до приватної інформації у налаштуваннях конфіденційності соціальної мережі, переглянути список друзів у соцмережі і, якщо там є незнайомі або сумнівні особи, видалити їх. Зокрема, не слід фотографувати місця з видимими ознаками ландшафту чи території, а також

військову техніку (важливо, щоб її неможливо було ідентифікувати за зовнішніми знаками і позначеннями). Зазначено, що вважається обов'язковими, а не просто рекомендаційними, оскільки ці обмеження для цієї категорії осіб не порушують їхні права як інтернет-користувачів.

Як підсумок наголосимо, що структуру публічно-правового механізму захисту персональних даних громадян можна представити наступним чином (Таб. 3.1).

Таблиця 3.1 Структура публічно-правового механізму захисту персональних даних громадян

Структурний елемент	**Опис функцій та завдань**
Уповноважений орган захисту персональних даних	Відповідальний за контроль за дотриманням законодавства з захисту персональних даних, розгляд скарг, надання консультацій та рекомендацій громадянам та організаціям.
Законодавча база	Розроблення та удосконалення відповідного законодавства, встановлення правил та обов'язків стосовно обробки персональних даних.
Комітет з захисту персональних даних в організації	Забезпечення виконання правил та стандартів щодо захисту персональних даних у внутрішніх процесах організацій, підготовка персоналу та вивчення нових тенденцій у цій сфері.
Судова система	Вирішення справ та конфліктів, пов'язаних із захистом персональних даних.
Облікові палати та ревізійні органи	Здійснення аудиту та перевірок щодо дотримання законодавства з захисту персональних даних, розгляд порушень та надання рекомендацій для виправлення недоліків.
Громадські організації	Захист інтересів громадян у сфері обробки персональних даних, інформаційна освіта та підвищення правової грамотності.
ІТ-експерти та кібербезпека	Консультування організацій з питань технічної реалізації та захисту персональних даних в онлайн середовищі.

Примітка: Складено автором

При аналізі регулювання обробки персональних даних варто відзначити їх уніфікованість, що виявляється у забезпеченні безпеки накопичених особистих даних, можливості суб'єкта ознайомлення та уточнення своїх персональних

даних, а також у вимозі чітко формулювати мету використання цих даних, яку можна змінювати без згоди суб'єкта. Також важливо встановлення спеціального контролюючого органу, такого як Комісія чи Управління, що відповідає за відстеження дотримання прав суб'єкта персональних даних.

Відмінності можна виявити переважно в сфері визначення осіб, які повинні дотримуватися законів, що регулюють захист персональних даних відповідно до конкретної сфери діяльності. Надзвичайно важливою є офіційна позиція окремих зарубіжних джерел, яка визначає персональні дані працівника як інформацію, яка характеризує його професійні та ділові якості, необхідні для виконання трудових або службових обов'язків.

Мета обмеження конституційного права на недоторканність приватного життя, особисту та сімейну таємницю, а відповідно, прав персональних даних, полягає у необхідності забезпечення захисту основ конституційного ладу, моральних цінностей, прав та свобод людини та громадянина, з охорони здоров'я та створенні сприятливого довкілля, а також у забезпеченні оборони країни та безпеки держави.

3.2 Шляхи вдосконалення організаційно-управлінських засад державного управління у сфері захисту персональних даних громадян під час воєнного стану

Проблеми, пов'язані із забезпеченням захисту персональних даних громадян, що виникли після 24 лютого 2022 року, потребують негайного вирішення, включаючи вжиття заходів на нормативно-правовому та організаційно-управлінському рівнях. У той же час важливо зауважити, що в умовах широкомасштабної військової агресії та наявності декількох театрів бойових дій на території України необхідно розглядати не лише встановлення законних обмежень окремих прав і свобод людини і громадянина, але також розробку нових правових механізмів їх захисту через діяльність органів публічної влади та громадянського суспільства.

Особливе хвилювання викликає ситуація з дотриманням прав у сфері захисту персональних даних певних груп громадян, таких як військовослужбовці, примусово переміщені особи, жителі тимчасово окупованих територій і інші. Вже зараз це питання стає дуже актуальним для громадських активістів і волонтерів, оскільки вони можуть мати справу з особистою інформацією людей або вчасно повідомляти колег про збір персональних даних. Це може бути пов'язано з проведенням опитувань, фокус-груп, веденням списків для різних запитів допомоги, створенням списків для евакуації, складанням внутрішніх звітів чи поданням інформації міжнародним організаціям, які надають допомогу і т.д. Інформація, що стосується конкретної особи (її біографічні дані, ім'я, національність, адреса проживання, медична історія, професійні навички, сімейний стан, звички, інтереси, моральні, політичні, релігійні переконання та інше), часто становить значну частину інформації, що циркулює в суспільстві. Людина залишає відповідні "інформаційні сліди" у кадрових відділах, соціальних службах, органах виконавчої влади, в сфері обслуговування та різних організаціях.

