

ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА  
ІМЕНІ ЛЕОНІДА ЮЗЬКОВА

ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ЕКОНОМІКИ

Кафедра: публічного управління та адміністрування

**МАГІСТЕРСЬКА РОБОТА**

на здобуття освітнього рівня Магістр

на тему:

**ДЕРЖАВНІ ІНСТРУМЕНТИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ  
ГРОМАДЯН В УМОВАХ ВІЙНИ**

**Виконав:** студент магістратури  
за спеціальністю 281 Публічне  
управління та адміністрування

**Бондар Дмитро**

**Володимирович**

\_\_\_\_\_ (прізвище та ініціали)

**Керівник:** кандидат наук з  
державного управління,  
доцент, доцент кафедри  
публічного управління та  
адміністрування

**Баюк Микола Іванович**

\_\_\_\_\_ (прізвище та ініціали)

**Рецензент:** \_\_\_\_\_

(прізвище та ініціали)

Хмельницький – 2022 рік

## АНОТАЦІЯ

**Бондар Д. В. Державні інструменти захисту персональних даних громадян в умовах війни.** 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, 2022. – 78 с.

Запропоноване таке визначення поняття "персональні дані", що враховує міжнародно-визнані критерії «ідентифікованості суб'єкта даних» та «чутливості»: персональні дані - це дані в машинно-орієнтованій формі, що містять інформацію про приватне життя конкретного живого індивіда (суб'єкта даних), що може бути ідентифікований на підставі цієї інформації (або за допомогою цієї та іншої інформації), якщо з точки зору будь-якої нормальної людини, наділеної звичайною чутливістю, суб'єкт даних має право вважати таку інформацію конфіденційною та контролювати її поширення. Захист персональних даних має всі необхідні ознаки, які притаманні підгалузі інформаційного права, а саме: предметна єдність регульованих правом на захист персональних даних суспільних відносин та їх суттєва суспільна значимість; використання комплексу самостійних способів та прийомів правового регулювання захисту персональних даних. Проблема забезпечення захисту персональних даних органами публічної влади в умовах війни залишається винятково гострою. Важливою умовою забезпечення захисту персональних даних громадян має бути контроль інформаційного середовища, що повинно покласти краї неконтрольованому розміщенню у соціальних мережах багаточисельних сторінок з фотографіями та відео українських полонених з їх персональними даними. Зазначені заходи носять явний акцент антиукраїнської пропаганди та є порушенням прав військовополонених у тому числі і у сфері захисту їх персональних даних.

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

## THE SUMMARY

**Bondar D. V. State tools for protection of personal data of citizens in war conditions.** Qualifying scientific paper on copywriting. 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, 2022. – 78 p.

The proposed definition of "personal data" takes into account the internationally recognized criteria of "identity of the data subject" and "sensitivity": personal data is data in a machine-oriented form containing information about the private life of a specific living individual (subject data subject) who can be identified on the basis of this information (or with the help of this and other information), if from the point of view of any normal person endowed with ordinary sensitivity, the data subject has the right to consider such information confidential and to control its dissemination. The protection of personal data has all the necessary features that are inherent in the sub-branch of information law, namely: the substantive unity of social relations regulated by the right to protect personal data and their essential social significance; use of a complex of independent methods and techniques of legal regulation of personal data protection; availability of own sources of legal regulation; own system organization, which is reflected in the regulations on personal data protection. The problem of ensuring the protection of personal data by public authorities in war conditions remains extremely acute. An important condition for ensuring the protection of personal data of citizens should be the control of the information environment, which should put an end to the uncontrolled placement in social networks of numerous pages with photos and videos of Ukrainian prisoners with their personal data. The specified measures have a clear accent of anti-Ukrainian propaganda and are a violation of the rights of prisoners of war, including in the field of protection of their personal data.

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

## ЗМІСТ

ВСТУП.....	5
РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ЗАСТОСУВАННЯ ДЕРЖАВНИХ ІНСТРУМЕНТІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ГРОМАДЯН В УМОВАХ ВІЙНИ.....	11
1.1 Поняття персональних даних та їх захисту .....	11
1.2 Режим воєнного стану як особливий правовий період .....	17
РОЗДІЛ 2. АНАЛІЗ ДЕРЖАВНИХ ІНСТРУМЕНТІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ГРОМАДЯН В УМОВАХ ВІЙНИ .....	23
2.1 Нормативно-правові засади застосування державних інструментів захисту персональних даних громадян .....	23
2.2 Суб'єкти відносин щодо застосування державних інструментів захисту персональних даних громадян під час війни.....	31
РОЗДІЛ 3. УДОСКОНАЛЕННЯ ОРГАНІЗАЦІЙНО-УПРАВЛІНСЬКИХ ІНСТРУМЕНТІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ГРОМАДЯН В УМОВАХ ВІЙНИ.....	39
3.1 Захист персональних даних громадян в умовах війни у контексті державного управління .....	39
3.2 Напрями удосконалення організаційно-управлінських засад державного управління у сфері захисту персональних даних громадян під час війни .....	52
ВИСНОВКИ.....	63
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	66

## ВСТУП

**Актуальність теми.** Актуальність теми пов'язана з сучасним етапом всеохоплюючого запровадження інформатизації процесів публічного управління через створення масштабних баз даних та широкого доступу органів влади до персональних даних. Побудова демократичної соціальної правової держави, найвищою цінністю в якій є людина, її честь і гідність, недоторканність і безпека, як і підтримання ефективного функціонування державних інститутів перебувають у нерозривному зв'язку із необхідністю вдосконалення захисту основних прав людини та громадянина.

Наукові відкриття в генній інженерії та використання комп'ютерної психотехнології, транскордонних інформаційних мереж піднімають проблеми правового захисту приватного життя не лише на національному рівні, а й на міжнародному, що, звичайно ж, потребує більш глибокого вивчення цих питань.

З одного боку, за умов сучасного розвитку цивілізації та повсюдного впровадження інформаційно-телекомунікаційних технологій розширюється доступ людей до інформації, об'єктивно сприяючи здійсненню прав людини на свободу інформації. Автоматизовані бази даних щодо можливостей зберігання інформації та зручності доступу до неї набагато перевершують сховища ручних архівів (дисккові накопичувачі комп'ютера здатні зберігати обсяги інформації, еквівалентні великим університетським бібліотекам). Комп'ютер уможливив ефективне комбінування неосяжних масивів інформації. Комп'ютерні процедури зіставлення даних з різних файлів (процедури типу *data matching*) дають можливість складання "біографічних портретів" індивідів за допомогою інформації, зібраної з різних баз даних.

З іншого боку, доступ фізичних осіб та колективних утворень до баз персональних даних посилює ризик вторгнення у сферу приватного життя та порушення права на його недоторканність. ІТТ гранично загострили правові проблеми, пов'язані з дилемою "розкриття інформації чи захист приватного життя". Звідси особливо гостро постає проблема створення ефективного

механізму правового захисту приватного життя як на національному, так і на міжнародному рівні під час транскордонної передачі даних.

У розвинених демократичних країнах, починаючи з другої половини ХХ століття, правовий захист сфери приватного життя у зв'язку з використанням інформаційних технологій став одним із пріоритетних напрямків у галузі охорони прав людини. Їй присвячено численні теоретичні дослідження. У національних системах правового захисту приватного життя – а нині є всі підстави говорити про такі системи – розроблено спеціальні засоби правового регулювання автоматизованої обробки персональних даних. У період комп'ютерів автоматизована обробка персональних даних є основним джерелом загроз для сфери приватного життя. Формування світового інформаційного простору, що почалося, на базі глобальних комп'ютерно-телекомунікаційних мереж поставило на порядок денний найважливіше завдання встановлення одноманітного національного та міжнародного правового регулювання обробки, використання та передачі персональних даних.

З моменту включення до Преамбули другої Гаазької конвенції 1899 р. про закони та звичаї сухопутної війни застереження Мартенса стало частиною права збройних конфліктів. Сенс застереження полягає в наступному: «Надалі до того часу, коли представиться можливість видати більш повне зведення законів війни, Високі Договірні Сторони вважають за доречне засвідчити, що у випадках, не передбачених прийнятими ними постановами, населення і воюючі залишаються під охороною та дією початків міжнародного права, оскільки вони впливають із законів людяності та вимог суспільної свідомості». Без врахування досвіду досконалого дослідження міжнародних стандартів щодо захисту персональних даних суб'єктами публічної адміністрації, базових принципів їх захисту, вивчення особливостей національних регулятивних підходів окремих держав, які мають розвинене законодавство і багаторічний досвід з питань захисту прав і свобод людини, у тому числі права на захист персональних даних, край ускладнюється розуміння сучасних проблем національного правового

регулювання відносин із захисту персональних даних в управлінських відносинах.

У сучасному інформатизованому світі персональні дані фізичних осіб набули особливо важливого значення, як самодостатня соціальна цінність та об'єкт правового регулювання. Ставлення до персональних даних на рівні правової політики та юридичної доктрини відзначається єдиними підходами для більшості країн світу. Інститут персональних даних – це відносно «молодий» за своїм історичним походженням. Його становлення та сучасне «піднесення» тісно пов'язано із розвитком конституційних прав і свобод людини й громадянина та, перш за все, із еволюцією права на недоторканість особистого життя. Інститут персональних даних відзначається своєю комплексністю, охоплюючи елементи властиві для предмету правового регулювання галузі конституційного, цивільного та адміністративного права.

Питання забезпечення захисту персональних даних громадян органами публічної влади останнє десятиліття носить актуальний характер та викликає гострі дискусії на науково-теоретичному та професійному рівнях. Водночас, війна викликана російською збройною агресією особливо загострила проблему забезпечення захисту державою, органами публічної влади основних прав та свобод громадян, в першу чергу права на життя. В умовах широкомасштабної військової агресії, на особливу увагу заслуговує питання забезпечення захисту персональних даних військовослужбовців, несанкціонований доступ до яких агресора може загрожувати їх життю.

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

Сутність персональних даних і окремі аспекти їх адміністративно-правового захисту досліджували такі вчені: Р.В. Ігонін, Р.А. Калюжний, А.В. Кучеренко, С.Й. Литвин, А.В. Пазюк, В.П. Радкевич, К.М. Рудой, В.О.

Серьогін, І.М. Солілко, В.І. Теремецький, А.М. Чвалюк, О.О. Шарібуріна, М.Я. Швець.

Проблемам особливостей відносин щодо сприяння забезпечення захисту персональних даних громадян суб'єктами публічної адміністрації сьогодні присвячено незначна кількість наукової публіцистики. Сутність персональних даних і окремі аспекти їх правового захисту досліджували такі вчені: Ю.Д. Белова, В.М. Брижко, А.М. Новицький, А.В. Пазюк, І.Я. Сенюта, О.М. Селезньова.

Водночас, підкреслимо, що значна кількість сучасних досліджень акцентує увагу на приватно-правових аспектах захисту прав персональних даних громадян, тобто, майже всі дослідження сконцентровані в площині цивільного права.

Загалом питання комплексного дослідження питання захисту персональних даних громадян під час воєнного стану є актуальним.

**Мета дослідження** – це комплексний загальнотеоретичний аналіз проблем забезпечення захисту персональних даних громадян органами публічної влади в умовах війни та способів їх вирішення.

Метою дослідження виступає зміст публічно-правової діяльності у сфері забезпечення захисту персональних даних громадян у період війни. Досягнення поставленої мети стає можливим завдяки виконання наступних завдань:

- визначити поняття персональних даних громадян та їх захисту;
- дослідити особливості режиму воєнного стану як особливого правового періоду;
- визначити нормативно-правові засади застосування державних інструментів захисту персональних даних громадян в умовах війни;
- окреслити суб'єктів державного управління у сфері захисту персональних даних;
- дослідити аспекти захисту персональних даних громадян в умовах війни у контексті державного управління;

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

*Об'єктом дослідження* є суспільні відносини, які виникають у сфері застосування публічних інструментів захисту персональних даних громадян в умовах війни.

*Предметом дослідження* є теоретико-методичні та практичні аспекти застосування публічних інструментів захисту персональних даних громадян в умовах війни.

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

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

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

**Структура та обсяг** зумовлені метою і завданнями здійсненого дослідження. Робота складається зі вступу, трьох розділів, шести підрозділів, висновків, списку використаних джерел (всього 89 найменувань). Загальний обсяг роботи становить 78 сторінок.

## **РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ЗАСТОСУВАННЯ ДЕРЖАВНИХ ІНСТРУМЕНТІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ГРОМАДЯН В УМОВАХ ВІЙНИ**

### **1.1 Поняття персональних даних та їх захисту**

Сучасний етап розвитку цивілізації відзначається всеохоплюючим запровадженням засобів інформатизації процесів державного управління через створення масштабних баз даних та широкого доступу органів влади до персональних даних громадян. Водночас, побудова демократичної соціальної правової держави, найвищою цінністю в якій є людина, її честь і гідність, недоторканність і безпека, як і підтримання ефективного функціонування державних інститутів перебувають у нерозривному зв'язку із необхідністю вдосконалення захисту основних прав людини та громадянина.

З розвитком інформаційних технологій, створенням баз даних виникла нова загроза цим правам – можливість легкого копіювання та об'єднання персональних даних. В останнє десятиліття багато картотек і баз даних державних та інших структур перетворені на електронну форму. З тих чи інших причин вони виявилися доступними третім особам і стали об'єктом купівлі-продажу. Остання обставина веде до неконтрольованого використання цієї інформації. Тим часом сам факт продажу баз даних або іншого поширення інформації, що міститься в них, становить підвищену суспільну небезпеку, оскільки відомості конфіденційного характеру можуть бути використані на шкоду конкретній особі (суб'єкту персональних даних).

