

**Міністерство освіти і науки України
Західноукраїнський національний університет
Навчально-науковий інститут новітніх освітніх технологій**

Кафедра адміністративного права та судочинства

**МІЖДИСЦИПЛІНАРНА КУРСОВА РОБОТА
з дисципліни «Актуальні питання адміністративного права та процесу»
на тему «Захист персональних даних у сфері надання адміністративних
послуг: європейські стандарти та українська практика»**

Студент групи ПРзм-11:

Сопіга В. О.

Керівник: к.ю.н., доц. Вербіцька М.В.

Національна шкала _____

Кількість балів: _____ Оцінка: ECTS ____

Члени комісії _____

(підпис) (прізвище та ініціали)

ЗМІСТ

ВСТУП.....	3
РОЗДІЛ І. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ АДМІНІСТРАТИВНИХ ПОСЛУГ	5
1.1. Поняття та правова природа персональних даних.....	5
1.2. Поняття адміністративних послуг та їх цифровізація.....	8
1.3. Принципи захисту персональних даних.....	11
РОЗДІЛ 2. ЄВРОПЕЙСЬКІ СТАНДАРТИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ПУБЛІЧНИХ ПОСЛУГ	15
2.1. Регулювання персональних даних у праві Європейського Союзу.....	15
2.2. Інституційні механізми контролю у країнах ЄС.....	18
2.3. Практика застосування європейських стандартів у сфері електронних адміністративних послуг.....	22
РОЗДІЛ 3. УКРАЇНСЬКА ПРАКТИКА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ АДМІНІСТРАТИВНИХ ПОСЛУГ ТА ШЛЯХИ ЇЇ ВДОСКОНАЛЕННЯ.....	28
3.1. Нормативно-правове регулювання захисту персональних даних в Україні.....	28
3.2. Особливості обробки персональних даних у центрах надання адміністративних послуг.....	33
3.3. Проблемні аспекти та напрями гармонізації українського законодавства з правом ЄС.....	38
ВИСНОВКИ.....	45
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	47

ВСТУП

Актуальність теми. У сучасному світі інформаційних технологій персональні дані набувають особливої цінності, оскільки вони дозволяють ідентифікувати особу. Кожна особа, яка звертається за певними адміністративними послугами розраховує, що після отримання послуги, її персональні дані не будуть розкриті та не будуть використані у недобросовісних цілях. Практично будь-яка взаємодія із органами державної влади або органами місцевого самоврядування пов'язана із наданням та обробкою персональної інформації про особу.

Особлива увага припадає на сферу надання адміністративних послуг, де органи публічної влади здійснюють збір, обробку та використання персональної інформації про особу у межах своєї компетенції. У зв'язку з цим питання належного захисту персональних даних набуває особливої актуальності як з точки зору забезпечення прав людини, так і з точки зору належного функціонування органів публічної влади при наданні адміністративних послуг.

Захист персональних даних є однією зі складових права на повагу до честі та гідності особи, право на таємницю приватного та сімейного життя визнається одним із фундаментальних прав людини. У міжнародному праві це право отримало широке нормативне закріплення, зокрема у Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних зобов'язує кожну державу, яка є підписала і ратифікувала цей документ, забезпечення для кожної особи її основоположного права на недоторканість приватного життя. В українському середовищі захист персональних даних при наданні адміністративних послуг є особливо актуальним у контексті європейської інтеграції та вдосконалення законодавства до рівня законодавства Європейського Союзу.

У ході опрацювання цієї тематики варто відмітити, що в Україні існують нормативно-правові акти, які регулюють питання захисту персональних даних. Серед них однойменний Закон України «Про захист персональних даних», Закон

України «Про адміністративні послуги». Але хоч у нас є нормативне врегулювання цього питання але проблема належного рівня захисту цих даних досі лишається.

Метою дослідження виступають європейські стандарти у сфері захисту персональних даних, порівнянням із українськими стандартами, визначення проблем у тій сфері, а також визначення шляхів вирішення висвітлених питань.

Відповідно до зазначеної мети курсової роботи слід вирішити наступні **завдання:**

- розкрити поняття та правову природу персональних даних;
- з'ясувати суть поняття адміністративних послуг та їх цифровізації;
- охарактеризувати принципи захисту персональних даних;
- проаналізувати європейські стандарти захисту персональних даних у сфері публічних послуг;
- розглянути українську практику захисту персональних даних у сфері адміністративних послуг, а також знайти шляхи її вдосконалення.

Об'єктом дослідження є суспільні відносини у сфері захисту персональних даних при наданні адміністративних послуг виходячи із європейських стандартів та сучасному стані в Україні.

Предмет дослідження. Предметом дослідження у даній курсовій роботі є європейські стандарти та правове регулювання захисту персональних даних у національному законодавстві України.

РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ АДМІНІСТРАТИВНИХ ПОСЛУГ

1.1. Поняття та правова природа персональних даних

Доцільно розпочати із визначення поняття персональних даних та подальшого тлумачення.

В українському законодавстві, а саме: у статті 2 Закону України «Про захист персональних даних» зазначено таке поняття: «Персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована» [1]. До таких відомостей може бути віднесена будь-яка інформація, яка стосується фізичної особи, що прямо або опосередковано надає можливість її ідентифікувати серед інших осіб. До таких відомостей належать: прізвище, ім'я, по батькові фізичної особи, дата та місце народження, її адреса проживання, стан здоров'я, освіта та будь-яка інша інформація, що дозволяє ідентифікувати особу.

Також аналіз свідчить, що відповідно до рішення Конституційного Суду України від 20.01.2012 р. №2-рп/2012, - це інформація про особисте та сімейне життя (персональні дані про особу) [2].

У Законі України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» є деякі поняття, які у подальшому матимуть значення у даному дослідженні, а також допоможуть легше зрозуміти її зміст [3].

Ідентифікація – це комплекс заходів, які дають змогу виконати пошук за критерієм «один до багатьох», зіставляючи дані особи з інформацією наявною у реєстрах [3]. Верифікація особи – це порівняння даних, для встановлення тотожності особи документам або інформації, які наявні у реєстрах, для підтвердження ідентичності [3].

Будь-яка інформація, що стосується фізичної особи, дані про її майнові та/або немайнові відносини з іншими особами, зокрема з членами сім'ї, а також

будь-які відомості про події, що відбувалися або відбуваються у її побутовому, інтимному, професійному, товариському, діловому та інших сферах життєдіяльності, окрім сфери виконання особою функцій держави або органів місцевого самоврядування, відносяться до конфіденційної інформації. Таку інформацію може бути поширено за добровільною згодою особи, крім випадків, які визначені законом, і тільки в інтересах національної безпеки, економічного добробуту і захисту прав людини.

Перелік даних про фізичну особу, які можуть визначатися як конфіденційна інформація, не є вичерпним [4]. У Законі України «Про інформацію» є таке поняття як «інформація з обмеженим доступом». Її поділяють на конфіденційну, таємну та службову [5]. Серед видів інформації з обмеженим доступом нас цікавить саме конфіденційна інформація. Конфіденційною інформацією є дані про фізичну особу, доступ до якої обмежено. Така інформація може бути поширена за бажанням або добровільною згодою володільця такої інформації, тобто фізичної особи [6].

Конституція України, як Основний Закон держави та нормативно-правовий акт найвищої юридичної сили зазначає, що ніхто не може зазнавати втручання у його особисте і сімейне життя, окрім випадків, які передбачаються Конституцією України. Також Конституція України, не допускає збирання, зберігання, використання та поширення конфіденційної інформації про особу без її добровільної згоди. Також громадянам України дозволяється ознайомлюватися інформацією про себе, яка не є захищеною законом таємницею, у органах державної влади, органах місцевого самоврядування, установах та організаціях [7].

Кожному громадянину України гарантується судовий захист права на спростування недостовірної інформації про себе і про членів сім'ї, і також особа має право вимагати вилучення будь-якої інформації із подальшим відшкодуванням матеріальної та/або моральної шкоди. Стрімкий розвиток інформаційних технологій, їх запровадження у всі сфери нашої життєдіяльності, яка пов'язана із збільшенням обсягів опрацювання інформації, що стосуються

особи, призвело до розширення можливостей збирання, зберігання, обробки і використання персональних даних [8].

Отже, актуальною є необхідність визначити правову природу персональних даних фізичної особи. Розкривши її дозволить нам визначити механізм правового регулювання суспільних відносин, які пов'язані з обігом даних про фізичну особу. Проводячи аналіз правової природи персональних даних, взявши за основу думки науковців, дозволяє визначити поняття «правова природа» як сутність та властивість певного явища, його місце у системі права із урахуванням його специфічних ознак. Для розкриття поняття «правова природа» С. Алексєєв у своїх напрацюваннях визначає як юридичну характеристику цього явища, що дозволяє побачити структуру, місце і роль серед інших явищ з урахуванням його соціальної природи [9].

Схожа думка по визначенні правової природи надає І Матвєєв, який зазначає це поняття, як вичерпну характеристику явищу, факту, події. Але при цьому він зазначає, що «правову природу» варто розуміти як сутність, загальну характеристику чого-небудь [9].

Природу персональних даних фізичної особи науковці вважають, що краще розглядати у контексті публічного права. Слід зауважити, що виключно у контексті публічного права неможливо пояснити природу персональних даних, хоча у деякій мірі нам допоможе це зрозуміти [10].

Публічне право враховує той факт, що персональні дані фізичної особи – це правовий засіб індивідуалізації у спектрі правових відносин. Передумовою інституту персональних даних є необхідність індивідуалізації особи, як суб'єкта права, адже будь-яка особа є частиною соціуму, і не може бути єдиним володарем інформації про себе. Інформація про особу перебуває у постійному обігу у суспільстві в будь-якій формі. Її персоніфікація є передумовою для реалізації правосуб'єктності, і як наслідок, є умовою для вступу у суспільні відносини [9].

Виникнення персональних даних особи, як окремої категорії в інформаційному та національному праві пов'язане із потребою захисту

приватного життя, адже в умовах інформаційного суспільства воно піддається різним видам загроз.

Необхідність забезпечення належного рівня захисту особи від різних видів інформаційних загроз призвела до виникнення потреби контролю над оборотом інформації про фізичну особу, які ми називаємо «персональними даними», що у сучасному світі виділяються в особливу категорію інформації, яка потребує належного рівня захисту [11].

На даний момент право на захист інформації про приватне життя особи, як і необхідність поваги приватної, особистої сфери життя і право на захист інформації про фізичну особу (персональні дані) варто вважати невід’ємними права людини.

У Цивільному кодексі України (надалі – ЦК України) зазначається, що особисті немайнові права кожній особі належать від народження або за законом. Такі права тісно пов’язані з фізичною особою [12].