Найчастіше розголошення такої інформації виникає з інтересів самої особи або стає умовою для отримання певного соціального статусу або послуг. Поширення особистої інформації без належної згоди може призвести як до формування позитивного іміджу, так і завдати серйозної шкоди, незалежно від того, чи є це моральна чи матеріальна шкода. Саме через це обробка інформації особистого характеру, включаючи персональні дані, потребує спеціального правового регулювання. На сьогодні можна заявити з упевненістю, що особиста інформація вважається одним із пріоритетних об'єктів захисту на рівні організаційно-правового середовища, оскільки в певних ситуаціях вона є вивідом права на приватне життя.

Очевидно, що людина, взаємодіючи як соціальний суб'єкт з іншими особами, організаціями і владними структурами, не може уникнути розголошення особистих даних, залишаючись анонімною в цих відносинах. У деяких випадках вона визначає, які саме дані слід повідомляти, а в інших (зазвичай у відносинах з державою) змушена надавати свої дані для здійснення юридично значущих дій, реалізації прав та виконання відповідних обов'язків.

Практично всі особи в суспільстві, за винятком можливо деяких рідкісних випадків, займаються трудовою діяльністю в різних формах. При вступі на роботу кожен громадянин, відповідаючи вимогам роботодавця, надає різноманітні документи та заповнює анкети, які охоплюють різні аспекти не лише професійної діяльності, але й затрагують сферу приватного життя особи. На першому етапі знайомства із потенційним працівником роботодавець виражає намір отримати максимальну інформацію про нього.

Проте відсутність чіткого критерію, який дозволяв би відрізняти інформацію особистого характеру, пов'язану з аспектами приватного життя особи, від інформації, що характеризує особу як працівника (на основі його ділових та професійних якостей, рівня освіти чи кваліфікації), є чинником, який ускладнює можливість роботодавця визначити ступінь припустимого втручання та меж вторгнення у приватне життя працівника.

Ця обставина породжує ситуації, коли відсутність чіткого розуміння того, яка інформація повинна бути визнана об'єктом захисту або особистими даними

працівника, призводить до неможливості реалізації норм, які визначають порядок та умови збору, зберігання, використання та поширення відповідної інформації в трудовій сфері.

З розвитком інформатизації суспільства та впровадженням нових та інтеграцією існуючих інформаційних систем, спрямованих на обслуговування населення, налагоджується збільшена увага до організації обробки персональних даних. Ці дані є важливою складовою інформаційного простору, яка містить відомості про фізичних осіб - суб'єктів персональних даних. Виділення цих даних в окремий підмножині обумовлено специфічними вимогами до організації їх обробки (діям з персональними даними), пов'язаними з можливістю завдання шкоди суб'єктам персональних даних. Таким чином, як у зарубіжних країнах, так і в Україні розвивається та вдосконалюється законодавча база, яка визначає правила обробки персональних даних і реалізацію прав громадян на конфіденційність інформації, що стосується їх. Особлива увага приділяється питанням захисту персональних даних в автоматизованих інформаційних системах персональних даних - ІСПД. Вимоги до захисту в ІСПД, відповідно до ряду документів, враховують категорію та кількість персональних даних, специфіку розв'язуваних завдань та інші показники.

Виконання цих вимог, як правило, пов'язане з значними матеріальними та фінансовими витратами, викликаними необхідністю створення системи захисту, забезпеченням високої кваліфікації персоналу та отриманням необхідних дозвільних документів. Однак це не завжди можливо для великої кількості користувачів інформації та операторів, які представляють малобюджетні організації, такі як медичні та освітні установи, підприємства та громадські організації.

У зв'язку з цим проводяться дослідження, спрямовані на розробку та аналіз методів обробки персональних даних, що дозволяють зменшити витрати на забезпечення безпеки в ІСПД. Однією з перспективних стратегій в цьому напрямку є обробка знеособлених персональних даних, коли стає неможливим визначити належність персональних даних конкретного суб'єкта без додаткової інформації. Це гарантує, що оператори та інші особи, які отримали доступ до

знеособлених даних, не можуть розкривати або передавати персональні дані третім особам без згоди суб'єкта персональних даних.

Для успішної реалізації цього підходу необхідно розробити та вивчити методи знеособлення та де-знеособлення персональних даних, а також встановити правила обробки знеособлених даних. Актуальність цього напряму досліджень обумовлена зростаючою потребою в розвитку ІСПД, відповідальністю за безпеку персональних даних та необхідністю підвищення ефективності створених систем при зменшенні витрат на їх експлуатацію, що досягається за наявності універсальних рішень.