Для захисту конституційних прав громадян від будь-яких посягань необхідна сувора правова регламентація обігу баз даних, що містять персональні дані, у тому числі встановлення юридичної відповідальності операторів цих баз за порушення правил збирання, зберігання та використання персональних даних. Це дозволить гарантувати ефективний правовий захист інтересів окремих

громадян та суспільства загалом. Всі ці та багато інших обставин актуалізують цю тему та зумовлюють необхідність її розробки у теоретико-правовому контексті.

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

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

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

Аналіз сучасної міжнародної практики, а також досвіду окремих країн у сфері правового забезпечення захисту персональних даних дозволяє констатувати наявність стійкої тенденції до розвитку універсалізму в цій галузі,

що виражається у формуванні загальних (наднаціональних) підходів до правового регулювання суспільних відносин, пов'язаних із захистом персональних даних, та міжнародних стандартів їхнього державно-правового захисту. Останні виступають правовим орієнтиром у розвитку законодавства, що встановлює правові механізми захисту персональних даних, та її правозастосовної практики.

У сучасних умовах склалися передумови для відокремлення у системі права щодо самостійного нормативного комплексу, в якому за предметною ознакою об'єднано різноманітні за своєю природою правові норми, що регулюють суспільні відносини, пов'язані із захистом персональних даних фізичних осіб.

У системі права його слід позиціонувати як комплексний правовий інститут – «інститут захисту персональних даних», в основу якого покладено норми міжнародного публічного та приватного права, а також конституційного, адміністративного, цивільного, кримінального, трудового, інформаційного та інших галузей національного права.

Комплексний характер даного інституту, а також предмета його регулювання не дозволяє погодитись з його характеристикою як багатогалузевого інституту, що входить до складу галузі інформаційного права. Специфіка суспільних відносин, що регулюються даним інститутом, а також галузева природа складових його юридичних норм зумовлюють міжгалузеве (комплексне) регулювання.

Поняття персональних даних пропонуємо визначати, як відомості або сукупність відомостей, що безпосередньо чи опосередковано стосуються фізичної особи, незалежно від її громадянства, постійного місця проживання чи іншого правового зв'язку з державою, яка є їх носієм, та дозволяють «прямо» або «опосередковано» її ідентифікувати за умови, що такі відомості було оброблено шляхом збирання, реєстрації, накопичення, зберігання, адаптування, зміни, поновлення, використання, поширення знеособлення, знищення, у тому числі – з використанням інформаційних (автоматизованих) систем.

Визнаючи високу динаміку розвитку даного інституту, його кількісних та якісних характеристик, доводиться констатувати, що на сучасному етапі він ще не набув ознак самостійної галузі права, тому твердження про галузеву самостійність даного нормативного комплексу, які у юридичній науці, видаються помилковими і позбавленими об'єктивних підстав.

Таблиця 1.1 Види персональних даних, пов'язаних з їх правовим режимом та обігом у мережі Інтернет

№	Види персональних даних	Характеристика	Особливості обробки
1	загальнодоступні персональні дані	відомості, до яких відносяться дані, що містяться у відкритих джерелах, таких як адресні книги та довідники (прізвище, ім'я, по батькові, місце та дата народження, інформація про освіту та підвищення кваліфікації, трудова діяльність), так і здатні ідентифікувати користувача в мережі Інтернет (мережевий псевдонім, ідентифікатор облікового запису користувача, електронна пошта)	Виняток загальнодоступних персональних даних із джерела, в яких вони містяться, відбувається на вимогу суб'єкта персональних даних;
2	особливі персональні дані	являють собою відомості, що містяться в закритих базах державних органів (серію та номер паспорта; відомості про військову службу та дані військового квитка, наявність посвідчення водія, страховий номер індивідуального особового рахунку, обов'язкового медичного страхування, індивідуального номера платника податків, інші ідентифікаційні дані, надані особі державними органами), номери мобільного телефону, кредитних карток та інші відомості, що містять персональні дані, включаючи особисті паролі та інші електронні ідентифікатори.	Обробка спеціальних персональних даних можлива при отриманні державних, муніципальних та інших послуг;
3	спеціальні персональні дані	інформація, до якої належать: національність, расова приналежність, ставлення до релігії, філософські переконання, політичні погляди, інтимне життя та стан здоров'я.	Обробка спеціальних персональних даних допускається у випадках і термінах, необхідні цієї обробки
4	біометричні персональні дані (важливі при питанні прижиттєвої та постсмертної ідентифікації)	відомості, необхідні ідентифікації суб'єкта, виходячи з його фізіологічних чи біологічних параметрів.	Обробка біометричних персональних даних можлива виключно за згодою суб'єкта даних

Примітка. Складено автором

Визначення поняття та видів персональних даних дозволяє охарактеризувати зміст заходів їх захисту.

Інститут захисту персональних даних є однією з юридичних гарантій конституційних прав людини на недоторканність приватного життя, особисту та сімейну таємницю, що кореспондують юридичні обов'язки інших суб'єктів на збереження цієї таємниці та забезпечення конфіденційності персональних даних. Саме ці конституційні права людини та сфера їх реалізації є системоутворюючими елементами цього нормативного комплексу. Зрозуміло, що певні правові режими, у тому числі і режим воєнного стану визначають певні особливості захисту прав громадян.

Під захистом персональних даних ми пропонуємо розуміти дії суб'єктів відповідних правовідносин, спрямовані на досягнення певного ступеня безпеки особистої інформації та персональних даних з метою:

- запобігання витоку, розкрадання, втрати, спотворення та підробки персональних даних;
- захисту від несанкціонованого доступу та дій щодо знищення, модифікації, спотворення, копіювання та блокування інформації, що стосується персональних даних, а також запобігання іншим формам незаконного втручання в інформаційні ресурси;
- захисту конституційних прав громадян на збереження особистої таємниці та конфіденційності персональних даних, що є в інформаційних системах;
- дотримання прав суб'єктів персональних даних при розробці, виробництві та застосуванні інформаційних систем, технологій та засобів їх забезпечення;
- запобігання завданню можливої шкоди суб'єкту персональних даних (завдання шкоди здоров'ю, незаплановані фінансові чи матеріальні витрати, втрата суб'єктом свободи дій внаслідок шантажу чи погроз, що здійснюються з використанням персональних даних, порушення конституційних прав суб'єкта внаслідок втручання у його особисте життя шляхом здійснення контактів із ним з різних приводів без його згоди).

Зміст права на захист персональних даних становлять дії, що обмежують можливість третіх осіб вчиняти будь-які дії з персональними даними особи без її згоди, а також правомочності суб'єктів персональних даних контролювати дії операторів, які опрацьовують ці дані.

Власне правове регулювання захисту персональних даних має ґрунтуватися на таких принципах, як:

- конфіденційність отримуваних персональних даних та обмеження доступу до них інших осіб;
- достовірність та повнота персональної інформації;
- цільовий характер персональної інформації, її обробки та зберігання;
- законність цілей та способів збирання та обробки персональної інформації;
- сумлінність оператора;
- вільний доступ особи до своїх персональних даних, право на повну інформацію про них;
- неприпустимість об'єднання баз персональних даних, створених для несумісних між собою цілей;
- неприпустимість створення інформаційних ресурсів персонального характеру, закритих чи обмежених у доступі для суб'єкта персональних даних, крім випадків, передбачених законом;
- гарантованість державою суб'єктивних прав особи, пов'язаних із захистом її персональних даних.

Підсумовуючи можемо запропонувати таке визначення поняття «персональні дані», що враховує критерії «ідентифікованості суб'єкта даних» та «чутливості»: *персональні дані* - це дані в машинно-орієнтованій формі, що містять інформацію про приватне життя живого індивіда (суб'єкта даних), який може бути ідентифікований на підставі цієї інформації (або за допомогою цієї та іншої інформації), якщо, з точки зору будь-якої нормальної людини, наділеної звичайною чутливістю, суб'єкт даних має право вважати таку інформацію конфіденційною та контролювати її поширення.

## 1.2 Режим воєнного стану як особливий правовий період

З метою забезпечення безпеки держави діяльність державних органів, котрий іноді всього держави, то, можливо пов'язані з використанням і забезпеченням конкретних правових режимів, тобто. жорстких установлень з боку державної влади (комендантська година, обмеження пересування тощо), з дотриманням Конституції, внутрішнього законодавства, норм міжнародного права та міжнародних зобов'язань. Загалом адміністративно-правовий режим є встановлена в законодавчому порядку сукупність правил діяльності державних установ, дій та поведінки громадян та юридичних осіб, а також порядок реалізації ними своїх прав у певних умовах забезпечення та підтримки суверенітету та оборони держави, інтересів безпеки та охорони громадського порядку, спеціально створеними з цією метою службами виконавчої. Стосовно об'єкта і предмета дослідження найбільший інтерес становлять режими, які можна використовувати під час збройного конфлікту міжнародного і неміжнародного характеру. Йдеться про режим *військового, надзвичайного стану, стану війни та режим антитерористичної операції* та їх вплив на можливість обмеження та встановлення додаткових вимог щодо здійснення прав пов'язаних зі свободою доступу до інформації, що демонструє зміст Таблиці 1.2

Таблиця 1.2 Особливі правові режими та їх зміст

№	Назви правових режимів	Можливості обмеження та встановлення додаткових вимог щодо здійснення прав пов'язаних зі свободою доступу до інформації
1	Воєнний стан (категорія національного законодавства)	підлягають обмеженню
2	Стан війни (міжнародно-правова категорія)	підлягають обмеженню
3	Надзвичайний стан (категорія національного законодавства)	підлягають обмеженню за певних умов
4	АТО (антитерористична операція)	підлягають обмеженню за певних умов

Примітка. Складено автором

Загальною метою і головним призначенням адміністративно-правових режимів є створення правових і організаційних бар'єрів, які б їх ускладнювали, а в ряді випадків і зовсім виключали досягнення злочинних цілей у сфері безпеки.

Характерною ознакою встановлення подібних заходів є вимушена (через вищі інтереси забезпечення безпеки особистості та держави) детальна регламентація діяльності державних органів та громадських організацій, поведінки громадян, запровадження деяких додаткових правил або вилучення із загальноприйнятих норм, встановлення особливого контролю за належним порядком розвитку правовідносин у охоронюваній сфері.

Водночас правові режими мають служити не лише справі безпеки держави, а й відповідати інтересам суспільства, відображати сучасні суспільні інтереси та міжнародні зобов'язання держави.

До цих правових режимів застосовуються загальні основні вимоги:

- 1) відкритість всього комплексу законодавчих та підзаконних актів, що стосуються правового становища суб'єктів режиму та правовідносин між ними;
- 2) зміст режимних законодавчих актів, що регулюють застосування режимів, має максимально вичерпувати все коло питань, що стосуються реалізації режиму;
- 3) переліки підстав, що містяться в законодавчих актах, для можливого застосування в ході реалізації режиму примусових заходів повинні бути вичерпними і виключати розширювального тлумачення;
- 4) будь-які можливі умови та необхідність обмеження прав і свобод громадян повинні бути передбачені законодавчими актами, відповідати нормам міжнародного права, ґрунтуватися на принципі розумності та застосовуватися відповідно до ситуації, що складається.

24 лютого 2022 року Указом Президента України № 64/2022 було введено військовий стан у відповідь на повномасштабне вторгнення Російської Федерації на територію України. Указ Президента України від 24 лютого 2022 року №64/2022 «Про введення воєнного стану в Україні» [47] передбачає, що у зв'язку із введенням в Україні воєнного стану тимчасово, на період дії правового режиму

воєнного стану, можуть обмежуватися конституційні права і свободи людини і громадянина, передбачені статтями 30 – 34, 38, 39, 41 – 44, 53 Конституції України, тобто : недоторканість житла, таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції, свобода пересування та свободу думки і слова, на вільне вираження своїх поглядів і переконань, а також вводиться тимчасові обмеження прав і законних інтересів юридичних осіб в межах та обсязі, що необхідні для забезпечення можливості запровадження та здійснення заходів правового режиму воєнного стану, які передбачені частиною першою статті 8 Закону України «Про правовий режим воєнного стану» [47].

Серед згаданих конституційних прав і свобод людини і громадянина передбачено можливість обмеження права на особисте і сімейне життя та встановлення особливого режиму збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди (ч.1 та 2 ст. 32 Конституції України) [34]. Зазначені обмеження, серед іншого, можуть бути обумовлені лише в інтересах національної безпеки.

Необхідно пам'ятати, що в умовах широкомасштабної військової агресії, наявності декількох театрів бойових дій на території України, необхідно одночасно вести мову не лише про встановлення законних обмежень окремих прав і свобод людини і громадянина але й про напрацювання нових правових механізмів їх захисту через діяльність органів публічної влади та окремих інститутів громадянського суспільства. Зазначені положення прямим чином вплинули на забезпечення прав моряків та морської безпеки, зокрема. Не останнім чином це стосується питання виїзду моряків торговельного флоту за кордон та виконання ними свої з зобов'язань за укладеними договорами. Постановою КМУ від 2 вересня 2022 р. № 992 вніс зміни до «Правил перетинання державного кордону громадянами України». Згідно з пунктом 2-12, що доповнив ці Правила, «у разі введення на території України воєнного стану громадяни України чоловічої статі віком від 18 до 60 років мають право перетинати державний кордон України, якщо вони прямують для роботи на

морських суднах, суднах внутрішнього плавання у складі екіпажів таких суден або для проходження практичної підготовки на суднах».

Водночас, широке залучення членів екіпажів до виконання свої обов'язків, у тому числі і у територіальних водах України вимагають аналізу того яким чином норми гуманітарного права захищають моряків та чи перебувають ці гарантії у залежності від нормативно-правового тлумачення категорій «*воєнний стан*» та «*стан війни*», що вживаються у законодавстві.