У цьому ж нормативно-правовому акті ще зазначається, що фізична особа визначає своє особисте життя та можливість ознайомлення з ним інших. Особа має право на збереження таємниці свого особистого життя. Така таємниця може бути розголошена за згодою особи [12].

1.2. Поняття адміністративних послуг та їх цифровізація

Доцільно цей підрозділ розпочати із визначення базових понять, які будуть у подальшому використовуватися.

Адміністративна послуга – це результат здійснення повноважень суб’єктом надання адміністративних послуг за заявою особи, яка спрямована на набуття, зміни чи припинення прав та/або здійснення обов’язків відповідно до закону [13]. У ЦК України зазначається, що послуга споживається у процесі вчинення певної дії, тому така діяльність не передбачає отримання конкретного продукту та/або результату [12]. Суб’єктом звернення є фізична або юридична особа, яка звертається за отриманням адміністративних послуг.

Суб'єктом надання адміністративних послуг виступає орган виконавчої влади або інший державний орган, орган місцевого самоврядування та /або їх посадові особи, які уповноважені надавати адміністративні послуги [13].

Адміністративні послуги не може надавати будь-хто, оскільки їх можуть надавати тільки суб'єкти, які наділені владними повноваженнями. Через активне введення системи автоматизованої обробки персональних даних особи була прийнята та країнами Європейського Союзу була підписана Конвенція «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних». Метою цієї Конвенції є захист і дотримання прав та основоположних свобод людини, і забезпечення її виконання на території країн, які підписали [14]. Цю Конвенцію підписала також Україна і згоду на обов'язковість була надана Верховною Радою України. Але варто зазначити, що адміністративна послуга є стандартизованою та уніфікованою, тобто така, яка надається усім однаково, хто звернувся по неї і має на це відповідне право [15].

Слід зазначити, що процес цифровізації адміністративних послуг в Україні активно розвивається у створенні електронних сервісів, онлайн-платформ та державних реєстрів для належної взаємодії громадян із державою. Важливим прикладом цифровізації сервісів та послуг в Україні є онлайн-платформа «Дія». Завдяки їй значно зменшився час отримання результату запиту, спрощено взаємодію із державними реєстрами, підвищило зручність для користувачів та зменшило корупційні ризики. Ця платформа активно розвивається і громадяни можуть отримати будь-які послуги знаходячись будь-де і в будь-який час, і має можливість переглядати все з смартфона.

Цифровізація послуг передбачає автоматизацію процесів обробки персональних даних, яка забезпечує швидке прийняття рішень, але і породжує нові ризики витоку даних. Процеси взаємодії з електронними реєстрами, систем ідентифікації і верифікації особи, обмін даними потребує належного рівня захисту [16]. У такому випадку особливу увагу набуває необхідність належного забезпечення захисту персональних даних при наданні адміністративних послуг. Обробка даних має відповідати принципам прозорості, законності, цільового

використання і мінімізації обсягу даних. У разі порушення цих принципів може спричинити несанкціонований доступ, неправомірному використанні або витоку персональної інформації [16].

Цифровізація даних передбачає сучасні механізми ідентифікації особи через електронний підпис, BankID, MobileID тощо. Ці способи забезпечують достовірну ідентифікацію особи і безпечний доступ до сервісів [17]. Тому цифровізація послуг є важливим етапом розвитку публічного управління, яка сприяє підвищенню ефективності діяльності органів та покращенню якості обслуговування.

Можна виділити наступні ознаки адміністративних послуг:

- 1) адміністративна послуга надається за наявності звернення особи;
- 2) надання адміністративних послуг пов'язане для забезпечення юридично значущих умов щодо реалізації прав конкретної особи;
- 3) адміністративні послуги надаються лише суб'єкти владних повноважень;
- 4) право на отримання адміністративної послуги та повноваження конкретного органу визначається лише законом;
- 5) результатом послуги є адміністративний акт – це рішення чи значуща дія адміністративного органу, яке задовольняє звернення особи [17].

Узагальнюючи вищевикладене можна зробити твердження, що адміністративні послуги – це публічні послуги, які надаються органами державної влади, органами місцевого самоврядування та/або їх посадовими особами, яке пов'язане із реалізацією владних повноважень.

Адміністративні послуги можна класифікувати за певними критеріями:

- 1) за рівнем встановлення повноважень та видом правового регулювання процедури:
 - адміністративні послуги із централізованим регулюванням (до них належить акти Кабінету Міністрів України);
 - адміністративні послуги із локальним регулюванням (до них відносяться акти органів місцевого самоврядування);

- адміністративні акти із «змішаним» регулюванням (це ті випадки, коли мають місце одночасне централізоване і локальне регулювання).

За критерієм платності: платні; безоплатні;

За змістом надання адміністративних послуг: реєстрація; надання дозволу; сертифікація; атестація; верифікація; легалізація; встановлення статусу тощо.

За характером питань, щодо яких звертаються особи: господарські послуги; соціальні послуги; земельні послуги; будівельно-комунальні послуги тощо [17].

Важливим для адміністративної послуги є якість його надання, який оцінюється за наступними критеріями:

- Результативність – це задоволення потреби особи в адміністративній послугі.
- Своєчасність – це надання послуги в установленій законодавством строк.
- Доступність – це фактична можливість особи звернутися за послугою.
- Зручність – це врахування інтересів та потреб отримувачів послуг.
- Відкритість – це безперешкодне одержання інформації, яка необхідна для отримання адміністративної послуги.
- Повага до особи – це ввічливе ставлення до особи.
- Професійність – це належний рівень кваліфікації працівників адміністративного органу [17].

Ті критерії у поєднанні дають можливість отримувати адміністративні послуги у повному обсязі, якісно та доступно.

1.3. Принципи захисту персональних даних

Принципи права – це загальні та стабільні засади, які сприяють утвердженню, забезпеченню та захисту суспільних цінностей, що виражають сутність права і визначають напрями його подальшого розвитку [18]. Кожна країна Європа і Україна вживають необхідних стосовно свого внутрішнього

законодавства, щоб у кожної держави набули чинності основні принципи у сфері захисту персональних даних.

Персональні дані, що підлягають автоматизованій обробці, повинні:

- 1) отримуватися і оброблятися сумлінно та законно;
- 2) зберігатися для визначених законом цілей і не використовувати у інший спосіб;
- 3) бути адекватними, відповідними і ненадмірними щодо цілей, для яких вони зберігаються;
- 4) бути точними і в разі потреби оновлюватися;
- 5) зберігатися у формі, що дозволяє ідентифікацію не довше, ніж це необхідно для цілей, задля якої вони зберігаються [14].

Персональні дані не можуть піддаватися автоматизованій обробці, якщо внутрішнє законодавство держави не забезпечує належний захист таких даних і не надає відповідних гарантій [19].

Файли, що містять відомості про персональні дані, які у подальшому підлягають автоматизованій обробці, державою уживаються заходи безпеки, щодо запобігання випадковому чи несанкціонованому знищенню, втраті або доступу, зміні і поширенні [20].

У статті 6 Закону України «Про захист персональних даних» зазначено, що метою обробки персональних даних має бути чітко сформульована у законах, інших нормативно-правових актах, які регулюють діяльність органів, які обробляють персональні дані. Це саме та норма, яка була закріплена у нашому законодавстві саме через вимоги Конвенції, яка згадувалася вище [1].

Обробка персональних даних має здійснюватися відкрито і прозоро, щоб особа могла відстежувати кожен крок цієї процедури. У разі зміни мети обробки персональних даних, то володілець (орган, який займається обробкою таких даних) має отримати згоду від суб'єкта персональних даних [14].

Персональні дані повинні бути точними, достовірними та оновлюватися в міру потреби. Законодавством передбачене обмеження щодо обробки персональних даних особи, які є конфіденційною інформацією, без її згоди,

окрім випадків, визначені законодавством і тільки в інтересах національної безпеки, економічного добробуту та прав людини. Але є також виняток, що обробляти персональні дані особи без згоди особи допускається для захисту важливих інтересів суб'єкта персональних даних до моменту, коли отримання згоди буде можливим. Персональні дані обробляються у формі, що надає можливість ідентифікації та не довше, ніж це необхідно [21].

З точки зору інформаційного права науковці виділяють наступні:

- 1) свободу отримання та поширення інформації;
- 2) об'єктивність, вірогідність, повноту і точність інформації;
- 3) гармонізація інтересів особи, суспільства і держави;
- 4) мінімізація негативного впливу;
- 5) мінімізація негативних наслідків;
- 6) недопущення несанкціонованого доступу до персональних даних;
- 7) приналежність інформації до цивільних правовідносин та її вільний обіг;
- 8) єдність та різниця інформації і її носія;
- 9) об'єктивність надання інформації;
- 10) первинність створення інформації;
- 11) обмеження доступу до інформації [18].

Виходячи із вищесказаного можна виділити основоположні принципи, які загальними і необхідними у діяльності, які пов'язані із обробкою персональних даних.

Принцип законності і справедливості. Обробка персональних даних має відбуватися лише на підставі закону і у тій мірі, яка є необхідною для встановлення потрібної інформації. Будь-яке безпідставне і незаконне отримання конфіденційної інформації стосовно особи є недопустимим і як наслідок є підставою притягнення винних до юридичної відповідальності [18].

Принцип точності актуальних даних означає, що інформація про особу мають бути актуальними на момент їх обробки і підтримуватися у такому стані постійно.

Принципи чесності. Є доповненням до попереднього принципу. Застосовується в основному під час обробки персональних даних. Володілець таких даних зобов'язаний у повній мірі проінформувати суб'єкта персональних даних щодо процедури обробки, прозорості та відповідно до правил захисту таких даних [18].

Принцип прозорості. Насамперед означає, що володілець персональних даних має вчиняти усіх необхідні дії, щоб суб'єкти таких даних чітко розумів для чого виконується кожна дія. Прозорість має бути присутня на кожній стадії обробки, адже кожна стадія взаємопов'язана і вимагають, щоб суб'єкт персональних даних були впевнені та повідомленні про інформацію, що може бути доступна [18].

Принцип обмеження мети. Цей принцип тісно пов'язаний із попереднім, оскільки він передбачає чітку мету обробки даних, і за межі цієї мети володілець не має права вийти без згоди суб'єкта персональних даних.

Принцип мінімізації. Означає, що для надання послуги необхідно зібрати мінімально даних про особу і такий обсяг є адекватним і достатнім для досягнення мети. Але обсяг необхідних даних і встановлена мета мають бути співрозмірними у кожній конкретній ситуації [18].

Отже, принципи є основоположними засадами щодо обробки персональних даних і їх дотримання визначає наскільки якісно, результативно та у повній мірі буде надана адміністративна послуга та надійно будуть захищені персональні дані, які були об'єктами під час обробки.