Однією з перших ініціатив у сфері створення нових правових механізмів для захисту персональних даних громадян від органів публічної влади є Постанова Кабінету Міністрів України від 12 березня 2022 року № 263 "Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану". Ця постанова передбачає, що протягом періоду дії воєнного стану, органи влади, міністерства, інші центральні та місцеві органи виконавчої влади, державні та комунальні підприємства, установи та організації, які перебувають у сфері їх управління та є власниками (держателями) або адміністраторами інформаційних, інформаційно-комунікаційних та електронних комунікаційних систем, а також публічних електронних реєстрів, мають право вживати додаткові заходи для забезпечення належного функціонування цих систем та захисту оброблюваної в них інформації. Зокрема, ці заходи включають розміщення державних інформаційних ресурсів та публічних електронних реєстрів на хмарних ресурсах або в центрах обробки даних за межами України, а також реєстрацію доменних імен у домені gov.ua для такого розміщення. У разі необхідності, органи влади можуть призупиняти, обмежувати роботу інформаційних, інформаційно-комунікаційних та електронних комунікаційних систем, а також публічних електронних реєстрів [14].

Отже, державні органи створили необхідні організаційно-технічні умови для захисту прав окремих громадян, зокрема тих, які виконують завдання з оборони України і потребують додаткових гарантій щодо захисту своїх

персональних даних. Забезпечивши можливості для захисту інформаційних ресурсів, органи влади створили організаційно-технічні умови для захисту певних категорій громадян, які вимагають додаткових гарантій щодо конфіденційності їх особистих даних.

На сьогодні можна виділити кілька груп громадян, відносно яких виникають питання захисту персональних даних. Однак найбільш актуальні та загострені проблеми в цьому контексті виникають у зв'язку з українськими військовослужбовцями. Особливий акцент робиться на представниках силових структур, таких як Збройні Сили України, Національна гвардія України, Служба Безпеки України, Національна поліція, Державна прикордонна служба України та інші військові формування, які, маючи зброю в руках, забезпечують оборону країни.

Доступ агресора до особистих даних даної категорії осіб становить загрозу не лише національній безпеці, а й порушує права цих осіб та членів їх сімей. Наприклад, група російських хакерів RaHDIt, яка пов'язана з прокремлівськими інтересами, розмістила у відкритому доступі дані про 700 співробітників Служби безпеки України. Ця інформація включає ім'я, по батькові, прізвище, дату народження, посаду, звання, адресу, телефон, паспортні дані, а в деяких випадках – електронну пошту, сторінки в соцмережах та інші особисті дані. Зазвичай це супроводжується фотографією [64]. Ці дані можуть і вже використовуються противником для шкоди правам цих осіб та їх сімей, таких як залякування, моральні та фізичні травми, а також загроза життю.

Також, наслідком перебування військовослужбовця у зоні бойових дій часто стає його потрапляння в полон, що означає обмеження свободи через насильне утримання державою-противником, з метою обмеження участі в бойових діях. Військовополонені набувають статусу відповідно до Женевської Конвенції про поводження з військовополоненими від 12 серпня 1949 року [21].

Отже, випадок, коли військовослужбовці Збройних Сил України та члени добровольчих військових формувань, які ведуть опір окупантам на тимчасово непідконтрольних територіях України, потрапляють у полон до сепаратистів або регулярних військ російської федерації, фактично визначає їх як

військовополонених. З цим статусом пов'язані права на гідне та гуманне поводження, яке виключає будь-яку жорстокість, катування та дискримінацію за соціальними, расовими, релігійними, гендерними тощо ознаками [21]. На сьогоднішній день українські військовополонені, на жаль, не можуть бути впевнені, що до них будуть повністю застосовані міжнародні правові норми, які регулюють звичаї ведення війни.

Здобуваючи доступ до особистих даних військовополонених, противник може використовувати цю інформацію для шантажу їхніх родичів та урядових органів України, поширення панічних настроїв та інших гібридних методів інформаційної війни.

Група суспільних правовідносин, пов'язаних з оборотом та обробкою персональних даних, є єдиною, і це відноситься до інформації обмеженого доступу, що ідентифікує фізичних осіб за допомогою терміну "персональні дані". Регулювання цієї групи відносин здійснюється через сукупність правових норм, які утворюють комплекс і становлять окрему правову категорію. В наш час чітко виявляється необхідність у законодавчому врегулюванні самостійного обмеження доступу користувачів до персональних даних у соціальних мережах та медіа. На даний момент законодавство не встановлює обов'язок операторів обмежувати доступ до особистих даних користувачів через Інтернет. Специфічні особливості окремих інтернет-ресурсів дозволяють зареєстрованим користувачам отримувати доступ до персональних даних інших осіб.