Ми вважаємо, що правовий режим воєнного стану за національним законодавством є більш регламентованим ніж стан війни. Водночас, системний аналіз положень національного законодавства України дає підстави для висновку про те, що не існує принципової відмінності між введенням правового режиму воєнного стану та оголошення стану війни у юридичних наслідках для публічних правовідносин.

Більше того, буквальний аналіз частини першої статті 4 Закону України «Про оборону України» дає підстави для висновку про те, що введення правового режиму воєнного стану є однією з передумов для оголошення стану війни: «У разі збройної агресії проти України або загрози нападу на Україну Президент України приймає рішення про загальну або часткову мобілізацію, *введення воєнного стану* в Україні або окремих її місцевостях, застосування Збройних Сил України, інших військових формувань, утворених відповідно до законів України, подає його Верховній Раді України на схвалення чи затвердження, а також вносить до Верховної Ради України подання про оголошення стану війни» [47].

При цьому, з огляду на положення частини другої статті 4 Закону України «Про оборону України», вжиття заходів для відсічі агресії не перебуває у прямій залежності від оголошення стану війни та/або введення правового режиму воєнного стану: «Органи державної влади та органи військового управління, не чекаючи оголошення стану війни, вживають заходів для відсічі агресії. На підставі відповідного рішення Президента України Збройні Сили України разом з іншими військовими формуваннями розпочинають воєнні дії, у тому числі

проведення спеціальних операцій (розвідувальних, інформаційно-психологічних тощо) у кіберпросторі.».

Водночас, щодо застосування норм міжнародного гуманітарного права, підкреслимо, що:

- системний аналіз положень Женевських конвенцій (Конвенція про поліпшення долі поранених та хворих в регулярних арміях; Конвенція про поліпшення долі поранених, хворих і осіб, потерпілих корабельну аварію, зі складу озброєних сил на морі; Конвенція про поводження з військовополоненими; Конвенція про захист цивільного населення під час війни) дає підстави для висновку про те, що *застосування останніх не пов'язується виключно з оголошенням стану війни*. Натомість, у вказаних конвенціях міститься норма, яка закріплює таке: «...ця Конвенція *застосовується до всіх випадків оголошеної війни чи будь-якого іншого збройного конфлікту*, що може виникнути між двома чи більше Високими Договірними Сторонами, *навіть якщо одна з них не визнає стану війни*.»;

- аналогічно Конвенція про закони і звичаї суходільної війни не встановлює обмежень у дії її норм виключно після оголошення стану війни;

- стаття 39 Статуту ООН також закріплює, що Рада Безпеки визначає існування *будь-якої загрози миру та безпеці, будь-якого порушення миру чи акту агресії* та надає рекомендації або вирішує про те, які заходи слід вжити відповідно до статей 41 і 42 для підтримки або відновлення міжнародного миру та безпеки.

Отже, *застосування норм міжнародного гуманітарного права не перебуває у залежності від оголошення стану війни та/або введення воєнного стану, що впливає і на питаннях захисту персональних даних громадян під час війни*.

Щодо власне, наслідків введення правового режиму воєнного стану та/або оголошення стану війни для приватних правовідносин:

- відповідно до частини першої статті 617 Цивільного кодексу України особа, яка порушила зобов'язання, звільняється від відповідальності за

порушення зобов'язання, якщо вона доведе, що це порушення сталося внаслідок випадку або непереборної сили. Так, цивільно-правові договори, які укладають у межах приватних правовідносин на території України, як правило, у частині форс мажору містять вказівку, як на збройні конфлікти, введення воєнного стану, так і на оголошення стану війни. Більш того, Торгово-промислова палата України листом №2024/02.0-7.1 від 28 лютого 2022 року засвідчила, що військова агресія Російської Федерації проти України з 24 лютого 2022 року до офіційного закінчення цих подій є форс мажорною обставиною (обставиною непереборної сили).

Отже, проведений системний аналіз норм національного законодавства та міжнародного гуманітарного права дає підстави для висновку про те, що сфера дії останніх не перебуває у прямій залежності саме від факту оголошення стану війни на території України.

## РОЗДІЛ 2. АНАЛІЗ ДЕРЖАВНИХ ІНСТРУМЕНТІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ГРОМАДЯН В УМОВАХ ВІЙНИ

### 2.1 Нормативно-правові засади застосування державних інструментів захисту персональних даних громадян

Пізніше питання піднесення важливості «людиноцентризму» у питаннях правового регулювання ми бачимо у період після завершення Другої Світової війни. Належна увага до прав людини на той час пояснюється, перш за все, руйнівними наслідками Другої Світової війни. Це знайшло своє відображення й у визначенні права на особисте життя. Головним пріоритетом того часу були найбільш значимі соціальні питання повоєнного періоду: недоторканість особистого і сімейного життя, таємниця листування. Водночас, на власне проблему захисту персональних даних, котра, здавалося б, є логічним продовженням права на особисте життя, не звертали належної уваги.

Формування загального поняття сфери приватного життя, яка визначається як сферу приватних відносин індивіда, в якій він вільний від втручання з боку держави, суспільства, інших індивідів, відбувається в контексті загального процесу виникнення та розвитку прав людини, ідеї правової держави та громадянського суспільства.

Поняття сфери приватного життя не є універсальним для різних країн і залежить від рівня розвитку суспільства, належності до певної цивілізації, особливостей історичного та культурного розвитку нації.

Поняття права на недоторканність приватного життя стосовно його місця у сучасній системі прав людини. Це право, що відноситься до основних прав людини і, в силу свого комплексного характеру, що охоплює всі цивільні (особисті) права людини, що визначають зміст сфери приватного життя, недоторканність, охорону та захист цієї сфери, а також соціальні, економічні та культурні права людини, що впливають на якість приватного життя.

Виходячи з того, що право на недоторканність приватного життя не є абсолютним, пропонується сформулювати принцип дуалізму цілей правового регулювання сфери приватного життя, який у загальному вигляді може бути представлений таким чином: метою правового регулювання сфери приватного життя є не абсолютний захист права індивіда на недоторканність його приватного життя, а підтримання оптимального для умов балансу інтересів індивіда і суспільства.

Домінуюча у світі концепція правової захищеності сфери приватного життя - "прайвеси" - виникла в рамках європейської цивілізації як територіально-просторова концепція. Витоком її є західна культурно-історична традиція, яка розглядає наявність фізичного анклаву, що належить індивіду або займаного ним, як неодмінна умова приватності сфери приватного життя, оскільки в цьому фізичному анклаві матеріалізується "персональний життєвий простір" індивіда. Відображенням територіально-просторового характеру концепції "прайвеси" служить превалююча у роки її існування формулювання права недоторканність приватного життя як права індивіда те що, "залишатися наодинці із собою" (to be let alone).

В ході подальшого розвитку концепція прайвеси трансформується з територіально-просторової в інформаційно-просторову. Превалюючим формулюванням права на недоторканність приватного життя в рамках цієї концепції стає право індивіда на те, щоб "контролювати циркуляцію відомостей про себе (тобто персональної інформації)".

На початку другої половини ХХ ст. починають розвиватися інформаційні технології, котрі дозволяли значно швидше опрацьовувати більшу кількість інформації. У 60-ті роки ці технології стають усе більш доступними, що викликало певне занепокоєння Ради Європи [79].

Пропонується концепція техногенної еволюції інституту Прайвеси. Згідно з цією концепцією, рушійним фактором еволюції інституту є розвиток інформаційних технологій у ході НТР. Виділяються три чітко виражених етапи еволюції "прайвеси", коли виникають нові форми інституту, характеризовані

взаємопов'язаною сукупністю нових видів посягань на право недоторканності приватного життя, нових принципів і засобів правового захисту сфери приватного життя. Ці етапи збігаються за часом з періодами домінування певних засобів збору, обробки та розповсюдження в суспільстві персональної інформації (далі для стислості - "основних носіїв інформації").

Як "основні носії інформації" послідовно виступають:

- 1) засоби інформації;
- 2) комп'ютери;
- 3) комп'ютерно-телекомунікаційні мережі.

Періоди їх домінування відповідно до періодизації еволюції інформаційного суспільства, запропонованої японським ученим Масао Хорібе, розглядаються як фази індустріального інформаційного суспільства і відповідно мають назви:

- 1) "мас-медійне інформаційне суспільство" (mass media information society);
- 2) "комп'ютерне інформаційне суспільство" (computer information society);
- 3) "мережеве інформаційне суспільство" (network information society)<sup>1</sup>;

Кожній фазі супроводжує виникнення відповідної форми інституту прайвесі:

- 1) "мас-медійного прайвесі";
- 2) "комп'ютерного прайвесі";
- 3) "мережевого прайвесі".

Запропонована концепція відображає еволюцію інституту прайвесі і дозволяє прогнозувати його подальший розвиток при переході до постіндустріального інформаційного суспільства.

Головним піонером у сфері Data Privacy стала саме Німеччина: перший національний закон про персональні дані (Bundesdatenschutzgesetz) з'являється у 1977 році у ФРН [83].

У 1974 році газета Le Monde публікує про це статтю із назвою «SAFARI ou la chasse aux Français» (САФАРИ або полювання на французів) та провокує

гучний скандал на тему масового стеження. Під тиском громадськості уряд був вимушений відступити, що привело до прийняття вище згаданого закону і створенню Комісії з інформатики та громадянських свобод. [73].

У 1981 році укладено перший міжнародний договір у сфері Data Privacy. Ним стає Конвенція про захист фізичних осіб при автоматизованій обробці персональних даних. Ця Конвенція стала найбільшим досягненням у відповідній сфері після прийняття Конвенції про захист прав людини і основоположних свобод від 04.11.1950 [33].

Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 [32], пізніше стане базою 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», яка була прийнята 24 жовтня 1995 р. [54], яка у наш час буде замінена Регламентом (Євросоюзу) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 р. про захист фізичних осіб щодо обробки персональних даних та про вільне переміщення таких даних [85].

Принципи, закладені у Європейській конвенції про захист прав і основних свобод, набули розвитку в спеціальних нормах Конвенції Ради Європи про захист прав фізичних осіб щодо автоматичної обробки персональних даних 1981 року. У цій Конвенції захист даних розглядається як захист основних прав і свобод індивідів, зокрема, їх права на недоторканість особистого життя щодо обробки персональних даних. Необхідність її прийняття пояснюється суперечністю, що виникла наприкінці 1970-х років між все більш активним впровадженням засобів автоматизованої обробки даних та їх поширенням у телекомунікаційних мережах, зловживання при використанні персональних даних, потреба у впорядкуванні експортно-імпортних операцій [6].

Україна ратифікувала цю Конвенцію лише 6 липня 2010 р. [59]. Значення цієї конвенції для уніфікації правового регулювання відносин з приводу персональних даних можна розкрити за допомогою наступних тезисів.

Саме у цей період в Україні починає на політичному рівні формуватися новітня національно орієнтована доктрина, прикладом якої можна згадати «Концепцію державотворення в Україні», яка була затверджена IV Всеукраїнськими зборами Народного Руху України 4-6 грудня 1992 року. У ній серед іншого йшлося про таке: «Рух прагне досягти такого співвідношення у стосунках між людиною, державою, суспільством і нацією, коли принцип визнання природних прав людини буде покладено в основу всього процесу державотворення в Україні. Дотепер найбільше гарантій прав мала держава, найменше – людина. Необхідно ж забезпечити гарантії для реалізації природних прав людини» [41].

Зазначені ідеологічні орієнтири в кінцевому рахунку втілюються у змісті Конституції України, яка у ст.29 визначає, що кожна людина має право на свободу та особисту недоторканність: ніхто не може бути заарештований або утримуватись під вартою інакше, як за вмотивованим рішенням суду і тільки на підставах і в порядку, встановленому законом [34]. Водночас, нормативне регламентування у сфері захисту персональних даних та наявність аспектів пов'язаних з війною можна акумулювати, що відображено у таблиці 2.1.

Таблиця 2.1 Нормативне регламентування у сфері захисту персональних даних та наявність аспектів пов'язаних з війною

Назва законодавчого акту	Характеристика правового регулювання	Наявність аспектів пов'язаних з війною
1	2	3
Конституція України	Встановлено заборону збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в окремих випадках	Не передбачено
«Про захист персональних даних» Закон України від 01 червня 2010 року	Загальне регулювання відносин у сфері персональних даних.	Не передбачено
Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних, підписана в Страсбурзі 28 січня 1981 року	Регламентування діяльності з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів	Не передбачено

Продовж.табл.2.1

1	2	3
Наказ Уповноваженого Верховної Ради України з прав людини №1/02-14 від 08 січня 2014 року “Про затвердження документів у сфері захисту персональних даних”	Порядком обробки персональних даних (далі - Порядок).	Не передбачено
Цивільний кодекс України	У частині відшкодування завданої шкоди (деліктні відносини)	Не передбачено

Примітка. Складено автором.

*Таким чином, діючі нормативно-правові акти у сфері захисту персональних даних не передбачають жодним чином особливостей правового регулювання питання захисту персональних даних громадян у період війни.*

Наближення українського законодавства до європейських стандартів, що визначають права фізичної особи при обробці персональних даних, обумовило прийняття Закону України «Про захист персональних даних» [53].

Так, 1 червня 2010 року Верховна Рада України прийняла Закон України «Про захист персональних даних» № 2273-VI. Таким чином, Україна зробила надзвичайно важливий крок на шляху правового регулювання обробки персональних даних. Закон України «Про захист персональних даних», який по факту є національною імплементацією стандартів Директиви 95/46/ЄС, а тому при тлумаченні його норм варто використовувати також і зміст відповідних норм Директиви.