РОЗДІЛ 2. ЄВРОПЕЙСЬКІ СТАНДАРТИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ПУБЛІЧНИХ ПОСЛУГ

2.1. Регулювання персональних даних у праві Європейського Союзу

У країнах Європейського Союзу закріплена загальна норма, що кожен має право на повагу до свого приватного та сімейного життя, свого життя і кореспонденції [22]. Органи державної влади не можуть безпідставно втручатися у приватне життя особи, окрім випадків, коли таке втручання здійснюється із необхідності і на підставі закону в інтересах національної, громадської безпеки, економічного добробуту, для запобігання вчиненню злочинів, а також такі дії спрямовані на захист здоров'я чи моралі, прав і свобод інших осіб. Забороняється безпідставне втручання у особисте і сімейне життя особи, посягання на недоторканість житла, таємницю кореспонденції та його честі і репутації. Кожна людина має право на захист від незаконних посягань [23].

Також зазначу, що Рада Європи була заснована після Другої світової війни з метою ствердження верховенства права, демократії, прав людини, соціального розвитку і єднання європейських держав. Одним із перших документів, яка була прийнята Радою Європи була Конвенція про захист прав людини і основоположних свобод у 1950 році, яка набула чинності у 1953 році. Кожна держава, яка підписує цю Конвенцію має в обов'язковому порядку її дотримуватися і вносити відповіді зміни у національне законодавство.

Для реалізації виконання Конвенції державами, які підписали дану її у 1959 році в місті Страсбург (Франція) був заснований Європейський Суд з прав людини. І щоб кожна людина, чи держава могла звернутися до ЄСПЛ, то ця Конвенція має бути підписана і ратифікована у тій державі. Право на захист персональних даних є частиною статті 8 Конвенції, яка гарантує право на повагу до приватного та сімейного життя, і визначає умови, за яких допускаються у реалізації цього права [22].

Одним із показників захисту персональних даних є те, що ЄСПЛ, з моменту свого створення, розглянув велику кількість справ, що стосуються персональних даних. Це нам говорить про те, що ідеального захисту даних немає, але країни Європи активно над цим працюють і вдосконалюються. І ще говорить нам про те, що захистити порушення своїх прав у сфері обробки персональних даних можливо. В основу законодавства країн Європи лежать договори Європейського Союзу. І всі ці договори лежать в основі національного законодавства держав ЄС. Усі регламенти, директиви та рішення ЄС ухвалюються уповноваженими і їх часто називають вторинним законодавством ЄС. Одним із основних нормативно-правових актів Європейського Союзу у сфері захисту персональних даних є Директива 95/46/ЄС Європейського парламенту та Ради Європи від 24 жовтня 1995 року «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних». Вона була прийнята для врегулювання питання, коли внутрішній ринок вимагав вільного потоку таких даних, який неможливо було зробити, поки держави не розрахували однаково високий рівень захисту персональних даних [20].

Система обробки персональних даних повинна поважати права і свободи людини, особливо право на невтручання у приватне та сімейне життя, а також сприяти економічному та соціальному прогресу. Також обробка персональних даних мають бути достатньо захищеними, щоб полегшити необхідний транскордонний потік інформації про особу [16].

У разі недотримання вимог щодо захисту таких даних може призвести до повільнішого економічного та соціального розвитку держав. Держави ЄС мають забезпечити однаковий захист даних про особу, так як зближення національних законодавств країн створює полегшену процедуру потоку персональних даних. Полегшена процедура обігу таких даних створює умови для економічного та соціального розвитку держав ЄС [21].

Особливе місце у законодавстві країн Європи в сфері обробки персональних даних посідає Конвенція Ради Європи від 28 січня 1981 р. «Про захист фізичних осіб у зв'язку із автоматизованою обробкою персональних

даних». Вищезгадана Директива прийнята на основі цієї Конвенції і посилює основні принципи, які викладені у ній [14].

Принцип захисту персональних даних мають застосовуватися до всіх випадків здійснення обробки персональних даних особи. Тобто, гарантії належного захисту даних має бути забезпечено у будь-якій діяльності, що мають відношення до обробки таких даних. Принцип захисту даних не поширюється у випадку, якщо вони створенні фізичною особою винятково особистого чи домашнього характеру, наприклад, переписування телефонної книги у смартфоні. У зв'язку із розвитком інформаційних технологій, які використовуються для прийому, передачі, реєстрації, збереженні, збиранні та іншим подібним діям, які стосуються обробки персональних даних, Директива 95/46/ЄС повинна бути застосована у кожному такому випадку, що стосується обробки даних [20].

Ще одним актом, який регулює сферу захисту персональних даних є Загальний регламент про захист даних (з англійської General Data Protection Regulation, скорочено – GDPR – під цим скороченням буде згадуватися у подальшому в курсовій роботі) – це нормативно-правовий акт, який оновлює законодавство Європейського Союзу в сфері захисту персональних даних, а також замінює Закон про захист даних від 1998 року. Тобто після спливу дворічного перехідного періоду. У GDPR внесенні зміни, щодо вдосконалення конфіденційності даних, які є складовою права на невтручання у приватне та сімейне життя особи [24].

Також цей документ є важливою складовою статті 8 Хартії основних прав Європейського Союзу, який також стосується обігу персональних даних, що покликаний спростити регулювання середовища їх обігу. Регламент вносить удосконалення до Директиви щодо опрацювання інформації про особу усередині країн Європи.

2.2. Інституційні механізми контролю у країнах ЄС

GDPR вводить однакові норми та стандарти в обробці персональних даних країнами Європи. Слід зазначити, що цей нормативно-правовий акт прийнятий у формі регламенту, адже така форма має пряму дію у країнах Європи. Уточнення, додаткові тлумачення по ньому допускаються вже на рівні національного законодавства [19]. Ще цей документ гарантує право на належну обробку та захист персональних даних особи і поза межами території країн Європи для осіб, чії дані обробляються. Регламент вводить низку нових термінів, серед яких є, контролер, оператор персональних даних та суб'єкт даних.

Для подальшого аналізу необхідно з'ясувати їхній зміст. Суб'єкт даних – це фізична особа, персональні дані якої підлягають обробці. Контролер – це фізична або юридична особа, які самостійно або спільно з іншими визначають цілі і засоби опрацювання персональних даних. Тобто, це суб'єкти, які визначають цілі обробки персональних даних [19]. Оператор – це суб'єкт, який здійснює безпосередню обробку персональних даних або за дорученням контролера [19].

Регламентом передбачається низка вимог щодо обробки та захисту персональних даних. Особливо це стосується контролера та оператора, які безпосередньо здійснюють таку діяльність. Перед початком обробки персональних даних контролер проводить аналіз, зокрема він з'ясовує обсяг інформації та джерело надходження. Адже Регламентом заборонено збирати більше інформації, аніж це необхідно для досягнення мети.

Після з'ясування обсягу і джерела інформації, контролер здійснює низку організаційних заходів для забезпечення належного захисту даних. Також контролер визначає коло осіб, яким доводить умови поводження з даними, і як правило, з ними укладається угода про нерозголошення даних [25].

Регламентом передбачено вичерпний перелік випадків, за яких в обов'язковому порядку має бути призначено співробітника з питань захисту даних. До таких умов належать:

- 1) якщо контролер даних належить до органів публічної влади, окрім суддів;
- 2) якщо контролер здійснює регулярний, систематичний та масштабний моніторинг суб'єктів даних, у силу специфіки своєї діяльності;
- 3) якщо контролер здійснює обробку даних, які відносяться до категорії «чутливих» (стан здоров'я, судимість, сімейні зв'язки тощо) [19].

Співробітник з питань захисту даних зобов'язаний надавати рекомендації контролеру або оператору та працівникам, які здійснюють обробку даних і здійснювати моніторинг щодо захисту таких відомостей. Такого співробітника може бути обрано як із числа працівника контролера, так із залучених осіб на умовах цивільно-правового договору [25].

Регламентом гарантовано забезпечення належного рівня захисту у серверах зберігання даних, способів доступу до них, запровадження належної системи верифікації у разі здійснення доступу.

Також обов'язковою вимогою до оператора є забезпечення рівня захисту даних не нижче, аніж обумовлений та гарантується контролером по відношенні до відповідного суб'єкта. Тобто, щоб здійснити обробку даних без порушень та у відповідності до Регламенту, суб'єктам, які здійснюють таку діяльність необхідно вжити багато організаційних заходів. Але навіть дотримання вищевказаних вимог, не є визначальним для законності обробки персональних даних, бо головною умовою є отримання згоди від суб'єкта даних [25].

Але у цьому питанні Регламент також ввів низку нововведень. Згода має бути прямою та активною. Тобто не тільки підтвердження, а й її надання у кожному конкретному випадку. Згода надається у формі погодження з повідомлення про обробку персональних даних. Така згода зазвичай надається у письмовій формі, а також в інший спосіб, у тому числі, за потреби, електронним способом. У випадку надання запиту суб'єктом даних, інформацію може бути надано усно за умови, що особу суб'єкта встановлено іншими засобами. Повідомлення має бути простим, доступним та зрозумілим. Але попри те, що згода суб'єкта даних є підставою для обробки відомостей про нього, але така

згода не може бути правовою підставою для обробки даних у діяльності правоохоронних і судових органів.

У відповідності до принципу законності, обробка даних має здійснюватися на підставі правового акту, який має відповідати підставам, визначених чинним законодавством. Така обробка може здійснюватися лише у зв'язку з виконанням конкретних завдань [19]. Дотримання Регламенту забезпечується системою штрафів у розмірах, який залежить від кожного конкретного випадку. Таке накладення має бути дієвим, пропорційним та стримувальним.

Також до критеріїв накладення штрафу відноситься: специфіка, ступінь тяжкості, тривалість правопорушення, обсяг та ціль відповідної обробки даних, а також кількість суб'єктів, які зазнали впливу, умисний чи необережний характер, будь-які дії, які були вжиті контролером або оператором для зниження рівня шкоди і відновлення захисту, категорії персональних даних, тощо [25].

Розмір штрафу може бути встановлений у чіткому розмірі, або у відсотковому відношенні від загального доходу, якщо мова йдеться про підприємство, враховуючи дохід за попередній фінансовий рік, та у залежності від того, яка сума буде вищою.

Вбачається за доцільне розглянути застосування Регламенту та перші випадки порушення порядку поводження з персональними даними.

Австрія. У вересні 2018 року Data Protection Authority наклав штраф на одне із підприємств за порушення вимог Регламенту. Порушення полягало у тому, що на фасаді приміщення було розташовано відеокамеру, яка охоплювала вхід у підприємство та значну частину тротуару. Її не було позначено належним чином, через що було порушено принцип прозорості збору даних. Не було б порушенням, якби перехожі знали про наявність відеокамери. Як результат на порушника було накладено 5280 євро [24].