Виникає нагальне питання, який орган публічної влади візьме на себе відповідальність за захист персональних даних військовослужбовців під час воєнних конфліктів і ким буде відповідати за їх розшук після припинення бойових дій. Також стурбованім викликає розповсюдження особистих даних військовослужбовців, включаючи військовополонених, в Інтернеті, що відбувається без контролю та в широкому масштабі.

Вільне розповсюдження аналогічної інформації під час ведення війни представляє собою серйозне порушення вимог міжнародних конвенцій, що стосуються військовополонених, і національного законодавства, включаючи захист персональних даних захисників України та громадян, які примусово

затримані чи викрадені. Зауважте, що Координаційний штаб із питань поводження з військовополоненими підкреслює, що публічне розповсюдження інформації про полонених може завдати шкоди процесу їх обміну. Розголошення інформації про значущі аспекти особистості, такі як політичні погляди, місце служби, попередні місця роботи, родинні зв'язки, може провокувати вороже ставлення. Це може призвести до переоцінки вимог до обміну конкретною особою, що ускладнює сам процес обміну. Важливо зазначити, що розповсюдження інформації про позивні, військові частини, місце розташування військових підрозділів та обставини потрапляння в полон несе загрозу не лише самому військовополоненому, але й його бойовим товаришам та військовому підрозділу в цілому" [43].

Міністерство оборони України веде інформаційну політику в цьому напрямку, наголошуючи, що громадські активісти, які збирають дані про загиблих і публікують цю інформацію, повинні розглядати той факт, що наразі таке розголошення інформації завдає шкоди обороні країни [24]. Сім'ї військовополонених часто не мають чіткого розуміння, як вони повинні діяти та до яких установ звертатися, коли надходить повідомлення про те, що їхній член сім'ї потрапив в полон, незважаючи на різні публікації в Інтернеті. Загальноприйнято вважати, що існують умовні "списки", на які вносяться відомості про полонених, після чого ці списки передаються уповноваженим державним органам для надання представникам Російської Федерації. В реальності ж не існує таких "списків", або, точніше сказати, такий підхід є дуже спрощеним. Фактично існує відповідний державний реєстр у Національному інформаційному бюро (https://nib.gov.ua/uk/).

Члени сімей військовослужбовців можуть внести інформацію про полоненого самостійно або через представника, використовуючи різні канали комунікації, такі як електронна пошта, спеціальна електронна форма або телеграм. В подальшому буде можливість моніторити статус військовослужбовця, наприклад, від статусу "ймовірно перебуває в полоні" до "перебуває в полоні". Важливо враховувати, що для підтвердження статусу

"перебуває в полоні" потрібно підтвердження від ворожої сторони або Міжнародного комітету Червоного Хреста.

Варто зауважити, що пріоритетів у визначенні осіб, які підлягають звільненню, не існує, і статус "ймовірного перебування в полоні" є досить умовним. Інформація, яка доступна у реєстрах Національного інформаційного бюро, використовується для координації пошуку та звільнення полонених, а також у проведенні перемовин щодо обмінів та звільнення.

Після проведеної зустрічі з сім'ями військовополонених був визначений алгоритм дій для офіційного внесення відомостей про полон членів їх сімей. Було уточнено, що Національне інформаційне бюро буде інформовано про перебування осіб в полоні, і взаємодія з НІБ передбачатиме інформування про цінність кожного окремого військового в контексті роз’яснення членам сімей механізму направлення звернень щодо перебування осіб в полоні.

В нашому розумінні важливо визначити конкретний орган публічної влади, який несе відповідальність за розповсюдження інформації про військовослужбовців та цивільних осіб, що стали жертвами війни, зникли безвісти або перебувають у незаконному утриманні окупаційною владою. Зараз існує "Гаряча лінія" Міністерства внутрішніх справ України для звернень родичів українських бійців, які перебувають у полоні, зникли безвісти або загинули. Фактично Міністерство внутрішніх справ України має обов'язок обробки інформації про персональні дані військовослужбовців, а реєстри цих осіб були створені співробітниками Міністерства з питань реінтеграції тимчасово окупованих територій.

Однак питання обміну військовополоненими на початкових етапах війни вирішувалося віце-прем'єром Міністерством з питань реінтеграції тимчасово окупованих територій, а після 2 червня 2022 року це питання неофіційно було передано до відома Головного управління розвідки України. Зрозуміло, що ці органи влади не мали офіційних повноважень і здійснювали їх ad hoc. На нашу думку, вирішення цього питання може бути досягнуте шляхом розширення повноважень Координаційного штабу з питань поводження з військовополоненими до рівня Міжвідомчого координаційного центру з обліку,

обміну та повернення полонених, зниклих безвісти та загиблих. До компетенції такого Міжвідомчого координаційного центру слід включити не тільки облік, обмін та повернення бойовиків, але й цивільних осіб (включаючи громадян іноземних держав або апатридів), які проживають або перебувають на території України.