Іншим важливим у контексті нормативно-правового регулювання виступає Закон України «Про інформацію» . Термін «персональні дані» представлений у цьому акті, як «інформації про фізичну особу» (ст. 11 Закону України «Про інформацію» [56]. В Україні також запроваджено електронну систему охорони здоров'я (ст. 11 Закону України «Про державні фінансові гарантії медичного обслуговування населення» [48]) – інформаційно-телекомунікаційну систему, що забезпечує автоматизацію ведення обліку медичних послуг. Функціонування

електронної системи охорони здоров'я повинно здійснюватися з урахуванням вимог законодавства про захист персональних даних [66].

Специфіка захисту персональних даних в трудових правовідносинах обумовлена насамперед ціллю їх обробки і регламентується Кодексом законів про працю України [30]. Тобто, роботодавець має законні підстави для обробки персональних даних працівника, але лише в межах, які необхідні при прийнятті його на роботу та подальшим виконанням ним трудової функції (ч. 2 ст. 24 Кодексу законів про працю України [30]).

Окремі норми Цивільного кодексу України також присвячені праву на особисте життя та його таємницю. З ними органічно пов'язані інші суб'єктивні немайнові права, які на практиці виступають правовими гарантіями забезпечення таємниці особистого життя. До числа таких відносимо: *право на інформацію* (ст. 302 ЦК України), *право на особисті папери* (ст. 303 ЦК України), *право на таємницю кореспонденції* (ст. 306 ЦК України) та *право на недоторканність житла* (ст. 311 ЦК України) [72].

Водночас, розвиток інформаційних технологій, що постійно пришвидшується, створює нові проблеми в сфері приватності та особистого життя. Головною такою проблемою стала поява Інтернету та його швидкий розвиток. Першим потенційну загрозу помічає Європейський Союз, який формує нормативну базу задля того аби адаптувати до нових загроз та уніфікувати законодавство про персональні дані країн-членів ЄС. Для цього були удосконалені механізми, передбачені міжнародною Конвенцією 1981 року, а також упровадженні нові зобов'язання для операторів персональних даних і нові права для громадян ЄС.

На питання необхідності «перенацілення» інструментів правового регулювання у сферу інтернет-середовища наголошують і вітчизняні науковці [16], а діючий Кодекс України про адміністративні правопорушення вже містить відповідні правові приписи. Так, у Кодексі України про адміністративні правопорушення, а саме у ст. 164-17, ст. 164-18 законодавець прописує відповідальність за порушення умов і за наведення завідомо недостовірної

інформації, що визначають порядок припинення порушень авторського права і (або) суміжних прав з використанням мережі Інтернет [31].

Таким чином, GDPR та інші закони у сфері приватності даних не є новелою європейського законодавства. Регламент щодо захисту персональних даних разом із усім пакетом реформ Privacy є результатом більш, ніж вікового розвитку юридичної думки, що ґрунтується на необхідності захисту особистого життя будь-якого громадянина. Відповідно у національному контексті розбудови системи захисту персональних даних провідне значення мають відігравати нормативно-правові акти спрямовані на задоволення публічно-правових вимог щодо створення системи захисту персональних даних, їх баз у різних інформаційних сферах та «середовищах». Особливої актуальності це набуває у контексті виняткової активності Міністерства цифрової політики України у запровадження застосунку «Дія».

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

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

даних дозволяє виділити такі заходи державного захисту права на недоторканність приватного життя в умовах автоматизованої обробки персональних даних та відповідні процедури їх застосування: - облік операторів обробки персональних даних у державному реєстрі; контроль за виконанням вимог безпеки при обробці персональних даних в автоматизованих інформаційних системах; ліцензування та контроль за дотриманням ліцензіатами відповідних вимог та умов при здійсненні діяльності з технічного захисту персональних даних як виду інформації обмеженого поширення; призупинення дії або анулювання ліцензії організації-оператора обробки, яка порушила конфіденційність персональних даних, якщо умовою ліцензії є заборона на передачу персональних даних третім особам без згоди у письмовій формі суб'єкта персональних даних; адміністративне зупинення чи припинення обробки персональних даних, що здійснюється з порушенням вимог законодавства; притягнення осіб, винних у порушенні законодавства у сфері захисту персональних даних, до цивільної, адміністративної, кримінальної відповідальності; опублікування звітів про стан захисту персональних даних у засобах масової інформації.

## **2.2 Суб'єкти відносин щодо застосування державних інструментів захисту персональних даних громадян під час війни**

Враховуючи особливий характер персональних даних, виділимо таких суб'єктів інформаційних відносин для використання у сфері регулювання збору, обробки, використання та передачі персональних даних як: суб'єкт персональних даних - фізична особа, що ідентифікується на підставі цих даних (або за допомогою цих даних та іншої) інформації, яка знаходиться у розпорядженні користувача даних), для якого згадані дані можуть, з точки зору людини середньої чутливості (або за прямою вказівкою закону), обґрунтовано вважатися інтимними та конфіденційними.

*Утримувач персональних даних* (контролер або розпорядник файлів) - фізична або юридична особа, яка має право приймати будь-які (в рамках закону) рішення щодо обробки, використання та передачі комп'ютеризованого або заснованого на іншій технології збору персональних даних як: 1) зареєстрованого та ліцензованого власника чи власника відповідних інформаційних ресурсів; 2) особи, спеціально уповноваженої компетентними державними органами.

*Користувач персональних даних* - фізична або юридична особа, яка за встановленими законом правилами використовує зібрані та оброблені персональні дані, для яких вона не є "власником даних" ("контролером файлів").

*Оброблювач персональних даних* - фізична або юридична особа, яка має комп'ютерні або інші потужності, ліцензовані для необхідної обробки персональних даних, та здійснює автоматизовану або ручну обробку даних, для яких вона не є "власником даних" ("контролером файлів"), і які вони отримують від комерційного замовника чи іншої особи, яка має права "власника" цих даних.

*Збирач персональних даних* - фізична або юридична особа, яка здійснює первинний збір персональних даних відповідно до власних законних повноважень або за дорученням особи, яка має такі повноваження.

В умовах ведення війни, на зазначену вище характеристику суб'єктів у сфері персональних даних впливатиме їх статус як учасників бойових дій або навпаки «некомбатантів», що визначено у міжнародному гуманітарному праві.

Захист жертв війни право збройних конфліктів приділяє особливу увагу. Відповідно до Женевських конвенцій 1949 р. до поранених і хворих та осіб, які зазнали аварії корабля, залежно від їх правового статусу (військовослужбовці або цивільні особи) застосовуються режими захисту та надання допомоги. Женевські документи закріплюють, що терміни «хворий» та «поранений» застосовуються незалежно від того, чи є громадянин військовослужбовцем чи цивільною особою. Конвенції встановлюють, що всі поранені та хворі незалежно від кольору шкіри, релігії, національного та соціального походження, політичних та інших переконань користуються однаковим заступництвом.

Сучасне міжнародне право містить вимоги, якими воюючі зобов'язані керуватися по відношенню до цивільного населення:

- а) воюючим заборонено нападати на громадянське населення;
- б) у будь-який час та за будь-яких умов воюючим необхідно проводити різницю між комбатантами та цивільним населенням.

Міжнародне право передбачає надання цивільному населенню різних рівнів захисту та надання певних режимів забезпечення безпеки. Право збройних конфліктів забезпечує як загальний, і спеціальний правовий захист від наслідків військових дій. Загальний захист надається всьому цивільному населенню незалежно від віку, політичних поглядів, релігійних переконань, віку, расової належності тощо.

Надання спеціального захисту пов'язане з підвищеною вразливістю певних категорій покровительствуючих (діти, жінки) в умовах збройних конфліктів або пояснюється їх особливою роллю у наданні допомоги цивільному населенню та забезпеченні його виживання під час бойових дій (персонал медичних формувань). У ході збройного конфлікту воюючі держави можуть проводити військові дії в певних просторових межах сухопутної, морської та повітряної території. У праві збройних конфліктів розрізняють поняття «театр війни» і «театр військових дій». Театр війни – це сухопутна, морська, повітряна територія воюючих сторін, а також відкрите море та повітряний простір над ним, на яких вони потенційно можуть вести військові дії. Театр військових дій - це територія, де воюючі сторони ведуть військові дії.

Джерела права збройних конфліктів закріплюють, що до комбатантам ставляться: по-перше, особовий склад збройних сил, що у конфлікті; по-друге, особовий склад ополчення та добровольчих загонів, що входять до складу збройних сил; по-третє, особовий склад організованих рухів опору; по-четверте, населення неокупованої території, яке береться за зброю для боротьби з військами, що вторгаються, не встигнувши сформуватися в регулярні війська; по-п'яте, військові розвідники, за дотримання певних умов.

Відповідно до положень Протоколу I збройні сили сторони, що перебувають у конфлікті, складаються з організованих збройних сил, груп та підрозділів, що знаходяться під командуванням особи, яка є відповідальною за своїх підлеглих. Віднесення до комбатантів особового складу регулярних збройних сил не залежить від факту визнання іншою воюючою стороною влади, у підпорядкуванні якої знаходяться збройні сили. Право бути комбатантами та обов'язок визнавати такий статус впливає із міжнародно-правових правил, а не з внутрішньодержавних установлень.

Можемо зробити висновок про те, що комбатанти безпосередньо ведуть бойові дії проти ворога зі зброєю в руках, і тільки до них застосовується військове насильство аж до фізичного знищення. Потрапивши до рук ворога, вони стають військовополоненими. Добровольці вважаються комбатантами, ними поширюється режим військового полону. Добровольці є військовослужбовцями, вони включені до особового складу армії конкретної держави, перебувають під її захистом та виконують накази та розпорядження військовонаачальників.

Військовополонені – це громадяни конкретної суверенної держави (а також добровольці, які є громадянами іноземної держави), на яких поширюються міжнародно-правові норми щодо захисту прав і свобод людини в період збройного конфлікту. Військовий полон можливий лише у період збройного конфлікту міжнародного характеру. У період ВКНМХ стан військового полону існувати не може. Крім того, ВКНМХ відрізняється від міжнародного збройного конфлікту ще низкою суттєвих особливостей: а) ВКНМХ відбувається в межах території однієї суверенної держави як суб'єкта міжнародного права і не виходить за межі її кордонів; б) конфлікт має внутрішній характер; в) визначається наявністю постійних та організованих дій між протилежними силами. Зазначене дозволяють провести різницю між військовополоненими та інтернованими, тобто. громадянами іноземної держави, які опинилися на території супротивника у період збройного конфлікту з різних підстав: постійне

чи тимчасове проживання, навчання, стажування, участь у роботі наукової конференції тощо.

Держава, з конкретної обстановки, реальних і потенційних загроз безпеці держави може ухвалити рішення про інтернування громадян ворожої держави, тобто. запровадити тимчасове обмеження їх права і свободи, наприклад, обмежити пересування, встановити місця проживання, тимчасово вилучити радіопередавальні устрою тощо. Тільки держава в особі вищих державних органів дає оцінку загрозам безпеці та приймає рішення про конкретні заходи щодо їх локалізації, у тому числі й інтернуванню іноземних громадян.

Законний учасник збройних конфліктів - це особа, що входить до складу збройних сил сторони, яка перебуває в конфлікті, має право брати безпосередню участь у військових діях (комбатант), а також особа зі складу збройних сил воюючої сторони, яка не має права безпосередньо брати участь у військових діях (некомбатант).

Як критерій для розмежування понять «комбатант» і «некомбатант» пропонуємо розглядати ознаку, закріплену п. 2 ст. 43 Додаткового протоколу I 1977 р. — право брати безпосередню участь у військових діях, а не причетність до процесу ведення збройної боротьби.

Особи, які підпадають під визначення «комбатант» (ст. 43 Додаткового протоколу I), мають таке право. Виняток із поняття «комбатант» зроблено ст. 43 для медичного та духовного персоналу, які таким чином не мають права брати безпосередню участь у військових діях.

Поняття «некомбатант» у міжнародному гуманітарному праві нормативно не закріплено. З цієї причини немає однозначного розуміння цього терміна в доктрині міжнародного правничий та міжнародної судової практики. Крім того, відсутність нормативного визначення «некомбатант» перешкоджає формуванню універсальної класифікації комбатантів та некомбатантів. На нашу думку, до некомбатантів належать тільки медичний персонал і духовенство, що належать до збройних сил сторін, які перебувають у конфлікті. Решта категорій осіб,

перелічені в Женевських конвенціях про захист жертв війни 1949 р., ставляться до комбатантам.

Законний учасник збройних конфліктів - це особа, що входить до складу збройних сил сторони, яка перебуває в конфлікті, має право брати безпосередню участь у військових діях (комбатант), а також особа зі складу збройних сил воюючої сторони, яка не має права безпосередньо брати участь у військових діях (некомбатант).

Як критерій для розмежування понять «комбатант» і «некомбатант» пропонується розглядати ознаку, закріплену п. 2 ст. 43 Додаткового протоколу I 1977 р. — право брати безпосередню участь у військових діях, а не причетність до процесу ведення збройної боротьби.

Особи, які підпадають під визначення «комбатант» (ст. 43 Додаткового протоколу I), мають таке право. Виняток із поняття «комбатант» зроблено ст. 43 для медичного та духовного персоналу, які таким чином не мають права брати безпосередню участь у військових діях.

Проблема встановлення статусу «військових радників та інструкторів» — категорії осіб, правове становище яких викликає суперечки в доктрині міжнародного права, заслуговує, на наш погляд, на пильну увагу з боку вчених і практиків, які займаються проблемами міжнародного гуманітарного права. Враховуючи характер діяльності таких осіб, а також відсутність нормативного визначення «некомбатант», можна дійти висновку про необхідність віднесення військових радників та інструкторів до іноземців, які перебувають у період конфлікту на території однієї з воюючих сторін. Інакше кажучи, такі особи є законними учасниками збройних конфліктів.