Португалія. Першим порушником GDPR став один із медичних закладів. Контролюючий орган встановив відразу 3 порушення Регламенту зі сторони лікувального закладу. Перше порушення стосувалося статті 5 Регламенту, а саме: до персональних даних мали доступ надмірна кількість працівників персоналу, а

також збирали та опрацьовували велику кількість відомостей про осіб і які не мали необхідності для конкретних цілей, що було порушенням принципу «мінімізації даних». Внаслідок цього було медичний заклад було оштрафовано на 150000 євро. Порушення цілісності та конфіденційності даних було ще одним у результаті незастосування організаційних та технічних заходів для запобігання незаконному доступу до відомостей пацієнтів, через що штраф склав ще 150000 євро. Останнім порушенням щодо медичного закладу стало те, що система зберігання та обробки даних не забезпечувала належний рівень захисту. Через що загальна сума штрафу за всі три порушення склала 400000 євро, яка контролюючим органом була оцінена як пропорційна і співрозмірна через врахування характеру інформації [24].

Франція. Французький регулятор – National Commission on Information and Liberty (Національна комісія з питань інформатики та свободи, CNIL – у січні 2019 року притягнув до відповідальності корпорацію Google за порушення вимог GDPR. До французького регулятора надійшла групова скарга про те, що корпорацію Google здійснює збір та обробку персональних даних, не маючи на це правових підстав, для здійснення персоналізованої реклами. У рамках розслідування французький регулятор прийняв новий рамковий документ, який довів до всіх країн Європейського Союзу, був належним чином розтлумачений та після цього внесли у вигляді змін до Регламенту. У подальшому розслідуванні було проаналізовано навігацію та документів користувача до яких Google отримує доступ [26].

Регулятором було виявлено наступні порушення:

1) порушення зобов'язання, що стосується прозорості та поінформованості, тобто інформація не є легкодоступною для перехожого користувача, а особливо така важлива інформація як: мета обробки інформації, період зберігання, категорії даних, що використовуються, потребують 5-6 кроків, щоб ознайомитися із цими документами. Але більше того, деяка інформація є недостатньо чіткою та незрозумілою для користувача;

2) відсутня правова підстава для персоналізації реклами корпорацією Google, але регулятор пояснив причину такої відсутності, а саме: недостатня поінформованість користувачів та не має ознак конкретної чи однозначної згоди на обробку даних. Як наслідок, Google було оштрафовано на 50 млн. євро[20].

Сфера захисту персональних даних у країнах Європейського Союзу та її правове регулювання зазнала значних змін після впровадження Регламенту Європейського Парламенту і Ради ЄС №2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку із опрацюванням персональних даних і про вільний рух таких даних – GDPR [19].

Регламент має екстериторіальну дію, через що суттєвих змін зазнає і процедура обробки персональних даних поза межами країн Європи. При здійсненні обробки даних потрібно дотримуватися принципів пропорційності, що стосується кількості даних відповідно до мети, часу зберігання, а також кількості осіб, які мають доступ до цих даних.

Також важливим є момент забезпечення захисту окремих даних, які віднесені до категорії «чутливих». Одним із ключових моментів є реалізація механізму прозорості обробки даних, що включає у себе допуск особи до ознайомлення з усіма операціями щодо відомостей про неї.

2.3. Практика застосування європейських стандартів у сфері електронних адміністративних послуг

У сфері цифрової трансформації адміністративних послуг досвід ЄС є важливим, адже він нам демонструє ефективні підходи для підвищення прозорості та ефективності державного управління. Вивчення європейської практики допомагає вдосконалити цифрові послуги в інших державах, які також прагнуть модернізувати адміністративні системи [16].

У цьому підрозділі метою дослідження буде узагальнення та аналіз досвіду ЄС у сфері цифрових технологій, які призначені для надання адміністративних

послуг. Основними напрямками підтримки ЄС у процесі модернізації та ефективного використання цифрових технологій в Україні є:

- 1) розвиток електронного урядування;
- 2) розбудова мережі центрів надання адміністративних послуг;
- 3) розвиток електронної ідентифікації;
- 4) підвищення цифрової грамотності [27].

У 2024 році адміністративні послуги розглядаються з точки зору комунікації між владою та суспільством. Співпраця ЄС та України у цій сфері може сприяти підвищенню якості та ефективності державного управління і задоволенню потреб громадян. Така співпраця також допомагатиме у підвищенні цифрової грамотності населення і створення зручних сервісів для громадян, що як наслідок покращить економічний добробут країни [28].

З попередніх підрозділів нам відомо, що принципи прозорості, відкритості і підзвітності у країнах ЄС є обов'язковими умовами роботи державних інститутів. Також створена нормативна база, розроблені програми та концепції щодо забезпечення стандартів якості надання таких послуг.

У країнах Європи надання послуг є дуже важливим, оскільки про це свідчить регулювання цієї сфери первинним (є загальним для всіх країн ЄС) і вторинним (на рівні національного) законодавством. І про це також свідчать попередні підрозділи. Однією з необхідних умов для того, щоб обмін послугами підпав під юрисдикцію ЄС, є існування факту перетину державного кордону однієї з країн Європи [28].

Також значну роль у регулюванні сфери послуг відіграє Суд ЄС, оскільки його рішення мають вплив на загальноекономічні інтереси. Але рішення досягаються на індивідуальній основі, адже враховуються умови і національні особливості кожної країни Європи. Суд ЄС – це вища судова інстанція Європейського Союзу, оскільки забезпечує дотримання права при тлумаченні і застосуванні договорів ЄС. У ЄС належне адміністрування включає у себе неупередженість, справедливість та розумний строк, право бути вислуханим, а також доступ до матеріалів справи і обов'язок адміністрації мотивувати своє

рішення. Водночас до цих критеріїв слід додати, що процедура є частиною послуги, тому її якість є важливим компонентом у сфері адміністрування [29]. Співвідношення принципів надання адміністративних послуг з принципами адміністративної процедури та із загальними принципами належного врядування варто розглядати як узгоджену систему, яка доповнює одне одну [28].

Загальні принципи врядування встановлюють стандарт легітимності адміністрування. Принципи адміністративної процедури конкретизують ті стандарти у процесуальних діях. Принципи надання адміністративних послуг виступають доповнення до сфери адміністрування і носять сервісний характер – доступність, зручність, мінімізації документів, інформації та дій як умови реалізації права на звернення громадян і отримання результату по зверненні.

Розглянемо приклад законодавчого закріплення та реалізації принципів адміністрування у деяких країнах Європи.

Німеччина. Ключові гарантії належного надання послуги закріпленні у законодавстві як обов'язок із наданням можливості бути вислуханим перед видачою адміністративного акта, а також його мотивувати у письмовому чи електронному вигляді із викладенням істотних і правових підстав [28].

Франція. Принципи сервісної держави вбудовані у законодавство шляхом реалізації права електронного звернення до адміністрації після ідентифікації особи, а також через вимогу мотивування індивідуальних несприятливих рішень.

Польща. Загальні принципи адміністрування закріплені у Кодексі адміністративного провадження як вимога діяти органам на підставі права і як обов'язок бути на сторожі правопорядку та вживати всі необхідні дії для точного, повного і всебічного з'ясування фактичного стану. При з'ясуванні стану органи мають посилатися на суспільний інтерес та слушний інтерес громадян, який у сфері послуг дисциплінує як людський, так і цифровий компонент рішення [28].

Принципи надання адміністративних послуг слід розглядати як нормативні вимоги, через які органи публічної влади формує юридично значущі результати для громадян [17].

З цієї точки зору принципи працюють так, щоб визначати, хто має право діяти та в яких межах, які шляхи досягнення результату, форма та юридичний спосіб закріплення результату, спосіб пояснення адресатові і контролюючим органам, а також строки та способи оскарження, перевірки і перегляду рішень. Такий підхід до розуміння принципів адміністрування слід розуміти як реальний критерій якості дій органів публічної влади, а не як рекомендацію. В українському законодавстві принципи адміністрування становлять вимоги до якості надання послуг на кожному етапі процедури, а не у загальному.

У порівнянні такий підхід є сумісним із європейськими стандартами щодо належного адміністрування, що перетворює принципи на вимоги до кожного етапу процедури надання адміністративних послуг. Взаємодія з державними електронними інформаційними ресурсами створює передумови щодо реалізації принципу мінімізації документів, а режим електронної ідентифікації особи та системи довірчих послуг створює умови для легітимного доступу без знецінення захисту персональних даних. У Німеччині та Франції проявляється як нормативно врегульований перехід до електронних каналів зі збереженням гарантій захисту даних. Етапи розгляду і ухвалення рішення нам показує, що принципи адміністрування повинні бути включенні як критерії якості надання послуг. Також ці принципи вимагають, щоб було дотримано справедливості та неупередженості від адміністрації, що включає у себе однакові підходи до однакових фактів. Своєчасність вимагає управління строками як юридичного обов'язку. Захист персональних даних нам показує легітимність доступу до речових відомостей і пропорційності їх обробки [17].

У епоху цифровізації послуг додається принцип прозорості при автоматизованій обробці даних, який дає можливість пояснити, які дані були використані при автоматичній обробці, які умови спрацьовують, як і на підставі чого сформований результат.

Завершальний етап дозволяє нам побачити, що принципи виконують не комунікаційну, а юридичну функцію, оскільки прозорість і доступність інформації означають, що особа повинна отримати результат свого звернення у

формі, що дозволяє зрозуміти його зміст, правові наслідки і підстави та способи оскарження. Юридична визначеність та підзвітність означає, що вся процедура рішення має бути відтворена у разі виникнення спору. Захист персональних даних означають, що доступ до результату і відомостей про особу не можуть створювати загрози їхнього витоку [17].

Цифрова трансформація виступає як своєрідний тест принципів надання адміністративних послуг зводиться до того, що процесу цифровізації надає можливість пришвидшити сервіси, але й одночасно розкриває ті місця, де принципи повинні працювати не як декларація, а як юридично встановлений стандарт. Але навіть перенесення адміністративних послуг у цифрове середовище не позбавляють їх автентичності відносно паперовим. Отримані результати мають також містити зрозумілі для особи підстави, мати ефективний контроль та можливість виправлення [16].

Перейдемо до практики європейських країн щодо електронного звернення громадян по адміністративні послуги.

Франція. Право електронного звернення громадян до адміністрації здійснюється після попередньої ідентифікації особи, яка поєднується із вимогою, щоб адміністрація була належним чином повідомлена та не вимагала дублювання звернення іншою формою [16].

Німеччина. Обов'язок онлайн-доступу до адміністративних послуг перетворює доступність із політичного орієнтира на юридичний стандарт, яка передбачає чітку і прозору організацію надання послуг [16].