Питання забезпечення безпеки особистих даних громадян у військовий період залишається дуже актуальним. Ефективний контроль інформаційного середовища стає ключовою умовою для гарантування захисту персональних даних громадян. Важливо покласти край неконтрольованому розміщенню у соціальних мережах численних сторінок з фотографіями та відео українських полонених, на яких також зазначені їх особисті дані. Ці заходи визначаються як чіткий акцент антиукраїнської пропаганди та як порушення прав військовополонених, включаючи сферу захисту їхніх особистих даних.

Додатково, для ефективного захисту персональних даних військовослужбовців пропонується розробити спеціальні інформаційні реєстри для цих категорій осіб. Ці реєстри повинні мати різні рівні верифікації доступу та стандартизовані можливості отримання інформації щодо осіб, включених до цих баз даних. Це буде сприяти запобіганню порушенням прав військовослужбовців, уникненню несанкціонованого доступу до їх особистих даних. До того ж, важливо визначити, який орган державної влади візьме на себе компетенцію забезпечення захисту персональних даних громадян у військовий час.

ВИСНОВКИ

1. Публічно-управлінські механізми забезпечення захисту персональних даних в сучасному світі відіграють важливу роль у забезпеченні прозорості, конфіденційності та безпеки особистої інформації. Ці механізми є ключовим елементом правового та організаційного впорядкування, спрямованого на захист індивідуальної приватності громадян. Одним з ефективних механізмів є створення та вдосконалення законодавчої бази, що регулює обробку та захист персональних даних. Закони та нормативні акти визначають права та обов'язки суб'єктів обробки даних, встановлюють процедури та відповідальність за порушення законодавства. Далі, важливою складовою є створення та діяльність органів з контролю за дотриманням законодавства з питань захисту персональних даних. Ці органи відповідають за моніторинг та реагування на можливі порушення, проведення розслідувань та захист прав громадян у цій сфері. Ще однією важливою ініціативою є розробка та впровадження стандартів безпеки та конфіденційності, які регулюють обробку та зберігання персональних даних. Це може включати в себе рекомендації щодо шифрування, захисту від несанкціонованого доступу та інші технічні аспекти забезпечення безпеки інформації. Публічно-управлінські механізми також можуть включати проведення освітніх кампаній та тренінгів для громадян та організацій, щоб підвищити їхню свідомість щодо захисту персональних даних та правильного використання інформації. Важливою частиною публічно-управлінських механізмів є також співпраця з приватним сектором та міжнародними партнерами для розробки інноваційних рішень та обміну кращими практиками в сфері захисту персональних даних. Усі ці елементи разом створюють ефективний публічно-управлінський механізм, спрямований на забезпечення надійного та сучасного захисту персональних даних у цифровому віці.

Запропоноване визначення терміну "персональні дані" враховує міжнародно визнані критерії, такі як «ідентифікованість суб'єкта даних» та «чутливість». Згідно з цим визначенням, персональні дані представляють собою дані у машинно-орієнтованій формі, які містять інформацію про приватне життя

конкретного живого індивіда (суб'єкта даних). Цей індивід може бути ідентифікований на підставі цієї інформації або за допомогою цієї та іншої інформації. Важливо, щоб суб'єкт даних, з точки зору будь-якої нормальної людини звичайною чутливістю, мав право вважати цю інформацію конфіденційною та контролювати її поширення.

Захист персональних даних має всі необхідні ознаки, які характерні для галузі інформаційного права. Це включає предметну єдність регульованих правом відносин на захист персональних даних, їх суттєву суспільну значимість, використання комплексу самостійних методів та прийомів правового регулювання, власні джерела правового регулювання, наявність спеціальних принципів захисту персональних даних і системна організація, яка відображена в нормах, регулюючих захист персональних даних.

2. У підсумку наголосимо, що з нашої точки зору варто на доктринальному та нормативно-правовому півні визначити категорію «обіг персональних даних», що має охоплювати суспільні відносини не лише зі збирання, реєстрації, зберігання, використання та поширення інформації, що містять персональні дані, але й включати видалення персональних даних їх знищення та псевдонімізацію.