Основні обов'язки комбатантів полягають у наступному: а) робити все можливе для того, щоб відрізнити себе від цивільного населення; б) дотримуватись при проведенні військових операцій балансу між вимогами гуманності та військової необхідності, тобто комбатант зобов'язаний не виходити за рамки таких дій, які є дійсно необхідними для виконання бойового завдання та не тягнуть за собою непотрібних втрат і страждань.

Визначальним моментом правового статусу комбатантів є те, що лише такі особи у період збройного конфлікту мають право застосовувати так зване «дозволене насильство». І у разі взяття в полон комбатант не переслідватиметься за це «дозволене насильство». Він отримує статус військовополоненого і утримуватиметься в таборі військовополонених.

На відміну від комбатантів, некомбатанти не можуть бути захоплені в полон ворогом, а можуть лише затримані ним. У цьому вони вважаються військовополоненими, але утримуються противником надання медичної та духовної допомоги військовополоненим.

Таким чином ми можемо систематизувати суб'єктів, що потребують захисту їх персональних даних (таблиця 2.2) В першу чергу мова йде про представників силових (мілітаризованих) структур (Збройних Сил України, Національної гвардії України, Служби Безпеки України, Національної поліції, Державної прикордонної служби України та інші).

Таблиця 2.2 Суб'єкти, що потребують захисту їх персональних даних в період війни

Суб'єкти, що потребують захисту їх персональних даних		
Жертви війни		Військовослужбовці (комбатанти)
Цивільні особи (некомбатанти)	Примусово переміщені особи	- представників силових (мілітаризованих) структур, які перебувають на дійсній службі;
		- представників силових (мілітаризованих) структур, що знаходяться безпосередньо в зоні ведення бойових дій;
		- особи, що перебувають на лікуванні у медичних закладах України та зарубіжних країн;
		- особи, що перебувають у полоні;
		- особи, що вважаються безвісно зниклими або загиблими.

Примітка: Розроблено автором.

У частині цивільного населення на особливу увагу заслуговують діти, у тому числі примусово депортовані без супроводження батьків або законних представників до держави-агресора. Так за інформацією МВС України станом на кінець травня 2022 року 234 тисячі дітей з України незаконно переміщено до країни агресора з тимчасово окупованих територій. Окремо наголосимо, що

лише 1 червня 2022 року запрацювала "гаряча лінія" МВС України для звернень рідних та близьких полонених, зниклих безвісти та загиблих українських захисників [39]. При цьому питання щодо формування відповідних реєстрів цивільних осіб ще не розглядаються.

Проблематика ведення зазначених реєстрів включає в себе створення особливого порядку їх наповнення та верифікації доступу про що ми наголосимо у наступному підрозділі. Уповноваженого органу захисту прав суб'єктів персональних даних запропоновано доповнити такими повноваженнями:

- ведення реєстру баз персональних даних;
- здійснення контролю за відповідністю транскордонної передачі персональних даних невизначеного кола осіб, неповнолітніх та інших соціально незахищених верств населення, вимогам законодавства;
- підготовка висновків на законопроекти, що зачіпають конституційне право на недоторканність приватного життя, особисту та сімейну таємницю при обробці персональних даних (до набрання чинності відповідними законами), а також участь у законотворчому процесі з метою більш оперативного реагування на прогалини у законодавстві, що виявляються у практичній діяльності із захисту прав суб'єктів персональних даних;
- розробка керівних принципів уніфікації заходів щодо виконання законодавства про захист приватного життя та персональних даних в умовах технологій, що постійно розвиваються, вироблення єдиних критеріїв та підходів у галузі захисту конституційного права на недоторканність приватного життя при обробці персональних даних.

Проведений аналіз змісту інституту захисту персональних даних, а також практики реалізації його норм у діяльності органів виконавчої влади показав, що правова основа захисту персональних даних в Україні не утворює міцної та єдиної системи норм. Нормативні акти, що закріплюють відповідні правові норми, містять чимало неточностей як теоретичного, і практичного характеру. Мають місце явні прогалини та колізії у правовому врегулюванні розглянутих суспільних відносин.

## **РОЗДІЛ 3. УДОСКОНАЛЕННЯ ОРГАНІЗАЦІЙНО-УПРАВЛІНСЬКИХ ІНСТРУМЕНТІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ГРОМАДЯН В УМОВАХ ВІЙНИ**

### **3.1 Захист персональних даних громадян в умовах війни у контексті державного управління**

Сучасні засоби забезпечення міжнародної безпеки поки що не стали гарантією мирних відносин між державами. У сучасних міжнародних відносинах існують джерела збройних конфліктів. Наукові досягнення у розвитку засобів ведення війни призводять до значного зростання потужності, швидкості та дальності дії сучасних озброєнь.

Століття тому у бойових діях брали участь, як правило, лише військовослужбовці. Громадянські особи, крім випадково опинилися поблизу поля бою, війною не торкалися. Але з того часу, і особливо після Другої світової війни, жертви серед цивільного населення стали значно перевищувати втрати серед військових. Відсоток загиблих на війні по відношенню до населення Землі кожні півстоліття збільшується у 4,5 рази. Якщо XVII столітті у війнах загинуло 3,3 млн. людина, з 1801 по 1913 гг. - 5,6 млн. У Першій світової війни загинуло 10 млн., тоді як у другий близько 55 млн. людина. Понад те, поява ядерної зброї змусило світове співтовариство інакше поглянути на найгострішу проблему сучасності - проблему війни та мира<sup>1</sup>.

Однією із центральних проблем сучасних міжнародних відносин є проблема підтримки міжнародного миру та стабільності на планеті. Формування такого світопорядку, за якого відсутні будь-які зовнішні загрози, засуджуються посягання на законні права та життєво важливі інтереси держави, не допускається втручання у їхні внутрішні справи, залишається найважливішим завданням кожної держави.

У різні періоди історичного розвитку забезпечення міжнародної безпеки надавалося різного значення. Аж до середини ХХ століття держави дбали лише про свою власну безпеку в цілях змінити на свою користь співвідношення сил на міжнародній арені загалом чи окремому регіоні. Становище змінилося лише після створення 1945 року ООН.

Діалектика сучасного світу така, що від безпеки всіх залежить безпека кожної держави. У свою чергу безпека кожної держави є умовою мирного співіснування всього світового співтовариства.

До найбільш істотних чинників, які негативно впливають на сучасний світ, слід віднести загрози виникнення та поширення збройних конфліктів міжнародного і неміжнародного характеру, прагнення окремих держав принизити роль існуючих механізмів забезпечення міжнародної безпеки, показати свою військову перевагу.

Сучасні дослідники зазначають, що війни стають дедалі політизованими, тобто. в них переслідуються далекосяжні політичні цілі, вони стають витонченішими. Політика підганяє вдосконалення зброї. Приміром, у війнах 1950-1953 гг. у Кореї було вперше використано 9 раніше невідомих видів бойової техніки, у В'єтнамі (1964-1975 рр.) – 25, у збройних конфліктах на Близькому Сході та Фолклендах – 30, а у війні у Перській затоці кількість нових зразків зброї та бойової техніки зросла у кілька разів і склало більше 100 різновидів.

Мета різноманітних засобів та методів ведення бойових дій – ослаблення військових сил ворога. Однак воюючі сторони обмежені у виборі методів та засобів досягнення такої мети. Відповідно до норм права збройних конфліктів право сторін, що у конфлікті, вибирати методи та засоби ведення війни не є не обмеженим. Більше того, при розробці та прийнятті на озброєння нових видів зброї, засобів та методів ведення війни держава повинна визначити, чи підпадає їх застосування під заборони, що містяться у міжнародно-правових актах.

Тому держави, як основні суб'єкти міжнародного права, намагалися зменшити згубні наслідки воєн шляхом створення та правового закріплення загальнообов'язкових для всіх норм з метою, по-перше, обмеження воюючих

сторін у виборі засобів та методів воєнних дій та, по-друге, захисту жертв учасників озброєних конфліктів.

Держави, починаючи з 1868 р., почали активно розробляти систему норм міжнародного права з метою обмеження воюючих у засобах та методах ведення війни, захисту цивільного населення, визначення статусу воюючих, військовополонених, інтернованих, правового становища осіб, які перебувають під захистом спеціальних норм, а також окремих категорій осіб. Можна стверджувати, що сучасний період розвитку суспільства характеризується суттєвими досягненнями у сфері регулювання збройних конфліктів та захисту жертв війни, розроблено та прийнято різні міжнародні договори. Це, перш за все, Гаазькі конвенції 1899 та 1907 р.р. про закони та звичаї війни, Женевські конвенції 1949р. та Додаткові протоколи до них 1977 р.

Розроблена та діюча система норм сучасного міжнародного права, що регулює відносини в період збройного конфлікту, дозволяє говорити про самостійну та специфічну галузь міжнародного права - право збройних конфліктів.

Внутрішні та міжнародні збройні конфлікти – реальність сучасного світу. Під час збройних конфліктів найбільше страждають невинні жінки, діти, старі. Значення норм права збройних конфліктів та його застосування стає дедалі актуальніше, оскільки вони спрямовані на захист жертв війни - цивільного населення, поранених, хворих, осіб, котрі зазнали аварії корабля, військовополонених.

Норми права збройних конфліктів зобов'язують воюючі сторони охороняти інтереси жертв війни, поводитися з ними за всіх обставин гуманно і надавати їм якнайшвидше і в найкоротші терміни медичну допомогу та догляд. Між ними не повинно проводитись жодної різниці, незалежно від кольору шкіри, релігії, статі, національного походження, політичних, релігійних та інших переконань. Причому такий захист забезпечується у разі війни, а й у ході будь-якого іншого збройного конфлікту між державами, навіть якщо одна з них не визнає стану війни. Норми захисту жертв війни застосовуються до всіх випадків

окупації, навіть якщо ця окупація не зустріне жодного збройного опору. Норми міжнародного права наказують воюючим вживати всіх можливих заходів для того, щоб розшукувати і підбирати поранених і хворих, захищати їх від протиправного звернення. При цьому воюючі сторони можуть звертатися до місцевих жителів з проханням підбирати та доглядати поранених та хворих, надаючи особам, які виявили бажання виконувати таку роботу, необхідну допомогу та пільги.

Під захистом права збройних конфліктів знаходиться незахищена і вразлива частина будь-якого суспільства - громадянське населення. До цивільного населення належать особи, які не належать до жодної категорії учасників бойових дій і безпосередньо не беруть участі у збройному конфлікті. Ще в Петербурзькій декларації про відміну вживання вибухових і запальних куль 1868 року вказувалося на неприпустимість нападу воюючих сторін на мирне населення, і єдина законна мета воюючих полягає в ослабленні військових сил ворога. Це становище набуло подальшого розвитку в нормах права збройних конфліктів. Зокрема, ст.51 Додаткового протоколу до Женевських конвенцій від 12 серпня 1949 року щодо захисту жертв збройних конфліктів міжнародного характеру закріплює, що цивільне населення та окремі цивільні особи не повинні бути об'єктом нападу.

У сучасних умовах положення Статуту ООН забороняють будь-які форми застосування сили; винятки становлять лише випадки самооборони. Норми Статуту ООН закріплюють вимоги щодо необхідності вирішення міжнародних суперечок мирними засобами, утримуватись у міжнародних відносинах від загрози силою або її застосування проти територіальної цілісності чи політичної незалежності будь-якої держави. Держава, яка для досягнення своєї мети використовує силу проти іншої держави або держав, порушує чинні норми міжнародного права.

Водночас, Статут ООН не обмежує право застосовувати збройну силу стосовно іншої держави під час здійснення права на самооборону (право на індивідуальну самооборону). Це ж справедливо і щодо дії третіх країн, які

надають допомогу державі-жертві агресії, наприклад, відповідно до міжнародної угоди про надання взаємної допомоги у разі агресії (право на колективну самооборону). І, нарешті, Рада Безпеки ООН, з дотриманням встановленої процедури, може здійснити збройні чи інші акції для підтримки чи відновлення міжнародного миру та безпеки.

Таким чином, сучасне міжнародне право забороняє ведення воєн, крім випадків здійснення права на самооборону, підтримання та відновлення миру, використовуючи при цьому відповідну процедуру прийняття рішень, закріплену у Статуті ООН.

Право збройних конфліктів захищає різні категорії осіб, які так чи інакше зачіпаються збройним конфліктом. Осіб, яких міжнародне право повністю позбавляло б захисту у процесі збройної боротьби, немає. Різні лише обсяг і зміст захисту. Для визначення обсягу та змісту необхідного захисту важливо правильно визначити характер участі конкретних осіб у збройному конфлікті. У разі йдеться про правове становище комбатантів і некомбатантів. Головною та визначальною умовою для визнання конкретної особи комбатантом є можливість її цілеспрямованої та законної участі у військових діях на користь (і від імені) воюючої сторони, до лав комбатантів якої вона зарахована. Тому необхідно уточнити, що комбатантами можуть бути особи, які входять до складу регулярних та іррегулярних сил.

Сучасне міжнародне право закріплює необхідність воюючих сторін забезпечувати захист цивільного населення. Воюючі по відношенню до цивільного населення керуються двома імперативними вимогами: за жодних умов не робити нападів на цивільне населення; у будь-який час проводити різницю між комбатантами і громадянським населенням. Міжнародне право передбачає надання цивільному населенню різних рівнів захисту та відповідно надання певних режимів забезпечення безпеки. Норми міжнародного права регулюють забезпечення як загального, так і спеціального правового захисту від наслідків воєнних дій. В даному випадку необхідно провести чітку межу між різними видами правових захистів, що надаються цивільному населенню.