Польща. Доцільно навести визначення поняття «Інтероперабельність», що означає можливість різних інформаційних систем взаємодіяти між собою для обміну даними, належним чином їх використовувати без додаткових перешкод. У правовому значенні це означає належну взаємодію систем і реєстрів як умову коректного обміну даними і як передумову відтворення підстав для винесення рішення [16].

Отже, цифрова держава надає дані замість довідок тільки за умови, що правовий режим реєстрових відомостей належним чином забезпечує їх

цілісність, зрозумілий порядок виправлення, та відстежуваність змін. Водночас кіберстійкість у наданні цифрових послуг є не тільки технічною умовою, а й юридичним критерієм, щоб забезпечує конфіденційність, цілісність та доступність даних. Регламент ЄС 2024/1183 демонструє запровадження Європейського гаманця цифрової ідентичності, який підкреслює контроль користувача і надає доступ до сервісів. Такий доступ побудований на режимі довіри та безпеки щодо своїх даних.

Паралельно Директива 2022/2555 від 14.12.2022 р. закріплює рамку управління кіберризиками й відповідальності за ризик-менеджмент, яка збігається з вимогою юридично встановленої надійності цифрових сервісів. Цифрова послуга є правовою підставою лише у тій мірі, наскільки вона здатна правомірно помилятися та виправлятися. Але якщо процедура опирається на реєстрові дані, то принцип справедливості юридичної визначеності, неупередженості та підзвітності вимагають чітких і зрозумілих маршрутів для коригування як технічно (шляхом внесення змін), так і юридично (шляхом перегляду результату) [30].

РОЗДІЛ 3. УКРАЇНСЬКА ПРАКТИКА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ АДМІНІСТРАТИВНИХ ПОСЛУГ ТА ШЛЯХИ ЇЇ ВДОСКОНАЛЕННЯ

3.1. Нормативно-правове регулювання захисту персональних даних в Україні

Нормативно-правове регулювання суспільних відносин – це організаційно-упорядкований, результативний вплив системи правових засобів. У сфері захисту персональних даних та надання адміністративних послуг це слід розуміти як систему нормативно-правових актів, які регулюють суспільні відносини у цій сфері.

Законодавче забезпечення захисту персональних даних та надання адміністративних послуг в Україні складають Конституція України, Закони України «Про інформацію», «Про захист персональних даних», «Про адміністративні процедури», «Про адміністративні послуги», «Про звернення громадян», рішення Конституційного Суду України, міжнародні акти тощо [1].

Відповідно до правової позиції у рішенні Конституційного Суду України №5-зп від 30.10.1997 р. у справі Устименка К. Г. зазначено, що забороняється не лише збирання, але й зберігання, використання та поширення конфіденційної інформації. Також у цьому рішенні зазначено, що іноземці та особи без громадянства користуються національним режимом захисту своїх прав [31].

У статті 32 Конституції України ніхто не може зазнавати втручання в особисте і сімейне життя, окрім випадків, які передбачені Конституцією України. Також не допускається збирання, зберігання, використання і поширення конфіденційної інформації щодо особи без її згоди. Кожній особі гарантується судовий захист права щодо спростування недостовірної інформації про себе та про членів сім'ї, і ще особа має право вимагати вилучення будь-якої інформації та подальше відшкодування матеріальної та/або моральної шкоди, яка була завдана [7].

Вільний обмін інформацією та новітні технології полегшують процеси обробки персональних даних, але й одночасно створюють додаткові загрози несанкціонованого доступу. Щоб врегулювати питання захисту персональних даних Верховною Радою України було прийнято однойменний Закон «Про захист персональних даних». У цьому Законі були визначені правові засади забезпечення захисту даних, що стало першим кроком для розбудови системи захисту персональних відомостей про особу в Україні.

Аналіз свідчить, що статтею 3 Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних країнам Європи надано змогу обмежити сферу застосування до певних категорій відомостей. Але у цьому питанні український законодавець пішов іншим шляхом і поширив дію національного законодавства про захист персональних даних на всі види діяльності, які пов'язані зі створенням бази відомостей про особу та їх обробку. Винятком є діяльність фізичної особи, яка здійснює обробку особистих даних для власних потреб [14].

Загальні положення Закону України «Про захист персональних даних» визначають сферу застосування в будь-якій області суспільного життя пов'язане з обробкою персональних даних в органах державної влади та органах місцевого самоврядування, установах, організаціях усіх форм власності [1]. Вважаємо за доцільне Закон України «Про захист персональних даних» доповнити принципами обробки персональних даних з урахуванням досвіду європейських держав і також з врахуванням наявних принципів: законності, обмеження використання даних, індивідуальної участі тощо.

У Кодексі законів про працю України не встановлено норм щодо захисту персональних даних працівника, через що це питання там досі не врегульоване. Але у проєкті Трудового кодексу України вже врегульовані деякі питання, що пов'язані із захистом персональних даних, а саме: встановлено заборону роботодавцю надавати іншим особам інформацію про причини звільнення, відомості про оплату праці віднесені до конфіденційної інформації, визначено відповідальність роботодавця у разі заподіяння моральної шкоди, у тому числі

пов'язаного із невиконанням обов'язку щодо шанування честі, гідності та інших особистих прав працівника [32].

У статті 25 Закону України «Про захист персональних даних» встановлено обмеження щодо обробки персональних даних. У ній зазначається, що обробка може здійснюватися настільки, наскільки це необхідно у демократичному суспільстві в інтересах національної безпеки, економічного добробуту або захисту прав і свобод людини. У частині статті 19 Конституції України встановлено, що органи державної влади та органи місцевого самоврядування зобов'язані діяти лише в межах повноважень, які встановлено Конституцією та законами України [1; 7].

Під час дії правового режиму воєнного стану підставами для обробки персональних даних, у відповідності вищезгаданого Закону, є:

- 1) дозвіл на обробку персональних даних, який наданий володільцю на підставах Закону;

- 2) необхідністю виконання обов'язків володільця персональних даних [33].

Але одночасно заборонено здійснювати обробку відомостей про особу, які віднесені до категорії «чутливих». Слід доповнити, що вищезгаданий Закон прийнятий задля реалізації права на невтручання в особисте та/або сімейне життя у процесі обробки персональних даних. Також він поширюється на діяльність обробки даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів [1].

Закон України «Про доступ до публічної інформації» забезпечує право кожного на доступ до інформації, яка знаходиться у володінні суб'єкта владних повноважень та/або інших розпорядників інформації [34].

Публічна інформація – це зафіксована будь-якими засобами на будь-яких носіях інформація, яка була створена або отримана у процесі виконання владних повноважень таким суб'єктом [34].

Метою цього Закону є забезпечення належної прозорості та відкритості суб'єктів владних повноважень, а також створення механізмів реалізації права

щодо доступу до публічної інформації. Але цей Закон не поширюється на відносини, які пов'язані із зверненням громадян та регулюється іншим Законом.

У цьому Законі зазначено, що публічна інформація, яка містить персональні відомості про особу, може бути оприлюднена і надаватися на запит у формі відкритих даних з додержанням однієї із наступних вимог:

- 1) персональні дані знеособлені та захищені;
- 2) суб'єкт даних надав згоду на поширення таких даних;
- 3) надання чи оприлюднення такої інформації здійснюється на підставі Закону;
- 4) обмеження доступу до такої інформації заборонено Законом [34].

Також у вищезгаданому Законі зазначено, що посадові та службові особи не несуть юридичної відповідальності за не розголошення інформації про правопорушення або про відомості, що стосуються серйозної загрози здоров'ю чи безпеці громадян, якщо при цьому особа керувалася добрими намірами і мала обґрунтування, що інформація є достовірною.

Закон України «Про звернення громадян» регулює питання та визначає процедуру реалізації громадянами України у відповідності до наданого Конституцією України права звертатися до органів державної влади, органів місцевого самоврядування, їх посадових осіб із пропозиціями та скаргами. Це забезпечує можливість громадян брати участь в управлінні державними та громадськими справами [35]. Письмові звернення, у яких не зазначено місця проживання, не підписане автором, а також таке, у якому неможливо встановити авторство, визнаються як анонімні і не підлягають подальшому розгляду. Також не підлягають розгляду повторні звернення, по тому самому питанню і до того ж самого органу [35].

Розголошення відомостей про особисте життя громадян без їх згоди, чи відомостей, які становлять державну або іншу таємницю, які стали відомі із звернення не допускається. Також не допускається з'ясування додаткових даних про особу, які не стосуються звернення. Така заборона не поширюється на випадки повідомлення інформації, які містяться у зверненні, особам, що мають

відношення до вирішення справи. За порушення цієї вимоги, винні у цьому особи несуть передбачену законодавством юридичну відповідальність.

У разі прийняття неправомірного рішення щодо звернення громадянина, винні особи відшкодовують завдані матеріальні збитки. Спори про стягнення витрат розглядаються у судовому порядку. Також на вимогу громадянина, може бути відшкодована моральна шкода [35]. У випадку подання звернення, яке містить наклеп, образи, дискредитацію органів державної влади, органів місцевого самоврядування, заклик до ворожнечі на будь-якому ґрунті, та інших дій, тягнуть за собою юридичну відповідальність, яка передбачена законом.

Витрати, які були здійсненні органом державної влади, органом місцевого самоврядування, у зв'язку із перевіркою звернення, які містили завідомо неправдиві відомості, можуть стягуватися з громадян на підставі рішення суду.

Закон України «Про інформацію» регулює суспільні відносини у сфері щодо створення, збирання, отримання, зберігання, використання, захисту інформації [5]. Право на інформацію забезпечується:

- 1) створенням механізму реалізації права на інформацію;
- 2) створення можливостей для вільного доступу до даних;
- 3) обов'язки суб'єктів владних повноважень постійно інформувати про свою діяльність і прийняті рішення, та забезпечувати доступ для запитувачів інформації;
- 4) здійснення державного та громадського контролю за додержанням інформаційного законодавства;
- 5) встановлення відповідальності за порушення законодавства про інформацію [5].

Не дозволяється збирання, зберігання, використання та поширення відомостей про особу без її згоди. Але при цьому забезпечується вільний доступ до інформації для кожного, яка стосується його особисто. Конфіденційними є відомості про фізичну особу, доступ до якої обмежено, та яка може бути поширена за згодою розпорядника такої інформації.

Закон України «Про електронну ідентифікацію та електронні довірчі послуги» визначає правові та організаційні засади щодо електронної ідентифікації особи, та надання доступу до електронних довірчих послуг. Цим Законом регулюються відносини, які виникають у процесі надання та отримання послуг електронної ідентифікації, гарантів із цифровою ідентифікацією та доступом до електронних довірчих послуг. Але цей же Закон не поширює свою дію на послуги у системах, які обробляють службову інформацію і державну таємницю [36].