Під псевдонімізацією необхідно розуміти глибоке (істотне) знеособлення персональних даних, шляхом обробки персональних даних фізичної особи таким чином, що їх більше неможливо було віднести до конкретного суб'єкта даних без використання додаткової інформації, і за умови, що така додаткова інформація зберігається окремо, та щодо неї вжито технічних та організаційних заходів, що запобігають її віднесенню ідентифікованій фізичній особі. Також, зважаючи на комплексне регулювання суспільних відносин у сфері персональних даних необхідно вести мову про процесуальні особливості обігу інформації, що містить персональні дані. Такі особливості відзначаються тим, що визначені у законодавстві про захист персональних даних принципи правового регулювання цих відносин мають бути відображені у процесуальних приписах окремих галузей права та міжгалузевих інститутах. До числа таких можна віднести процесуальні вимоги захисту персональних даних у адміністративно-управлінських, фінансово-податкових, митних, господарсько-цивільних,

кримінально-процесуальних, трудових відносинах, відносинах у сфері соціального захисту, медичного забезпечення. проходження військової служби, оперативно-розшукової та контррозвідувальної діяльності. Їх головна особливість полягає у необхідності забезпечення захисту чутливої інформації фізичної особи на основі балансу суспільних інтересів та інтересів особи шляхом неухильного дотримання законності, адекватності, точності, обмеженості та цілісності і конфіденційності персональних даних. Таким чином у кожній сфері суспільних відносин мають бути розроблені відповідні процесуальні вимоги щодо обігу інформації яка містить персональні дані на основі базових правових вимог визначених у спеціальному законі та регламенті.

3. Підсумовуючи, слід зауважити, що в національній правовій системі створені важливі передумови для правового регулювання суспільних відносин, пов'язаних із захистом персональних даних. Нормативно-правове регулювання персональних даних відрізняється своєю комплексністю, включаючи елементи, які є характерними для конституційного, цивільного та адміністративного права. Систематичне регулювання суспільних відносин у сфері персональних даних передбачає використання ряду законодавчих та нормативно-правових актів, що визначають права та обов'язки суб'єктів відносин у цьому полі.

В Україні існують закони, що стосуються захисту персональних даних та регламентують їх обіг, такі як Закон України "Про захист персональних даних", Закон України "Про інформацію", Закон України "Про державну реєстрацію актів цивільного стану", Закон України "Про публічні електронні реєстри" і т.д. Крім того, існують різні нормативно-правові акти, що визначають правила обробки персональних даних у різних сферах, таких як медична, соціальна, фінансова і інші.

Отже, на сучасному етапі розвитку суспільних відносин у сфері персональних даних громадян виникає потреба в проведенні кодифікації нормативно-правового матеріалу та формуванні *окремого "Інформаційного кодексу України",* де важливим елементом буде інститут персональних даних громадян. У національному контексті будівництва системи захисту персональних даних також велике значення мають нормативно-правові акти, які

спрямовані на врахування публічно-правових вимог до створення системи захисту персональних даних та їх баз в різних інформаційних сферах та "середовищах".

4. Підкреслимо, що право на захист персональних даних проявляє всі необхідні риси, що є характерними для підгалузі права. Це включає предметну єдність регульованих правом суспільних відносин, а також їх значимість для суспільства. Право на захист персональних даних реалізується через використання комплексу самостійних засобів та методів правового регулювання. Воно має свої власні джерела та спеціальні принципи, що діють в системі, спрямовані на цілеспрямоване регулювання суспільних відносин, що становлять предмет цього права. Забезпечено власну системну організацію, яка відображена в нормах щодо захисту персональних даних.

Перші норми щодо захисту персональних даних були розглянуті в контексті права на недоторканність особистого життя. Однак, в умовах переходу до інформаційного суспільства, де активно використовуються інформаційні технології та проводиться широкий збір і обробка інформації, виникла необхідність в правовому регулюванні обробки персональних даних. З поширенням "доби Інтернету" ця потреба стала тимчасовою і вимагає нормативно-правового регулювання захисту персональних даних.

Аналіз законодавства у сфері автоматизованої обробки персональних даних вказує на ряд заходів державного захисту права на недоторканність приватного життя в умовах автоматизованої обробки персональних даних та відповідні процедури їх застосування. Це включає облік операторів обробки у державному реєстрі, контроль за безпекою при обробці персональних даних в автоматизованих інформаційних системах, ліцензування та контроль за дотриманням ліцензіатами вимог та умов технічного захисту персональних даних, призупинення дії ліцензії у випадку порушення конфіденційності персональних даних. Також визначено процедури адміністративного припинення обробки персональних даних при порушенні законодавства, притягнення винних до відповідальності та опублікування звітів про стан захисту персональних даних у засобах масової інформації

5. В умовах воєнного стану в Україні надзвичайно важливим є захист персональних даних від випадкової втрати чи знищення, незаконної обробки, включаючи незаконне знищення чи несанкціонований доступ до цих даних. Також важливо забезпечити захист державних інформаційних ресурсів, ІТ-систем об'єктів критичної інфраструктури та державних реєстрів, які містять персональні дані. Обробка персональних даних повинна відповідати вимогам законодавства України, стандартам ЄС та бути пропорційною та здійснюватися виключно для конкретних та законних цілей.