Важливим та актуальним питанням права збройних конфліктів є регулювання військового полону та відповідного режиму, що визначає знаходження військовополонених у владі ворожої держави (а не окремих польових командирів, керівників тимчасової військової адміністрації тощо). Норми права закріплюють, що з військовополоненими завжди слід поводитися гуманно. Вони під захистом держави від насильства, залякування, образ, застосування репресалій тощо. Спеціально виділено заборону на проведення над військовополоненими наукових чи медичних дослідів, якщо це не виправдовується станом здоров'я чи інтересами військовополоненого. Останнє недостатньо чітко регулюється нормами права збройних конфліктів та потребує розробки. Законодавство, не містить визначень військового полону та добровільної здачі в полон. Це питання потребує необхідного теоретико-правового обґрунтування.

Стан збройного конфлікту безпосередньо впливає правове становище іноземних громадян. Відповідно до норм права збройних конфліктів такі громадяни можуть бути інтерновані. Теоретико-правові питання режиму інтернування, правового становища інтернованих та їх власності, що перебуває в державі тимчасового перебування через їх важливість та складність, потребують детального наукового опрацювання. Більше того, норми права збройних конфліктів, окрім інтернування, закріплюють можливість застосування до іноземних громадян заходів, пов'язаних із примусовим поселенням, але не розкривають їх сутність. Інтернування та примусове поселення - терміни не рівнозначні і передбачають здійснення різних організаційно-правових заходів щодо іноземних громадян.

Участь найманців у збройних конфліктах, яка від них реальна (чи потенційна) загроза безпеці та стабільності конкретної держави, викликали негативне ставлення до них з боку членів світової спільноти. Закріплення у джерелах права збройних конфліктів положення, що використання найманців - це злочин, означає, що засуджується не лише дія (поведінка) найманців, а й поведінка відповідної держави. Дія держави, яка посиляє найманців в іншу

країну або терпимо ставиться до вербування та діяльності найманців своїх громадян, повинні розглядатися як протиправні. Значне місце у боротьбі та протидії найманству має відводитися механізму співробітництва держав.

Міжнародне право передбачає надання цивільному населенню різних рівнів захисту та відповідно надання певних режимів забезпечення безпеки. Право збройних конфліктів забезпечує як загальний, і спеціальний правовий захист від наслідків військових дій. Загальний захист надається всьому цивільному населенню незалежно від віку, політичних поглядів, релігійних переконань, віку, расової належності тощо. Надання спеціального захисту пов'язане з підвищеною вразливістю певних категорій заступництв (діти, жінки) в умовах збройних конфліктів або пояснюється їх особливою роллю у наданні допомоги цивільному населенню та забезпеченні його безпеки та виживання під час бойових дій (персонал медичних формувань).

Під режимом військового полону слід розуміти сукупність міжнародно-правових і внутрішньодержавних приписів, регулюючих правове становище військовополонених. Цей режим включає такі елементи:

- а) повагу та дотримання прав військовополоненого;
- б) обов'язки та права військовополоненого;
- в) відповідальність військовополонених та посадових осіб, які забезпечують дотримання правил поведінки з військовополоненими.

Сучасне міжнародне право та національне законодавство не містить визначень військового полону та добровільної здачі в полон. Військовий полон це стан, у якому військовослужбовці і прирівняні до них нормами права особи що неспроможні виконувати обов'язки військової служби з того, що перебувають під владою іншої воюючої держави.

Під добровільним здаванням у полон слід розуміти самовільне припинення виконання обов'язків військової служби, керуючись особистими мотивами.

Крім того, у сучасному міжнародному та національному праві відсутні норми, що регулюють обмін військовополоненими. Розробка механізму та

процедур обміну військовополонених, їх законодавче закріплення усуне правову прогалину у вирішенні цього питання.

Під інтернуванням слід розуміти санкціоноване державою тимчасове обмеження прав і свобод громадян держави супротивника та його союзників, виходячи з інтересів забезпечення власної безпеки, а також для забезпечення безпеки самих іноземних громадян.

Особливості відносин, пов'язаних із захистом персональних даних зазначених вище категорій осіб систематизовано нами у таблиці 3.1.

Таблиця 3.1. Особливості відносин, пов'язаних із захистом персональних даних

№	Характеристика особливостей
1	вони мають конституційно-правову природу, оскільки пов'язані із забезпеченням права людини на недоторканність приватного життя та суміжних із ним конституційних прав в умовах розвитку технологій автоматизованої обробки інформації;
2	ці відносини пов'язані з реалізацією прав (чи повноважень) інших суб'єктів, визначених Конституцією України, що породжує різноманітні конфлікти інтересів сторін даних правовідносин;
3	їх учасниками є специфічні суб'єкти: оператор баз даних, власник баз даних, суб'єкт персональних даних та уповноважений орган, який розглядає звернення суб'єкта персональних даних щодо відповідності змісту персональних даних та способів їх обробки цілям обробки та приймає відповідні рішення;
4	об'єктом цих відносин є будь-яка документована інформація, що міститься в інформаційних системах, неправомірне поводження з якою може завдати шкоди її власнику, власнику, користувачеві чи іншій особі;
5	вони мають специфічний зміст, особливості якого виражаються у цьому, що оператор має як юридичні обов'язки, а й декларація про отримання певної інформації про суб'єкт персональних даних обсягом, передбаченому законами і підзаконними актами. Відповідно у суб'єкта персональних даних виникає обов'язок надати інформацію, яка відповідає вимогам повноти та достовірності;
6	реалізація суб'єктивних прав їх учасників безпосередньо залежить від етапів розвитку правовідносин;
7	ці відносини мають правозахисний характер.

Примітка: Розроблено автором

Особливими також є аспекти використання мережі Інтернет, як окремими категоріями населення в звичайних умовах так і умовах ведення бойових дій.

Так, важливим аспектом реалізації свободи доступу до інтернет-середовища є доступ певних категорій осіб таких як: працівники правоохоронних органів, військовослужбовці, військовозобов'язані під час проведення військових зборів, осіб, які відбувають різні види кримінальних покарань, пов'язаних з обмеженням або позбавленням волі. Особливого загострення в Україні це питання набуло у контексті проведення на сході держави АТО і обумовлено необхідністю захисту життя і здоров'я цієї особливої групи інтернет-користувачів, а також мотивами збереження державної та військової таємниці. Ми вважаємо, що можна скористатись європейським досвідом, яскравим прикладом якого є справа Калда проти Естонії (рішення від 19 січня 2016 року). Рішення у справі стосується питання щодо права в'язнів на доступ до Інтернету. Це рішення має серйозні наслідки, адже створює перший прецедент для потенційно широкого розширення права на доступ до Інтернету для ув'язнених [88].

Позивачем у справі виступив громадянин Естонії, що відбував довічне покарання у в'язниці міста Пярну. У 2005 році він попросив її керівника надати йому доступ до трьох сайтів: он-лайн версії Державної Газети; рішень Верховного Суду та адміністративних судів, що є доступними в мережі Інтернет; бази даних HUDOC із рішеннями ЄСПЛ [89].

У наданні доступу йому було відмовлено. В результаті процедури оскарження цього рішення Верховний Суд Естонії постановив, що така відмова є неправомірною. Водночас, позивача було переміщено до іншої в'язниці у місто Тарту, де він стикнувся із аналогічною проблемою. Мотивуючи свій запит наявністю спорів із адміністрацією в'язниці, Калда вимагав надати йому доступ до інших трьох сайтів: Інформаційного офісу ради Європи у Таллінні; Канцлера юстиції; Естонського парламенту[89]. Щоправда, на цей момент в'язниця вже забезпечила своїх ув'язнених доступом до деяких сайтів, серед яких – сайт ЄСПЛ, проте він містив інформацію лише англійською та французькою мовами. Адміністративний Суд, розглядаючи скаргу Калди вирішив, що йому має бути надано доступ до сайту Інформаційного офісу Ради Європи, що містить переклади рішень ЄСПЛ на естонську, проте вказав, що доступ ув'язнених до

двох інших сайтів не передбачений за законом. Таке рішення не задовольнило жодну із сторін, що призвело до подальшого оскарження. Цього разу Верховний Суд не визнав за позивачем права доступу до жодного з перелічених сайтів, мотивуючи це рішенням захистом правопорядку, збільшенням коштів на контроль за використанням Інтернету та наявністю в ув'язнених альтернативних шляхів отримання офіційної інформації (бібліотека та пошта) [89].

ЄСПЛ розглянув цю справу в контексті порушення права на інформацію за ст. 10 Європейської конвенції з прав людини. Суд нагадав, що суспільство має право отримувати інформацію, що становить загальний інтерес, тому держави повинні утримуватись від створення перешкод для доступу особи до такої інформації. Проте він зазначив, що це право не можна тлумачити, виводячи з нього загальний обов'язок забезпечення доступу ув'язнених до Інтернету або до окремих сайтів, адже ув'язнення як таке неминуче та призводить до ряду обмежень. Суд визнав, що втручання було передбачене законом, адже містилося у Акті про ув'язнення, що встановлював коло дозволених сайтів, та переслідував легітимні цілі захисту прав інших осіб та запобігання заворушенням і злочинам [89].

Вирішуючи питання щодо необхідності у демократичному суспільстві вищезазначених свобод, Суд звернув увагу на таке: по-перше, інформація сайтів, до якої хотів отримати доступ позивач, була передусім правовою інформацією та інформацією про основні права людини, зокрема права в'язнів, потрібною позивачеві для захисту своїх прав у суді; по-друге, Суд вказав на суттєву різницю між можливістю самостійного пошуку інформації на сайті та можливістю зробити запит до відповідного органу, що тягне за собою додаткові кошти; по-третє, Суд звернув увагу на те, що переклади рішень ЄСПЛ з'являються на доступних позивачеві сайтах набагато пізніше, ніж на сайті Ради Європи, а також, що офіційним оприлюдненням правових актів у Естонії є їх публікація в Інтернеті, а не публікація друкованих версій, які можна знайти у бібліотеці в'язниці [89]. Врешті, Суд зазначив, що національні суди посилались на ризик безпеки як на загальну підставу, не зробивши детального оцінювання ризиків

безпеки доступу до ще трьох конкретних сайтів. Враховуючи те, що доступ до Інтернету ув'язнені здійснюють зі спеціально обладнаних комп'ютерів, надання доступу до цих сайтів не має спричинити значних додаткових витрат. Отже, на підставі таких суджень ЄСПЛ зробив висновок, що ст. 10 Конвенції було порушено [89]. Зазначене рішення підштовхує до необхідності врахування позиції ЄСПЛ при реалізації прав засуджених на доступ до Інтернету в Україні, яке передбачено ст. 110 Кримінально-виконавчого кодексу України та наказом Міністерства юстиції України від 19 жовтня 2017 року № 3233/5.

На особливу увагу заслуговують питання свободи доступу до Інтернету військовослужбовців під час виконання ними своїх обов'язків та несення служби у зоні ООС (АТО). Так, відповідно до правил інформаційної та кібернетичної безпеки в зоні проведення АТО, які носять рекомендаційний характер, наголошується на дотриманні наступних правил безпеки: недопущення визначення місцерозташування за допомогою геолокації, функції якої увімкненні на персональних пристроях військовослужбовців; необхідність використання паролів та якісного антивірусного обладнання; неприпустимість використання WiFi-роутерів та інтернет-модемів; дотримання безпечної поведінки при користуванні Інтернетом; обережне ставлення до використання соціальних мереж з метою недопущення розповсюдження інформації, яка може становити військовий або розвідувальний інтерес для супротивника.

Необхідно зазначити, що виконання завдань військовими в зоні АТО часто означає збільшення ймовірності втрати, конфіскації, крадіжки мобільного телефону, флеш-картки чи ноутбука. На останніх можуть зберігатися, зокрема, 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» за підтримки програми МАТРА від уряду Нідерландів, що реалізовує ГО «Інтерньюз-Україна» було підготовлено рекомендації, метою яких є покращення комунікацій під час

конфлікту, окреслення викликів для свободи Інтернету та підвищення цифрової безпеки на рівні як інституцій, так і інтернет-користувачів.

У рекомендаціях для військовослужбовців запропоновано: блокувати пристрої щоразу, коли відходите від них, встановлювати повне шифрування на всі диски комп'ютера, встановити надійний пароль для входу в соціальну мережу, не заходити в акаунти соцмереж з незнайомих чи незахищених пристроїв, публікуйте часткову або несправжню інформацію про себе (наприклад, зазначення в профілі Facebook місцем навчання військової інституції та участь у групі з конкретною військовою частиною можуть точно вказати місце служби військовослужбовця), обмежте доступ до приватної інформації в налаштуваннях конфіденційності соціальної мережі, перегляньте список ваших друзів у соціальній мережі (якщо серед них є незнайомі або сумнівні особи - видаліть їх), не фотографуйте місця з примітними ознаками ландшафту чи території та військову техніку (головне, щоб її не можна було ідентифікувати за допомогою зовнішніх знаків і позначень) тощо.

На нашу думку, зазначені правила поведінки та рекомендації мають носити не лише рекомендаційний, а обов'язковий характер, адже певні обмеження, які встановлюються для цієї категорії осіб не можуть вважатися порушенням їх прав, як інтернет-користувачів.

У контексті зазначеного необхідно виділити структуру діяльності з «Опрацювання даних», яка означає будь-яку операцію або низку операцій з такими персональними даними та системотворчу роль публічних органів влади, що встановлюють базові принципи та вимоги щодо захисту інформації персонального характеру, у формуванні відповідної національної галузевої законодавчої політики (Рисунок 3.1).