Схеми електронної ідентифікації мають забезпечувати низький, середній та/або високий рівень довіри до засобів такої ідентифікації. Використання кваліфікованих підписів та печаток, що містять персональні відомості про особу, забезпечує високий рівень довіри до засобів електронної ідентифікації [36].

Виходячи із вищенаведеного, слід зробити висновок, що законодавство України у сфері захисту персональних даних досить насичене на кількість нормативно-правових актів. І кожен регулює суспільні відносини у конкретній сфері життєдіяльності особи.

3.2. Особливості обробки персональних даних у центрах надання адміністративних послуг

Підставами для обробки персональних даних є:

- 1) Згода суб'єкта персональних даних;
- 2) Дозвіл на обробку персональних даних, які надані володільцю даних відповідно до своїх повноважень;
- 3) захист важливих інтересів суб'єкта персональних даних;
- 4) необхідність виконання обов'язків володільця даних, відповідно до Закону;
- 5) необхідність захисту законних інтересів володільця даних, яким передаються персональні дані [1].

Обробка персональних даних, які є конфіденційною інформацією – не допускається, окрім випадків, які визначені Законом, і тільки в інтересах національної безпеки, економічного добробуту та прав людини. Обробка персональних відомостей про фізичну особу без її згоди допускається для захисту важливих інтересів суб'єкта персональних даних, але тільки до моменту, коли отримання такої згоди стане можливою [14].

Збирання даних є одним зі складових процесу обробки, яка передбачає дії з підбору чи впорядкування відомостей про особу. Володілець даних після отримання згоди на обробку, здійснює це шляхом реєстрації, накопичення, зберігання, адаптування, зміни, поновлення та поширення у відповідності до посадових обов'язків і керуючись нормами чинного законодавства.

Як зазначалося у попередніх підрозділах, у кожному випадку обробки персональних даних має бути конкретно визначена мета. Метою обробки персональних даних суб'єктів звернень у центр надання адміністративних послуг (далі – ЦНАП) є надання такої послуги. Така мета обробки є реалізацією права громадян на звернення до органів державної влади, органів місцевого самоврядування, їх посадових осіб [13]. Обробка персональних відомостей має здійснюватися відкрито і прозоро, із застосуванням технічних засобів і у спосіб, що відповідає цілям обробки. У випадку зміни мети обробки персональних даних на нову, яка є несумісною із попередньою, то для подальшої обробки володілець даних повинен отримати нову згоду від суб'єкта персональних даних у відповідності до зміненої мети [13].

Склад персональних даних визначаються у відповідності до чинного законодавства. Зміст та склад даних мають бути відповідними, адекватними і не надмірними відносно визначеної мети обробки. Першоджерелом відомостей про фізичну особу є документи видані на її ім'я, відомості, які особа надає про себе, а також підписані нею документи. У кожному ЦНАП існує свій, локальний документ, яким регулюються діяльність та визначаються функціональні обов'язки. У таких документах встановлюються загальні вимоги до технічних та

організаційних заходів щодо захисту персональних даних під час здійснення їхньої обробки [37].

Профільним нормативно-правовим актом у сфері надання адміністративних послуг є Закон України «Про адміністративні послуги». У ньому визначається, що адміністративні послуги надаються лиш суб'єктами владним повноважень і здійснюється як безпосередньо, так і через ЦНАП.

Адміністративні послуги надаються у електронній формі з використанням Єдиного державного вебпорталу електронних послуг, який пов'язаний з інформаційними системами органів державної влади та органів місцевого самоврядування [37].

Для отримання адміністративної послуги необхідно подати заяву. ЦНАП та інші суб'єкти надання адміністративних послуг на вимогу суб'єкта звернення забезпечують складання заяви в електронній формі, після чого її друкують та надають для перевірки і підписання суб'єкту звернення [37]. При наданні таких послуг законодавством передбачається заборона на вимагання документів або інформації, які не потрібні для надання послуги.

Для отримання адміністративної послуги суб'єкт звернення подає документи, у випадку, якщо відсутні відомості у електронних інформаційних базах в тому обсязі, що є достатньою для надання послуги:

- 1) документи, що посвідчують особу і підтверджують громадянство;
- 2) документи, що посвідчують особу іноземця, особу без громадянства, або особу зі статусом біженця;
- 3) військово-облікові документи;
- 4) свідоцтво про державну реєстрацію актів цивільного стану;
- 5) документи, що підтверджують надання особі спеціального права;
- 6) документи на транспортний засіб;
- 7) документи про трудову діяльність;
- 8) документи про освіту;
- 9) документи, які видані закладами охорони здоров'я;
- 10) документи, які підтверджують наявність інвалідності [13].

Суб'єкт надає адміністративну послугу шляхом отримання документів або інформації за відсутності суб'єкта звернення на підставі поданих відомостей у заяві [13]. Суб'єкт надання адміністративної послуги, який володіє інформацією та/або документами, що належить до сфери його управління, зобов'язаний:

- 1) забезпечити безоплатне надання таких документів та/або інформації;
- 2) вживає заходи для міжвідомчої електронної взаємодії, забезпечує відкритий і безоплатний доступ до власних інформаційних баз;
- 3) відповідно до законодавства забезпечує зберігання та захист інформації, яка стала відома у результаті надання адміністративної послуги;
- 4) забезпечує віддалений доступ до власних інформаційних систем;
- 5) вживає заходів для надання послуг у електронній формі.

Суб'єкти надання адміністративних послуг забезпечують вільний доступ із належними умовами до приміщень, у яких здійснюється прийом суб'єктів звернення [37].

Адміністративна послуга у відповідності до Закону України «Про адміністративні послуги», вважається наданою в момент її отримання особисто суб'єктом звернення або відправлення поштою рекомендованим листом із повідомленням про вручення. Поштою може бути надіслано результат послуги за бажанням суб'єкта звернення, кур'єром за додаткову плату, а також за допомогою електронних комунікацій. Але слід зазначити, що строк відправки поштою, не входить у строк надання послуги [13].

Адміністратор – це посадова особа, яка приймає рішення про утворення ЦНАП, надає адміністративні послуги та/або організовує їх надання.

Завданнями адміністратора є:

- 1) надає суб'єктам звернення вичерпну інформацію та консультацію;
- 2) приймає документи, які необхідні для надання послуги;
- 3) видача та/або забезпечення направлення результатів надання послуги через засоби поштового зв'язку;
- 4) організує забезпечення надання послуги;
- 5) здійснює контроль за дотриманням термінів надання послуги;

- 6) надає адміністративні послуги за рішенням органу;
- 7) складає протоколи про адміністративні правопорушення;
- 8) розглядає справу про адміністративні правопорушення та накладає адміністративні стягнення, у межах санкцій конкретної статті [13].

Організація забезпечення надання послуг здійснюється шляхом:

- 1) забезпечення безоплатного, віддаленого, автоматизованого доступу у режимі реального часу до інформації, що містяться у інформаційних системах;
- 2) надання на підставі запиту інформації, необхідної для виконання завдань;
- 3) забезпечення надання послуг у межах строків, які встановлені законом.

Закон України «Про адміністративні процедури» регулює відносини органів державної влади та органів місцевого самоврядування щодо здійснення функцій публічної адміністрації, розгляду і вирішення адміністративних справ, забезпечення та захист прав, свобод та/або законних інтересів осіб [38].

Адміністративне провадження розпочинається:

- 1) за заявою особи для забезпечення реалізації її права, свободи та/або законного інтересу, чи виконання нею визначеного Законом обов'язку, у тому числі і для отримання адміністративної послуги;
- 2) за ініціативою адміністративного органу у зв'язку із виконанням нею повноважень [38].

Особа має право подати до адміністративного органу заяву із вимогою прийняти адміністративний акт щодо забезпечення реалізації її прав, свобод та/або законних інтересів, у межах компетенції адміністративного органу.

Заява може бути подана як індивідуально, так і колективно [38].

Захист та обробка персональних даних, які містяться у документах та відомостях, що витребовуються уповноваженим адміністративним органом, здійснюється у відповідності до вимог Закону України «Про захист персональних даних» [1].

Право ознайомлюватися із матеріалами справи, отримання копій документів та відомостей може бути обмежено лиш за певних умов та протягом

строку доступу до таких даних. Персональні дані можуть надаватися лише в обсязі, які є необхідними для розгляду справи, надання послуги та/або прийняття рішення. Суб'єкт, який розглядає звернення, може публікувати на офіційному вебпорталі практику розгляду звернень і прийнятих рішень лиш за умови дотримання вимог Закону України «Про захист персональних даних» [1].

Отже, надання адміністративної послуги досить складна процедура з точки зору його законодавчого регулювання, адже потребує дотримання вимог законодавства у сфері захисту персональних даних, і щоб ця процедура була прозора і зрозуміла для отримувача послуги. Але надання послуг у електронній формі значно спрощує процедуру із дотриманням усіх вимог щодо захисту даних.

3.3. Проблемні аспекти та напрями гармонізації українського законодавства з правом ЄС

Наскільки б досконало не було розписано у нормативно-правових актах щодо надання адміністративних послуг, захисту та обробку персональних даних особи, все ж таки залишаються питання, які потребують їх врегулювання.

Якість надання адміністративних послуг можна підвищити, якщо:

- 1) децентралізувати їх надання;
- 2) забезпечити належну оплату праці в адміністративних органах;
- 3) покращити стандарти надання послуг;
- 4) покращувати наявні і запроваджувати сучасні форми надання послуг.

Аналізуючи рекомендації щодо використання досвіду ЄС в Україні, може включати у себе низку заходів, які спрямовані на модернізацію і ефективне використання цифрових технологій [39].

Основними напрямками підтримки ЄС у цьому напрямку є:

- 1) розвиток електронного урядування;
- 2) розбудова мережі ЦНАП;
- 3) удосконалення електронної ідентифікації особи при наданні послуг;

4) підвищення медіаграмотності [40].

Починаючи з 2024 року в Україні адміністративні послуги розглядаються з точки зору налагодження комунікації між суспільством та владою. Ключовим для успіху у цій комунікації є низка факторів, яка виражається у кількості запитів, часу реагування, доступності, актуальності тощо. Такі заходи спрямовані на підвищення якості і доступності адміністративних послуг в Україні за підтримки країн Європейського Союзу та сприяють підвищенню ефективності державного управління, а також задоволенню потреб суспільства.

Така співпраця із країнами ЄС надає можливість Україні вдосконалювати державне управління шляхом запровадження цифрових технологій та підвищенню якості надання адміністративної послуги. Це також сприяє підвищенню медіаграмотності населення, посиленню співпраці з ЄС та покращення економічного клімату в країні [40].