Адміністративно-правове забезпечення захисту персональних даних в умовах воєнного стану має включати не лише застосування «пасивних» засобів захисту персональних даних але й комплексу *активних заходів спрямованих на виявлення та здір і обробку персональних даних* військовополонених, цивільних громадян та особливо дітей незаконно депортованих на територію країни-агресора. Зазначені повноваження мають знайти своє відображення у компетенції окремих органів публічної влади. Забезпечення захисту персональних даних має включати інформацію яка дозволяє ідентифікувати осіб, що співпрацюють з правоохоронними органами України та міжнародними чи іноземними агенціями, які займається збором даних про злочини вчинені військовослужбовцями або керівництвом росії. Підкреслимо, що сьогодні питання захисту персональних даних, їх баз та реєстрів лишаються винятково важливими завданнями для органів публічного адміністрування.

У рекомендаціях для військовослужбовців пропонується використовувати такі заходи для захисту особистої інформації: блокувати пристрої кожного разу, коли ви віддаляєтеся від них, встановлювати повне шифрування для всіх дисків комп'ютера, встановлювати надійний пароль для входу в соціальну мережу, уникати входу в облікові записи соціальних мереж з невідомих або неповірених пристроїв, публікувати часткову або micleading інформацію про себе, таку як вказування невірної інформації у профілі Facebook, наприклад, щодо місця навчання у військовій інституції та участь у конкретних групах.

6. Проблема забезпечення безпеки особистих даних громадян органами публічної влади в умовах війни залишається надзвичайно актуальною.

Ключовим аспектом для гарантування захисту персональних даних громадян є контроль над інформаційним середовищем, яке має призвести до уникнення несанкціонованого розміщення на соціальних мережах численних сторінок з фотографіями та відео українських полонених із їх особистою інформацією. Зазначені заходи розглядаються як прояв антиукраїнської пропаганди та порушення прав військовополонених, включаючи сферу захисту їхніх персональних даних.

Крім того, на нашу думку, для ефективного захисту персональних даних військовослужбовців необхідно розробити окремі інформаційні реєстри для зазначених вище категорій осіб з різним рівнем верифікації доступу до них та стандартизації можливості отримання інформації про суб'єктів, включених до цих баз даних. Це має включати різні рівні доступу та регламентувати можливість одержання інформації про конкретні особи в цих базах даних чи, навпаки, визначати, що інформація про певні особи відсутня. Зазначений підхід покликаний протидіяти неконтрольованому розміщенню в соціальних мережах численних сторінок з фотографіями та відео українських військових і військовополонених із їх особистими даними, забезпечуючи запобігання порушенням прав військовослужбовців через несанкціонований доступ до їх особистих даних.

Додатково важливо визначити, до компетенції якого з органів державної влади має відноситися питання забезпечення захисту персональних даних громадян в умовах війни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аномалії в цивільному праві України : навч.-практ. посіб. / відп. ред. Р. А. Майданик. Київ : Юстініан, 2007. 912 с.
2. Булеца С. Б. Персональні дані пацієнта. *Науковий вісник Ужгородського національного університету*: Серія ПРАВО. Випуск 22. Частина 2. Том 1, 2014. С. 186-191.
3. Бєлова Ю.Д. Стандарти захисту права на персональні дані відповідно до практики ЄСПЛ. *Україна на шляху до Європи: реформа цивільного процесуального законодавства*. Зб. наук. праць Матеріали Міжнар. наук.-практ. конф. Київ: ВД Дакор, 2017. С. 86-89.
4. Бєлова Ю.Д. Цивільні правовідносини щодо персональних даних. Хмельницький: ФОП Мельник А.А., 2019, 192 с.
5. 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.
6. Брижко В. М. Захист персональних даних: реалії та практика сучасності. *Інформація і право*. 2013. № 3. С. 31-48.
7. Брижко В. М. Захист персональних даних: реалії та практика сучасності. *Інформація і право*. 2013. № 3. С. 31-48.
8. Булеца С. Б. Персональні дані пацієнта. *Науковий вісник Ужгородського національного університету*: Серія ПРАВО. Випуск 22. Частина 2. Том 1, 2014. С. 186-191.
9. Великий тлумачний словник сучасної української мови (з дод. і допов.) / Уклад, і голов, ред. В. Т. Бусел. Київ; Ірпінь: ВТФ «Перун», 2005. 1728 с.
10. Власко С. Захист персональних даних: чий досвід може стати в нагоді Україні. URL:https://www.eurointegration.com.ua/experts/2018/01/16/7076152/
11. Волкова Н. В. Засоби індивідуалізації фізичних осіб (окремі аспекти). *Актуальні питання держави і права*. 2008. № 39.С. 238-243.

12. Гега П.Т. Основи податкового права : навчальний посібник. Київ : Т-во «Знання», КОО. 2003. 318 с.

13. Гражданское право: актуальные проблемы теории и практики /Под общ. ред. В.А. Белова. М.: Юрайт-Издат, 2007. 993 с.

14. Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану: Постанова КМУ від 12 березня 2022 р. № 263. URL: https://www.kmu.gov.ua/npas/deyaki-pitannya-zabezpechennya-funkcionuvannya-informacijno-komunikacijnih-sistem-elektronnih-komunikacijnih-sistem-publichnih-elektronnih-reyestriv-v-umovah-voyennogo-stanu-263. (дата звернення 30.05.2022 р.)

15. 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.

16. 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;

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

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

19. Еннан Р. Є. Правове регулювання відносин у мережі Інтернет. IT право: проблеми і перспективи розвитку в Україні URL: http://aphd.ua/publication-173/.Інтернет-відносин. *Право України*. 2003. №5. С. 124-127

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

21. Женевська Конвенція про поводження з військовополоненими: Міжнародна Конвенція від 12 серпня 1949 р. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/995_153?find=1&text=%D0%B2%D1%

96%D0%B9%D1%81%D1%8C%D0%BA%D0%BE%D0%B2%D0%BE%D0%BF%D0%BE%D0%BB%D0%BE%D0%BD%D0%B5%D0%BD#w1_4 t (дата звернення 05.07.2022 р.)

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

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

24. Заступниця міністра оборони пояснила, чому не розголошують скільки військових загинули. URL: https://www.pravda.com.ua/news/2022/07/14/7358178. (дата звернення 05.07.2022 р.

25. 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.

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

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

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

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

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

31. 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

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

33. 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

34. Конституція України : Закон України від 28 червня 1996 року № 254к/96-ВР. Верховна Рада України. База «Законодавство України». URL: http:// http://zakon2.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80. (дата звернення 30.05.2022 р.)

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

36. 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.

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

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

39. МВС запустило гарячу лінію для звернень родичів українських військових, які загинули або зникли безвісти. URL: https://www.kmu.gov.ua/news/rozpochinaye-svoyu-robotu-garyacha-liniya-mvs-dlya-zvernen-ridnih-ta-blizkih-polonenih-zniklih-bezvisti-ta-zagiblih-ukrayinskih-zahisnikiv. (дата звернення 30.05.2022 р.)

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

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

42. Новицький А. Щодо питання структуризації інформаційного права як наукової категорії. *Актуальні проблеми правознавства*. 2016. Вип. 4. С. 34-38.

43. Оприлюднення інформації про полонених може зашкодити обміну – ГУР. URL: https://www.pravda.com.ua/news/2022/07/15/7358266/. (дата звернення 05.07.2022 р.)

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

45. 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.

46. 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

47. Про введення воєнного стану в Україні: Указ Президента України від 24 лютого 2022 року №64/2022 URL: https://www.president.gov.ua/documents/642022-41397 (дата звернення 30.05.2022 р.)

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

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

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

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

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

53. 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

54. 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.

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

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

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

58. 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.

59. 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.

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

61. 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.

62. 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.

63. 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.

64. Российские хакеры опубликовали данные 700 сотрудников СБУ. URL: https://www.newsru.co.il/world/1jun2022/sbu_hack_106.html. (дата звернення 30.05.2022 р.)

65. Селезньова О.М. Теоретико-методологічні основи інформаційного права України : моногр. Чернівці: Місто, 2014. 408 с.

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

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

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

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

72. Цивільний кодекс України : Закон України від 16.01.2003 р. № 435-IV. URL : https://zakon.rada.gov.ua/laws/show/435-15

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

74. 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.

75. Що варто знати про захист персональних даних в період воєнного стану? URL: https://www.prostir.ua/?news=scho-varto-znaty-pro-zahyst-personalnyh-danyh-v-period-vojennoho-stanu. (дата звернення 30.05.2022 р.)

76. 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

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

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

79. 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

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

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

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

83. 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/

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

85. 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

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

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

88. Case of Kalda v. Estonia. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22-

89. Калда проти Естонії: ЄСПЛ висловився щодо права в’язнів на доступ до Інтернету. 15.08.2016 р. URL:https://cedem.org.ua/news/kalda-proty-estoniyi-yespl-vyslovyvsya-shhodo-prava-v-yazniv-na-dostup-do-internetu/

Виконав: студент магістратури

спеціальності 281 Публічне управління та адміністрування заочної форми навчання		Назарова Катерина Юріївна
«____» грудня 2023 р.	Підпис	Ініціали, прізвище

Науковий керівник

доктор наук з державного управління, доцент, доцент кафедри публічного управління та адміністрування		Маланчій Микола Олександрович,
«____» грудня 2023 р.	Підпис	Ініціали, прізвище

Робота допущена до захисту:

Завідувач кафедри публічного управління та адміністрування доктор наук з держ. управління, професор		Щепанський Едуард Валерійович
«____» грудня 2023 р.	Підпис	Ініціали, прізвище