При розгляді досвіду регулювання опрацювання персональних даних привертає увагу уніфікованість, яка виявляється у забезпеченні безпеки зібраних персональних даних; забезпечення можливості суб'єкта ознайомлення та уточнення персональних даних; вимога чітко формулювати мету використання персональних даних, яка може бути змінена без згоди суб'єкта персональних

даних; створення спеціального органу, що забезпечує контроль за дотриманням прав суб'єкта персональних даних (наприклад, Комісії, Управління та ін.). Відмінності стосуються, перш за все, кола осіб, які зобов'язані виконувати норми законів, що регламентують захист персональних даних у відповідній сфері діяльності.

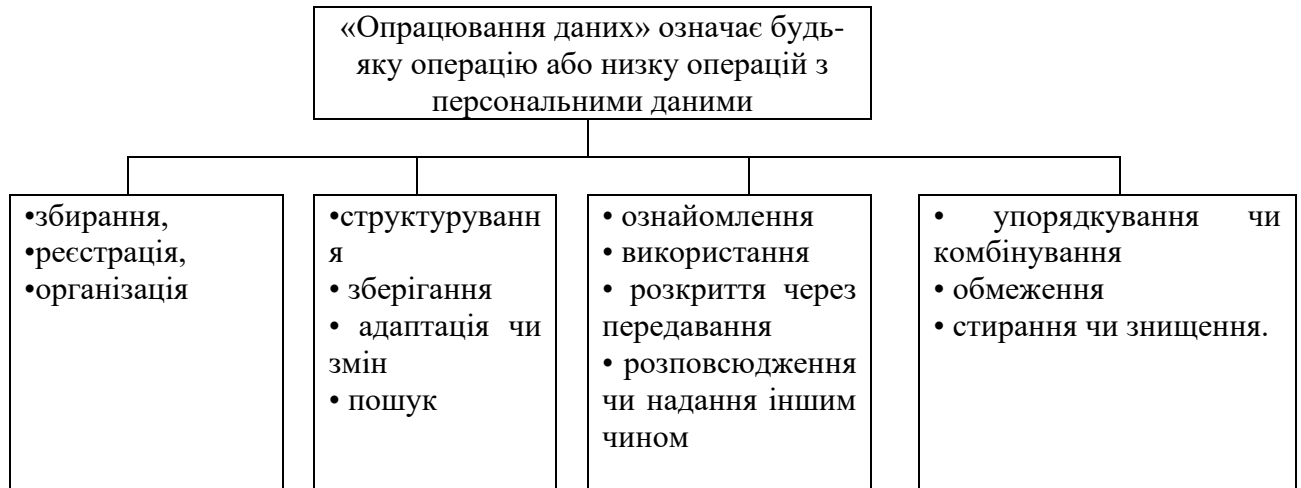


Рисунок 3.1 Структура діяльності з «Опрацювання даних», яка означає будь-яку операцію або низку операцій з такими персональними даними

На особливу увагу заслуговує офіційна позиція окремих зарубіжних джерел, згідно з якою персональні дані працівника розглядаються як інформація, що характеризує професійні та ділові якості громадянина, необхідна для виконання особою трудової (службової) діяльності.

Мета обмеження конституційного права на недоторканність приватного життя, особисту та сімейну таємницю та, відповідно і прав персональних даних полягає у наступному, необхідність: захисту основ конституційного ладу (забезпечення територіальної цілісності та захист суверенітету); захисту моральних цінностей; дотримання та захист прав і свобод людини та громадянина за умови, що при цьому не порушуються права та свободи третіх осіб; охорони здоров'я та забезпечення сприятливого довкілля; забезпечення оборони країни; забезпечення безпеки держави.

### **3.2 Напрями удосконалення організаційно-управлінських засад державного управління у сфері захисту персональних даних громадян під час війни**

Проблеми забезпечення захисту персональних даних громадян поставлені перед суспільством після 24 лютого 2022 року вимагають свого негайного вирішення у тому числі на нормативно-правовому та організаційно-управлінському рівнях.

Водночас, необхідно пам'ятати, що в умовах широкомасштабної військової агресії, наявності декількох театрів бойових дій на території України, необхідно одночасно вести мову не лише про встановлення законних обмежень окремих прав і свобод людини і громадянина але й про напрацювання нових правових механізмів їх захисту через діяльність органів публічної влади та окремих інститутів громадянського суспільства.

Особливе занепокоєння викликає стан дотримання прав у сфері захисту персональних даних військових, примусово переміщених громадян, мешканців тимчасово окупованих територій та інших категорій громадян.

Вже сьогодні, для громадських активістів і волонтерів дійсно є актуальним це питання, адже вони мають/можуть мати справу з персональними даними людей, або можуть вчасно поінформувати колег щодо збирання персональних даних. Це випадки різних анкетувань, фокус-груп, це ведення списків на різні запити допомоги, це, можливо, списки на евакуацію, це якась внутрішня звітність або для міжнародних організацій, які передають допомогу тощо [75].

Інформація, безпосередньо пов'язана з конкретною людиною (факти її біографії, номінативні (називні) дані, національність, місце проживання, відомості про захворювання, про професійні знання та навички, про сімейне життя, звички, захоплення, моральні, політичні, сексуальні та релігійні уподобання та багато іншого), становить велику або навіть більшу частину інформації, що циркулює в суспільстві. Людина залишає відповідні

«інформаційні сліди» у відділах кадрів, соціальних службах, органах виконавчої влади, у сфері послуг, різних організаціях.

Найчастіше повідомлення подібної інформації перебуває у інтересів самого індивіда чи є необхідною умовою отримання конкретного соціального статусу чи певних послуг.

Поширення такої інформації без згоди самої людини може сприяти формуванню її позитивного іміджу, а може завдати непоправної шкоди, моральної чи матеріальної шкоди. Саме тому поводження з інформацією персонального характеру (персональними даними) потребує особливої правової регламентації.

Сьогодні з упевненістю можна стверджувати, що інформацію персонального характеру визнано одним із пріоритетних об'єктів організаційно-правового захисту, оскільки за певних умов та обставин вона є похідною від права на недоторканність приватного життя.

Очевидно, що людина як соціальний елемент, який постійно перебуває у відносинах з іншими людьми, організаціями, органами влади, не може не повідомляти про себе персональні дані, залишаючись інкогніто в цих відносинах. У якихось ситуаціях він сам визначає, які персональні дані йому слід повідомити, а в якихось (найчастіше у відносинах з державою) він змушений повідомляти свої дані для того, щоб зробити юридично значущі дії, реалізувати свої права та покладати на себе відповідні обов'язки.

У суспільстві майже всі люди, можливо за рідкісним винятком, здійснюють трудову діяльність у різних формах. Вступаючи на роботу, практично кожен громадянин на вимогу роботодавця надає численні документи та заповнює анкети, в яких містяться розділи, що належать не тільки до професійної діяльності, а й торкаються аспектів приватного життя особи.

Вже при першому заочному знайомстві з потенційним працівником має намір отримати максимальну інформацію про нього, проте відсутність чіткого критерію, що дозволяє розмежувати інформацію персонального характеру, що стосується аспектів приватного життя особи, та інформацію, що характеризує

особу безпосередньо як працівника, тобто. з погляду його ділових та професійних якостей, рівня освіти чи кваліфікації, є «камнем спотикання», що утрудняє для роботодавця можливість визначення ступеня допустимого втручання та меж вторгнення у приватне життя працівника.

Подібна обставина породжує ситуації, в яких відсутність чіткого розуміння того, яку інформацію необхідно визнати об'єктом захисту або персональними даними працівника, призводить до неможливості реалізації норм, що визначають порядок та умови збору, зберігання, використання та розповсюдження відповідної інформації у трудовій сфері.

З розвитком процесів інформатизації суспільства, створенням нових та інтеграцією існуючих інформаційних систем, орієнтованих обслуговування населення, дедалі більше уваги приділяється організації обробки персональних даних. Персональні дані становлять важливу частину інформаційного простору, що містить відомості про фізичних осіб - суб'єктів персональних даних.

Виділення таких даних в окреме підмножина обумовлено особливими вимогами до організації їх обробки (діям з персональними даними), пов'язаними з можливістю шкоди суб'єктам персональних даних. Тому як у зарубіжних країнах, і у Україні розвивається і вдосконалюється законодавча база, яка регламентує правила обробки персональних даних і реалізацію прав громадян на конфіденційність інформації, що їх стосується.

Особлива увага приділяється питанням захисту персональних даних в автоматизованих інформаційних системах персональних даних - ІСПД. Вимоги до захисту в ІСПД, відповідно до низки документів, враховують категорію та кількість персональних даних, специфіку розв'язуваних завдань та низку інших показників.

Виконання цих вимог, як правило, пов'язане із суттєвими матеріальними та фінансовими витратами, викликаними необхідністю створення системи захисту, забезпеченням високої кваліфікації персоналу, отриманням дозвільних документів, що не завжди можливе для великої кількості користувачів

інформації та операторів, які представляють малобюджетні організації (медичні та освітні установи), підприємства, громадські організації).

У зв'язку з цим цікаві дослідження спрямовані на розробку та аналіз методів обробки персональних даних, що дозволяють знизити витрати на забезпечення безпеки в ІСПД.

Одним із перспективних підходів у цьому напрямі є обробка знеособлених персональних даних, коли стає неможливим без використання додаткової інформації визначити належність персональних даних конкретного суб'єкта і, отже, забезпечується неможливість для операторів та інших осіб, які отримали доступ до знеособлених даних, розкривати третім особам та поширювати персональні дані без згоди суб'єкта персональних даних.

Для реалізації цього підходу потрібно розробити та дослідити методи знеособлення та де-знеособлення персональні дані, правила роботи з знеособленими даними.

Своєчасність заданого напрямку досліджень обумовлена зростаючою потребою у розвитку ІСПД, пов'язаної з виконанням різних програм, посиленням відповідальності за безпеку персональних даних та необхідністю у зв'язку з цим підвищувати ефективність створюваних систем при одночасному зниженні витрат на їх експлуатацію, що можливо за наявності достатньо універсальних рішень.

Одним з перших кроків у сфері формування нових правових механізмів захисту персональних даних громадян органами публічної влади стала Постанова КМУ від 12 березня 2022 р. № 263 "Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану" на період дії воєнного стану міністерства, інші центральні та місцеві органи виконавчої влади, державні та комунальні підприємства, установи, організації, що належать до сфери їх управління, для забезпечення належного функціонування інформаційних, інформаційно-комунікаційних та електронних комунікаційних систем, публічних електронних реєстрів, володільцями

(держателями) та/або адміністраторами яких вони є, та захисту інформації, що обробляється в них, а також захисту державних інформаційних ресурсів, можуть вживати таких додаткових заходів, серед іншого це: розміщувати державні інформаційні ресурси та публічні електронні реєстри на хмарних ресурсах та/або в центрах обробки даних, що розташовані за межами України, та реєструвати доменні імена у домені gov.ua для такого розміщення та зупиняти, обмежувати роботу інформаційних, інформаційно-комунікаційних та електронних комунікаційних систем, а також публічних електронних реєстрів [14].

Таким чином, органами державної влади було створено необхідні організаційно-технічні передумови для захисту прав окремих категорій громадян, в першу чергу тих, хто виконує завдання щодо оборони України, захисту її суверенітету, територіальної цілісності та потребують додаткових гарантій захисту їх персональних даних.

Отримавши можливості захисту інформаційних ресурсів, органами влади було створено організаційно-технічні передумови до захисту окремих категорій громадян, що потребують додаткових гарантій захисту їх персональних даних.

Сьогодні ми можемо виділити наступні групи громадян щодо яких постають питання захисту персональних даних.

Водночас у найбільш гострій формі питання забезпечення захисту персональних даних торкається українських військовослужбовців. В першу чергу мова йде про представників силових (мілітаризованих) структур (Збройних Сил України, Національної гвардії України, Служби Безпеки України, Національної поліції, Державної прикордонної служби України та інших військових формувань), які безпосередньо, зі зброєю в руках, забезпечують оборону нашої держави.

Доступ агресора, який він постійно намагається отримати, до персональних даних даної категорії осіб несе загрозу не тільки національній безпеці, а й правам цих осіб та членам їх сімей. Наприклад, російська прокремлівська хакерська група RaNDIt виклала у відкритий доступ дані 700 співробітників Служби безпеки України. Дані про співробітників Служби

Безпеки України доповнили список військовослужбовців української армії, що існував раніше, де зазначені: ім'я, по батькові, прізвище, дата народження, посада, звання, адреса, телефон, паспортні дані, у ряді випадків – електронна пошта, сторінки в соцмережах та інші дані. Як правило, запис ілюструється фотографією [64].

Ці дані можуть бути використані, і використовуються ворогом, на шкоду правам цих осіб, членів їх сімей. Наприклад, для залякування членів сімей, завдання моральних страждань, завдання фізичної шкоди здоров'ю, загрози життю.

Так, наслідком перебування військовослужбовця у зоні ведення бойових дій доволі часто може стати його полон, тобто – у найзагальнішому розумінні – обмеження свободи (насильне утримання) військовослужбовця державою-противником в особі її військових органів із метою обмеження участі у бойових діях. Комбатанти які перебувають у військовому полоні набувають статусу військовополоненого відповідно до Женевської Конвенції про поводження з військовополоненими (від 12.08. 1949 р.) [21].

Таким чином, військовослужбовці Збройних Сил України, і члени військових добровольчих формувань, котрі ведуть боротьбу із окупантом на тимчасово непідконтрольних Україні територіях, у разі потрапляння у полон до сепаратистів та регулярних військ Російської Федерації, набувають фактично статусу військовополонених, а відтак – мають право на гідне, гуманне поводження, що виключає жорстокість і катування, а також дискримінацію за будь-якою соціальною, расовою, релігійною, гендерною тощо ознакою [21].