Українське законодавство у сфері надання адміністративних послуг та обробки персональних даних розглядає принципи державної політики у цій сфері, де верховенство права, юридична визначеність, відкритість, прозорість, своєчасність, мінімізацію документів та процедурних дій, справедливість, неупередженість, доступність, зручність, а також захищеність даних через призму вимог, а не лише як до іміджу сервісу. Порівнюючи із європейським стандартом належного адміністрування, де принципи виступають як критерії для процедурних дій, то наше законодавством у цьому питанні збігається [39].

Українська модель принципів має певну інфраструктуру, як до прикладу, режим електронної взаємодії електронних інформаційних ресурсів створює умови для реалізації принципу мінімізації документів, а режим електронної ідентифікації особи та довірчих послуг формує той довірчий поріг щодо легітимного доступу до сервісів зі збереженням належного захисту персональних даних. У Німеччині та Франції такий принцип закріплений як нормативний перехід до електронних каналів надання послуг зі збереженням процедурних гарантій. У Польщі проявляється як підкріплення електронного контакту процедурною дією [9].

Українська модель щодо мінімізації документів у міжвідомчій електронній взаємодії і до правових режимів електронної ідентифікації переводить принцип із сфери гасел у сферу обов'язку, особливо при налагодженій взаємодії електронних каналів отримання даних.

Через це цифровий сервіс перетворює принципи на вимоги до діяльності та прийнятті рішень. Вони мають бути вбудовані у правила доступу, дизайн процедурних кроків, стандартами кіберстійкості, моделі обміну даними та у механізми перегляду. Інакше зручність стає формальним, а прозорість стає видимим але без пояснень [41].

Прозорість і пояснюваність автоматизованої обробки даних полягає у тому, що суб'єкт звернення бачить не тільки результат, але й кроки, які породили те чи інше рішення. Також людина повинна знати, які саме дані і для чого були використанні. І без дотримання вищезгаданих принципів породжує проблему мовчазного адміністрування діяльності органу.

Переосмислення механізмів виправлення помилок даних і можливості перегляду результату дозволяє сформулювати висновок, що цифрова послуга є правовою лиш тоді і в тій мірі, наскільки електронна система здатна помилятися і виправлятися. Якщо процедурні дії спираються на реєстрові дані, то відповідно до принципів справедливості, неупередженості, юридичної визначеності та підзвітності вимагають визначення чітких і зрозумілих маршрутів внесення коректив як технічно (внесення змін у реєстр), так і юридично (шляхом перегляду рішень). Це має забезпечити людині право бути почутою, отримати мотивовану відповідь на свій запит і мати можливість оскаржити результати, які сформовані автоматизованими системами, а не повернення до паперового вирішення питання [41].

У порівняльній перспективі у відповідності до стандартів країн ЄС показує, що це є основа гарантії належного адміністрування. У французькій моделі електронне звернення кодифіковане у законодавчу систему, яка утримує його в процесуальному колі дій. Німецька модель підсилює перевірки через вимогу до належного мотивування результату і процедурних гарантій. У Польщі

це виражається через обов'язок точного з'ясування усіх фактичних обставин справи і захисту інтересів.

Українська цифрова трансформація вийшла на нормативну точку росту, оскільки принципи адміністративних послуг мають бути виражені у процедурних корекціях та перегляді рішень так, щоб надійність надання цифрової послуги вимірювалася не інтерфейсом, а можливістю відновлювати справедливість у правомірному колі, після виявлення помилки у процедурі, результаті, мотивуванні та контролі. Цифрова трансформація має бути дисциплінованою, юридичною інфраструктурою вироблення правового результату, а не лише формальною модернізацією процесу [41].

На даний момент основною проблемою у сфері захисту персональних даних особи в Україні полягає у відсутності нормативно-правових актів, які б забезпечували на достатньому та належному рівні захисту персональних відомостей, що відповідало б до міжнародних стандартів у цій сфері. Система законодавства України у сфері захисту персональних даних налічує велику кількість нормативно-правових актів, але жоден не має чіткого та відкоригованого з європейським стандартом визначення персональних даних. Відсутність законодавства, яка забезпечувала б відповідність міжнародним стандартам у цій сфері та належного технологічного рівня розвитку призводить до незадовільного рівня реалізації конституційного права на повагу до приватного та сімейного життя в Україні. У подальшому це призведе до визнання України на міжнародному рівні як держави, яка не здатна забезпечити належний рівень персональних даних особи. Відповідно до пункту 11 Плану заходів імплементації Угоди про асоціацію між Україною та країнами Європейського Союзу, який затверджений 25 жовтня 2017 року – Україна зобов'язана вдосконалити законодавство у сфері захисту персональних даних для приведення його у відповідності до GDPR. Головним завдань України у цій сфері є визначення напрямів правового регулювання та створення гарантій, які є необхідними для забезпечення реалізації суб'єктів в інформаційній сфері.

Оскільки проаналізувавши законодавчу базу, то сьогоднішній стан захисту персональних даних є незадовільним і загрозливим [41].

Про незадовільний стан захисту даних свідчить несанкціонований доступ до інформаційних баз даних сервісу «Дія», яке відбулося 22 січня 2022 року [42]. Також про незадовільний стан захисту даних свідчить несанкціонований доступ до застосунку «Резерв+» у жовтні 2024 року [39]. У обох випадках був відкритий доступ до персональної інформації осіб. Хоч протиправний доступ був швидко припинений, це не скасовує того факту, що несанкціонований доступ був здійснений.

Основним завданням законодавця є забезпечення пріоритету прав і свобод людини. Важливу роль у цьому відіграють закріплення вимоги якості товарів та послуг. У суспільстві більшу увагу приділяють зараз саме споживачу товарів та послуг. Захист прав споживачів на сьогоднішній день є окремим інститутом права, який продовжує розвиватися та вдосконалюватися. Так само в Україні потрібно розвивати і вдосконалювати захист персональних особи.

GDPR застосовується на території країн ЄС, а також має відношення до організацій та осіб, які є громадянами Європейського Союзу, але знаходяться за її межами. Законодавство України застосовується виключно на території України, та визначає права і обов'язки суб'єктів даних, які знаходяться під юрисдикцією України [24].

GDPR визнає персональні дані як будь-яку інформацію, яку можна пов'язати з особою та/або при допомозі якої можна її ідентифікувати. Закон України «Про захист персональних даних» визначає такі відомості як будь-яку інформацію про особу, якою можна її ідентифікувати. Але у GDPR надає більш розширене поняття таким відомостям, включаючи у себе такі складові, як біометричні, генетичні та особливі категорії даних, які стосуються расової та етнічної приналежності, релігійних, політичних та/або філософських переконань, стану здоров'я тощо.

Окрім цього, у GDPR встановлює вимогу щодо заходів безпеки персональних даних, які включають обов'язкове проведення оцінки захисту даних і призначення відповідальної особи з питань захисту даних [24].

Обидва нормативно-правових акти мають за мету забезпечення захисту персональної інформації особи. Однак, навіть при схожості обох законодавчих актів, все ж таки існує відмінність, серед яких це рівень захисту даних, вимоги до обробки та передачі даних та механізмів забезпечення прав особи. Слід зазначити, що у процесі цифровізації, зростаючої кількості міжнародних обмінів даними, все більш важливого значення набуває взаємодія між законодавствами ЄС та України. Така співпраця забезпечує належний захист даних, економічному та технологічному розвитку.

Розберемо термін «апроксимація», яке описує процес гармонізації законодавства. Апроксимація – це включення методів та способів перенесення законодавства Європейського Союзу у національне законодавство держави. Також включає його внесення у національне законодавство та через процес імплементації, яке проявляється через реалізацію прав або взяття на себе конкретних зобов'язань. Термін апроксимація використовується до тих держав, які ще не є членами ЄС і включає у себе три терміни: гармонізація, наближення та координація, які означають різні рівні інтеграції законодавства [39].

Адаптація національного законодавства до законодавства країн ЄС – це процес приведення нормативно-правових актів у відповідність із законами ЄС. Але це включає у себе не тільки вдосконалення наявного законодавства, але і розробку нових нормативно-правових актів.

Імплементація – це застосування правил положень, які нещодавно включені у національну правову систему. Якщо норми законодавства Європейського Союзу були включені у національне законодавство держави-кандидата, але на практиці ті положення не застосовуються, то процес імплементації є незавершеним [39].

Щодо директив, які прийняті країнами ЄС, то їх особливість полягає у тому, що вони охоплюють правила, яких потрібно дотримуватися або визначає

ціль, якої потрібно досягти і тоді кожна держава вирішує, яким саме чином забезпечити включення директив у національне законодавство. Інколи забезпечення директив виражається у накладенні санкцій. Але варто зазначити, що пряме перенесення директив у національне законодавство не забезпечує належної імплементації, оскільки директива не є нормативно-правовим актом у повному розумінні. Механізм реалізації директиви визначаються кожною державою, яка проводить імплементацію.

Щодо регламентів ЄС, то варто зазначити, що вони не застосовуються до держав, які не є членами ЄС, адже вони перед цим мають ратифікувати установчі договори. Тільки після узгодження національного законодавства із регламентами ЄС, лиш тоді потрібно їх запроваджувати у національне законодавство [39].

Отже, проблема надання адміністративних послуг та захисту і обробки персональних даних є на законодавчому рівні, і лиш після внесення коректив у національне законодавство можна стати на шлях вирішення проблем.

ВИСНОВОК

Отже, виходячи із вищенаведеного змісту курсової роботи можемо сказати, що персональні дані – це будь-які відомості про особу, які дозволяють її ідентифікувати. Поняття персональних даних в Україні на перший погляд схоже із поняттям, яке існує у країнах ЄС. Але відмінність полягає у тому, що українське поняття персональних даних дещо вужче, аніж те саме поняття у країнах ЄС. У Європейському Союзі до таких відомостей відносяться і ті дані, які мають відношення до особи, а також охоплюють генетичні, біометричні та категорію чутливих даних про особу, до прикладу, про расову та/або релігійну приналежність.

Адміністративні послуги – це послуги, які надаються суб'єктами владних повноважень. У країнах Європи під цими послугами розуміють як взаємодію між органами державної влади, органами місцевого самоврядування та особою, шляхом реалізації своїх повноважень.

В Україні принципи захисту персональних даних є основоположними засадами щодо обробки даних і їх дотримання визначає наскільки якісно, результативно та у повній мірі буде надана адміністративна послуга та надійно будуть захищені персональні дані, які були об'єктами під час обробки.

Актом, який регулює сферу захисту персональних даних є Загальний регламент про захист даних – це нормативно-правовий акт, який оновлює законодавство Європейського Союзу в сфері захисту персональних даних, а також замінює Закон про захист даних від 1998 року. І цей нормативно-правовий акт є основою у діяльності країн ЄС щодо обробки та забезпечення захисту персональних даних.

Також доцільно зазначити, що у країнах Європи існують механізми, які забезпечують належний контроль та захист від несанкціонованого доступу до персональних відомостей особи. Процес цифровізації послуг та обробки персональних відомостей особи збільшує обсяги обробки даних, а також їх обмін між країнами ЄС. Тому через це забезпечення належного контролю, обробки та

захисту даних від несанкціонованого доступу стає все більш актуальним у сьогоденних реаліях.

Українське законодавство містить велику кількість нормативно-правових актів, які регулюють суспільні відносини у сфері обробки та захисту персональних даних при наданні адміністративних послуг. Але не дивлячись на її кількість вона не забезпечує належного захисту цих даних на рівні із рівнем захисту у країнах ЄС.

Забезпечення належного рівня захисту персональних даних в Україні на рівні країн ЄС, потрібно здійснити заходи, щодо внесення змін у законодавство України, щоб її норми відповідали міжнародним стандартам. Також варто зазначити, що внесенні зміни мають бути не тільки наявні у законодавстві, а й практично застосовуватися у повсякденні, коли виникає потреба у обробці та захисту персональних відомостей особи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. Дата оновлення: 14.06.2026. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 09.04.2026).
2. Справа за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частини першої, другої статті 32, частини другої, третьої статті 34 Конституції України: Рішення Конституційного Суду України від 20.01.2012 р. № 2-рп/2012. Дата оновлення: 20.01.2012. URL: <https://zakon.rada.gov.ua/laws/show/v002p710-12#Text> (дата звернення: 14.04.2026).
3. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус: Закон України від 20.11.2012 р. № 5492-VI. Дата оновлення: 14.06.2025. URL: <https://zakon.rada.gov.ua/laws/show/5492-17#Text> (дата звернення: 09.04.2025).
4. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. Дата оновлення: 14.06.2026. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 09.04.2026).
5. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. Дата оновлення: 20.01.2026. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (дата звернення: 09.04.2026).
6. Конфіденційна інформація: енциклопедія. URL: https://uk.wikipedia.org/wiki/Конфіденційна_інформація (дата звернення: 15.04.2026).
7. Конституція України від 28.06.1996 р. Дата оновлення: 01.01.2020. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text> (дата звернення: 09.04.2026).

8. Європейське право у сфері захисту персональних даних: *посібник*. 2015. 216 с. URL: https://apladm.dn.court.gov.ua/userfiles/posibnik_1.pdf (дата звернення: 16.04.2026).

9. Каретник О. С. До питання про правову природу персональних даних фізичної особи: цивілістичні аспекти. *Наукова стаття Таврійський національний університет імені В. І. Вернадського*. 2014. С. 192-200. URL: https://pravoua.com.ua/storage/files/magazines/files/pravoukr-2014-9-pravoukr_9_14.pdf#page=192 (дата звернення: 16.04.2026).

10. Михайлик А. С. До питання нормативно-правового регулювання захисту персональних даних працівників в Україні. *Наукова стаття Національного юридичного університету імені Ярослава Мудрого*. 2022. С. 82-87. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2022/10/15-1.pdf> (дата звернення: 18.04.2026).

11. Апетик А. М. Юридична природа персональних даних. Сучасний конституціоналізм: проблеми теорії та практика. *Наукова стаття*. 2021. URL: <https://law.ukma.edu.ua/apetyk-a-m-yurydychna-pryroda-personalnyh-danyh-suchasnyj-konstytutsionalizm-problemy-teoriyi-ta-praktyky/> (дата звернення: 16.04.2026).

12. Цивільний кодекс України від 16.01.2003 р. № 435-IV. Дата оновлення: 01.02.2026. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text> (дата звернення: 10.04.2026).

13. Про адміністративні послуги: Закон України від 06.09.2012 р. № 5203-VI. Дата оновлення: 02.03.2026. URL: <https://zakon.rada.gov.ua/laws/show/5203-17#Text> (дата звернення: 09.04.2026).

14. Про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Конвенція від 28.01.1981 р. № 2438-VI. Дата оновлення: 06.07.2010. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 09.04.2026).

15. Адміністративні послуги: енциклопедія. URL: https://uk.wikipedia.org/wiki/Адміністративні_послуги (дата звернення: 15.04.2026).

16. Вовк Н. Досвід ЄС у цифровій трансформації адміністративних послуг. *Наукова стаття*. 2024. URL: <https://journals.uran.ua/bdi/article/view/350635> (дата звернення: 16.04.2026).
17. Колпаков В. К. Принципи надання адміністративних послуг: морфологічний аналіз у координатах європейського стандартів і цифрової трансформації. *Журнал «Наукові інновації та передові технології»*. 2026. С. 3164-3176. URL: <https://perspectives.pp.ua/index.php/nauka/article/view/37309/37309> (дата звернення: 17.04.2026).
18. Галінкіна В. С. Основні принципи обробки та захисту персональних даних. *Науковий вісник Ужгородського Національного Університету*. 2024. С. 111-115. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/03/19.pdf> (дата звернення: 15.04.2026).
19. Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних: Регламент Європейського Парламенту і Ради від 27.04.2016 р. № 2016/679. Дата оновлення: 27.04.2016. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 11.04.2026).
20. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних: Директива Європейського Парламенту і Ради від 24.10.1995 р. №95/46/ЄС. Дата оновлення: 25.05.2018. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text (дата звернення: 10.04.2026).
21. Європейське право у сфері захисту персональних даних: *посібник*. 2015. 216 с. URL: https://apladm.dn.court.gov.ua/userfiles/posibnik_1.pdf (дата звернення: 16.04.2026).
22. Про захист прав людини і основоположних свобод: Конвенція від 04.11.1950 р. № 475/97-ВР. Дата оновлення: 01.08.2021. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 10.04.2026).

23. Загальна декларація прав людини від 10.12.1948 р. № 217 А (III). Дата оновлення: 10.12.1948. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text (дата звернення: 10.04.2026).

24. Рогальська Н. В. Захист персональних даних в ЄС відповідно до GDPR. *Наукова стаття Національний юридичний університет імені Ярослава Мудрого*. 2019. 10 с. URL: <https://nauka-online.com/wp-content/uploads/2019/05/Rogalska-.pdf> (дата звернення: 16.04.2026).

25. Блащук О. О. Цифрова участь громадянського суспільства у нормотворчості в умовах євроатлантичного розвитку України. *Юридичний науковий електронний журнал*. 2025. С. 29-32. URL: https://lsej.org.ua/8_2025/5.pdf (дата звернення: 18.04.2026).

26. Google святкує 26-річчя. З якими гучними справами компанія мала клопіт за останні роки. *Стаття*. 2024. URL: <https://suspilne.media/845125-google-svatkue-26-ricca-z-akimi-gucnimi-spravami-kompania-mala-klopit-za-ostanni-roki/> (дата звернення: 18.04.2026).

27. Омбудсман України. Захист персональних даних: стаття. URL: <https://ombudsman.gov.ua/uk/zahist-personalnih-danih-faq> (дата звернення: 15.04.2026).

28. Тимченко Л. М. Європейський досвід удосконалення системи надання адміністративних послуг. *Наукова стаття Дніпровського регіонального інституту державного правління Національної академії державного управління при Президентові України*. 2015. С. 136-140. URL: http://www.investplan.com.ua/pdf/3_2015/31.pdf (дата звернення: 17.04.2026).

29. Суд Європейського Союзу. *Лекція*. URL: <https://studies.in.ua/lekcii-pravo-es/4246-sud-yeuropeyskih-splnot.html> (дата звернення: 18.04.2026).

30. Про заходи для високого спільного рівня кібербезпеки на всій території Союзу: Директива Європейського Парламенту і Ради від 14.12.2022 р. № 2022/2555. Дата оновлення: 14.12.2022. URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text (дата звернення: 11.04.2026).

31. Справа щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закон України «Про інформацію» та статті 12 Закону України «Про прокуратуру»: Рішення Конституційного Суду України від 30.10.1997 р. № 5-зп. Дата оновлення: 30.10.1997. URL: <https://zakon.rada.gov.ua/laws/show/v005p710-97#Text> (дата звернення: 14.04.2026).

32. Кодекс законів про працю України від 10.12.1971 р. № 322-VIII. Дата оновлення: 01.01.2026. URL: <https://zakon.rada.gov.ua/laws/show/322-08#Text> (дата звернення: 13.04.2026).

33. Гета Д. С. Нормативно-правове регулювання захисту персональних даних працівників у трудових відносинах в Україні. *Наукова стаття Харківського національного університету внутрішніх справ*. 2019. С. 76-77. URL: https://univd.edu.ua/general/publishing/konf/11_04_2019/pdf/34.pdf (дата звернення: 18.04.2026).

34. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. Дата оновлення: 08.08.2025. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text> (дата звернення: 13.04.2026).

35. Про звернення громадян: Закон України від 02.10.1996 р. № 393/96-ВР. Дата оновлення: 24.01.2026. URL: <https://zakon.rada.gov.ua/laws/show/393/96-вр#Text> (дата звернення: 11.04.2026).

36. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017 р. № 2155-VIII. Дата оновлення: 18.12.2024. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text> (дата звернення: 14.04.2026).

37. Порядок обробки та захисту персональних даних при виконанні функціональних обов'язків у Центрі надання адміністративних послуг виконавчого комітету Кілійської міської ради. *Нормативна база*. 2023. URL: <https://kiliyska-gromada.gov.ua/news/1679041302/> (дата звернення: 18.04.2026).

38. Про адміністративну процедуру: Закон України від 17.02.2022 р. № 2073-IX. Дата оновлення: 15.11.2024. URL: <https://zakon.rada.gov.ua/laws/show/2073-20#Text> (дата звернення: 11.04.2026).

39. Адаптація законодавства України до права ЄС: теоретичні та практичні аспекти. *Путівник долідницької служби Верховної Ради України*. Київ. 2023. 120 с. URL: <https://research.rada.gov.ua/uploads/documents/32597.pdf> (дата звернення: 17.04.2026).

40. Завертнева-Ярошенко В. А., Кисель А. С. Проблеми гармонізації законодавства України та Європейського Союзу в сфері захисту прав споживачів. *Наукова стаття Одеський національний університет імені І. І. Мечникова*. 2018. С. 95-101.

41. Гармонізація законодавства України з правом Європейського Союзу: реалії та перспективи. *Науково-практична конференція*. / Рябчинська О. П. та ін. Львів. 2023. 204 с. URL: <http://catalog.liha-pres.eu/index.php/liha-pres/catalog/download/220/5185/17905-1?inline=1> (дата звернення: 17.04.2026).

42. Злам «Дії». Чи справді з держпорталу витекли дані та чим це вам може загрожувати. *Стаття*. 2022. URL: <https://forbes.ua/inside/diya-zliv-26012022-3389> (дата звернення: 19.04.2026).