Сьогодні, на жаль, українські військовополонені не можуть почуватися впевнено у тому, що до них у повному обсязі буде застосовано норми міжнародного законодавства, що встановлює і регулює звичаї ведення війни. Отримуючи доступ до персональних даних військовополонених ворог може використати їх для здійснення шантажу його рідних та органів державної влади України, розповсюдження панічних настроїв та інших гібридних способів інформаційної складової війни.

Оборот та обробка персональних даних – єдина група суспільних правовідносин, яка пов'язана з інформацією обмеженого доступу, що визначає фізичних осіб за допомогою поняття «персональні дані». Самостійне регулювання цієї групи відносин досягається сукупністю правових норм, що утворюють єдиний комплекс, окрему правову категорію.

Сьогодні явною є необхідність законодавчого встановлення самостійного обмеження користувачем доступу до персональних даних у соціальних мережах та медіа.

Законодавчо не встановлено обов'язок операторів обмежувати доступ до персональних даних користувачів за допомогою Інтернету. Конструктивні особливості окремих інтернет-ресурсів дають змогу зареєстрованим користувачам отримувати доступ до чужих персональних даних.

Відповідно постає актуальне питання, який саме орган публічної влади має який має забезпечити захист персональних даних військовослужбовців в умовах війни та буде займатися їх пошуком після завершення бойових дій. Також викликає занепокоєння широке та неконтрольоване розповсюдження персональних даних військовослужбовців в тому числі і військовополонених у мережі Інтернет.

Так, наприклад, практично з самого початку бойових дій у соціальній мережі "Фейсбук" з'явилися численні сторінки на яких розміщено фотографії осіб у військовій формі з твердженням, що ці особи є військовополоненими Збройних Сил України та інших військових формувань України.

До числа таких активно діючих сторінок можна віднести "Пошук людей, зниклих під час війни в Україні", "Пошук зниклих людей на війні. Не забудемо, не пробачимо!!!", "Пошук людей по всій Україні", "Сиделки Херсон" та багато інших. На зазначених сторінках у соціальній мережі розміщено багаточисельні фотографії, у тому числі з супроводженням написами на таблицях які тримають у руках ймовірно військовополонені, багато з сфотографованих не мають на собі військової форми та одягнуті у цивільний одяг. Зазначені ресурси активно

репостять користувачі інтернету, розповсюджуючи інформацію із закликами до проведення візуального впізнання військовополонених.

Вільне розповсюдження подібної інформації в умовах ведення війни є серйозним порушенням вимог міжнародних конвенцій щодо військовополонених та національного законодавства, в тому числі і у частині захисту персональних даних захисників України та примусово затриманих або викрадених цивільних.

Як наголошує Координаційний штаб із питань поводження з військовополоненими "публічне розповсюдження інформації про полонених може зашкодити процесу обміну. Інформація про значущість людини, її політичні погляди, місце служби, попередню роботу, рідних та близьких провокує прискіпливе ставлення ворога. В результаті вимоги до обміну конкретної особи можуть бути завищені, а сам процес максимально ускладнений. Звертаємо увагу, що розповсюдження інформації про позивні, військову частину, місце дислокації підрозділу, обставини потрапляння в полон несе загрозу не тільки самому полоненому, але його бойовим побратимам та підрозділу" [43].

У подібному напрямку інформаційну політику здійснює і Міністерство оборони України, підкреслюючи, що громадським активістам, які збирають дані про загиблих і оприлюднюють цю інформацію варто зважити на те, що оприлюднення такої інформації наразі шкодить обороні країни [24].

Родини військовополонених здебільшого не мають чіткого розуміння, як їм діяти та до яких установ звертатися, коли прийшла звістка про потрапляння в полон члена сім'ї, попри різні публікації в мережі Інтернет.

Загальноприйнято вважати, що існують умовні «списки», до яких вносяться відомості про полоненого, після чого уповноваженими державними органами вони надаються представникам РФ.

Насправді не існує таких «списків». Чи точніше сказати, саме такий підхід є дуже спрощеним.

Насправді ж існує відповідний державний реєстр Національного інформаційного бюро, (<https://nib.gov.ua/uk/>).

Члени сімей самостійно чи через представника можуть внести відомості про військовополоненого до реєстру. Канали комунікації є різними: звернення на електронну пошту, спеціальна електронна форма, телеграм.

Надалі буде можливість відстежувати статус військовослужбовця, наприклад, зі статусу «ймовірно перебуває в полоні» на «перебуває в полоні».

Важливим є те, що для того, щоб особа опинилася у статусі «перебуває в полоні», цей факт мають підтвердити або ворожа сторона, або Міжнародний комітет Червоного хреста.

Проте потрібно мати на увазі, що пріоритетів щодо осіб, які підлягають звільненню, не існує, і статус ймовірного перебування в полоні є досить умовним.

Вся наявна у реєстрах Національного інформаційного бюро інформація використовується для координації пошуку та звільнення полонених, а також в процесі ведення перемовин щодо обмінів та звільнення.

Після проведеної зустрічі із сім'ями військовополонених ми окреслили алгоритм дій щодо офіційного внесення відомостей про полон членів їх сімей.

Визначили, що Національне інформаційне бюро буде проінформоване про перебування осіб в полоні, що НІБ буде проінформовано про цінність кожного окремо взятого військового, що буде взято курс на роз'яснення членам сімей військовослужбовців механізму направлення звернень про перебування осіб в полоні.

Вважаємо, що сьогодні необхідно визначити конкретний орган публічної влади відповідальний за розповсюдження інформації щодо військовослужбовців та цивільних осіб які стали жертвами війни, зникли безвісти або незаконно утримуються окупаційною владою. На даний час встановлена "Гаряча лінія" Міністерства внутрішніх справ України для звернень рідних українських бійців полонених, зниклих безвісти та загиблих. Фактично на Міністерство внутрішніх справ України покладено обов'язок здійснення обробки інформації щодо

персональних даних військовослужбовців. При цьому реєстри зазначених осіб було створено співробітниками Міністерства з питань реінтеграції тимчасово окупованих територій.

Водночас питання обміну військовополоненими здійснювалося на перших етапах війни віце-прем'єр Міністерством з питань реінтеграції тимчасово окупованих територій, а після 2 червня 2022 року було неофіційно передано до відома Головного управління розвідки України. Зрозуміло, що зазначені органи влади офіційно не мали подібних повноважень і здійснюють їх *ad hoc*.

З нашої точки зору вирішення питання можливе шляхом розширення повноважень Координаційного штабу з питань поводження з військовополоненими до рівня Міжвідомчого координаційного центру з питань обліку, обміну та повернення полонених, зниклих безвісти та загиблих. До компетенції такого Міжвідомчого координаційного центру необхідно віднести, як обліку, обміну та повернення комбатантів так і некомбатантів (у тому числі і громадян іноземних держав або апатридів, які проживали/перебували на території України).

*Проблема забезпечення захисту персональних даних органами публічної влади в умовах війни залишається винятково гострою.* Важливою умовою забезпечення захисту персональних даних громадян має бути контроль інформаційного середовища, що повинно покласти краї неконтрольованому розміщенню у соціальних мережах багаточисельних сторінок з фотографіями та відео українських полонених з їх персональними даними. Зазначені заходи носять явний акцент антиукраїнської пропаганди та є порушенням прав військовополонених у тому числі і у сфері захисту їх персональних даних.

Також, на нашу думку, для забезпечення захисту персональних даних військовослужбовців необхідно розробити окремі інформаційні реєстри згаданих нами вище категорій осіб з різним ступенем верифікації доступу до них та унормування можливості отримання інформації щодо суб'єктів, які внесені до цих баз даних або навпаки отримати інформації що у цих базах даних інформація щодо певних осіб відсутня. Зазначене має покласти краї неконтрольованому

розміщенню у соціальних мережах багаточисельних сторінок з фотографіями та відео українських військових, військовополонених з їх персональними даними. Це дозволить запобігти порушенням прав військовослужбовців через несанкціонований доступ до їх персональних даних.

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

## ВИСНОВКИ

1. Запропоноване таке визначення поняття "персональні дані", що враховує міжнародно-визнані критерії «ідентифікованості суб'єкта даних» та «чутливості»: персональні дані - це дані в машинно-орієнтованій формі, що містять інформацію про приватне життя конкретного живого індивіда (суб'єкта даних), що може бути ідентифікований на підставі цієї інформації (або за допомогою цієї та іншої інформації), якщо з точки зору будь-якої нормальної людини, наділеної звичайною чутливістю, суб'єкт даних має право вважати таку інформацію конфіденційною та контролювати її поширення.

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

2. Правовий режим воєнного стану за національним законодавством є більш регламентованим ніж стан війни. Водночас, системний аналіз положень національного законодавства України дає підстави для висновку про те, що не існує принципової відмінності між введенням правового режиму воєнного стану та оголошення стану війни у юридичних наслідках для публічних правовідносин. Застосування норм міжнародного гуманітарного права не перебуває у залежності від оголошення стану війни та/або введення воєнного стану, що впливає і на питаннях захисту персональних даних громадян під час війни.

3. Діючі нормативно-правові акти у сфері захисту персональних даних не передбачають жодним чином особливостей правового регулювання питання захисту персональних даних громадян у період війни. У національному контексті

розбудови системи захисту персональних даних провідне значення мають відігравати нормативно-правові акти спрямовані на задоволення публічно-правових вимог щодо створення системи захисту персональних даних, їх баз у різних інформаційних сферах та «середовищах». Особливої актуальності це набуває у контексті діяльності Міністерства оборони України, Міністерства внутрішніх справ України, Служби безпеки України та інших відомств, службовці яких задіяні у військових діях.

4. Особливу групу суб'єктів, що потребують захисту їх персональних даних є військовослужбовці (комбатанти). В першу чергу мова йде про представників силових (мілітаризованих) структур (Збройних Сил України, Національної гвардії України, Служби Безпеки України, Національної поліції, Державної прикордонної служби України та інші). При цьому зазначену групу осіб, що потребують додаткових гарантій захисту їх персональних даних, необхідно розділити на підгрупи, залежно від того, де і як вони виконують свої службові обов'язки: представників силових (мілітаризованих) структур, які перебувають на дійсній службі; представників силових (мілітаризованих) структур, що знаходяться безпосередньо в зоні ведення бойових дій; особи, що перебувають на лікуванні у медичних закладах України та зарубіжних країн; особи, що перебувають у полоні; особи, що вважаються безвісно зниклими або загиблими.

5. У рекомендаціях для військовослужбовців запропоновано наступні способи захисту персональної інформації: блокувати пристрої щоразу, коли відходите від них, встановлювати повне шифрування на всі диски комп'ютера, встановити надійний пароль для входу в соціальну мережу, не заходити в акаунти соцмереж з незнайомих чи незахищених пристроїв, публікувати часткову або несправжню інформацію про себе (наприклад, зазначення в профілі Facebook місцем навчання військової інституції та участь у групі з конкретною та інші.

6. Проблема забезпечення захисту персональних даних органами публічної влади в умовах війни залишається винятково гострою. Важливою умовою

забезпечення захисту персональних даних громадян має бути контроль інформаційного середовища, що повинно покласти краї неконтрольованому розміщенню у соціальних мережах багаточисельних сторінок з фотографіями та відео українських полонених з їх персональними даними. Зазначені заходи носять явний акцент антиукраїнської пропаганди та є порушенням прав військовополонених у тому числі і у сфері захисту їх персональних даних.

Також, на нашу думку, для забезпечення захисту персональних даних військовослужбовців необхідно розробити окремі інформаційні реєстри згаданих нами вище категорій осіб з різним ступенем верифікації доступу до них та унормування можливості отримання інформації щодо суб'єктів, які внесені до цих баз даних або навпаки отримати інформації що у цих базах даних інформація щодо певних осіб відсутня. Зазначене має покласти краї неконтрольованому розміщенню у соціальних мережах багаточисельних сторінок з фотографіями та відео українських військових, військовополонених з їх персональними даними. Це дозволить запобігти порушенням прав військовослужбовців через несанкціонований доступ до їх персональних даних.

Також необхідно 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. Белова 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. Белова Ю.Д. Цивільні правовідносини щодо персональних даних. Хмельницький: ФОП Мельник А.А., 2019, 192 с.
5. Белова 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-voynnogo-stanu-263>. (дата звернення 30.05.2022 р.)
15. Дмитренко О. А. Право фізичної особи на 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](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. ІТ 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. ІТ 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](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](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](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.] ; Спільна 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. Кирилук О. Становление универсального международно-правового регулирования в сфере защиты персональных данных. *Leges 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-Х. 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](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://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 Україні : 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-poloneni-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-ХІІ. *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](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](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](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](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](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-privatne-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*. 29-30 квітня 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=ENM>
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#%7B%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-estoniyye-spl-vyslovyv-sya-shhodo-prava-v-yazniv-na-dostup-do-internetu/>

Виконав: студент магістратури

спеціальності 281 Публічне  
управління та адміністрування  
заочної форми навчання  
«\_\_\_» грудня 2022 р.

\_\_\_\_\_  
Підпис

Бондар Д. В.

\_\_\_\_\_  
Ініціали, прізвище

Науковий керівник  
кандидат наук з державного  
управління, доцент, доцент кафедри  
публічного управління та  
адміністрування  
«\_\_\_» грудня 2022 р.

\_\_\_\_\_  
Підпис

Баюк М. І.

\_\_\_\_\_  
Ініціали, прізвище

Робота допущена до захисту:

Завідувач кафедри публічного  
управління та адміністрування д.  
наук з держ. управління, доцент  
«\_\_\_» грудня 2022 р.

\_\_\_\_\_  
Підпис

Е.В. Щепанський

\_\_\_\_\_  
Ініціали, прізвище