НАЦІОНАЛЬНА АКАДЕМІЯ ПРАВОВИХ НАУК УКРАЇНИ
НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ
ПРИВАТНОГО ПРАВА І ПІДПРИЄМНИЦТВА
ІМЕНІ АКАДЕМІКА Ф. Г. БУРЧАКА

Кваліфікаційна наукова
праця на правах рукопису

КОСТЮК ДМИТРО ІГОРОВИЧ

УДК 342.95(477):347.97/.99

ДИСЕРТАЦІЯ

АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ ЦИФРОВІЗАЦІЇ ПУБЛІЧНОГО УПРАВЛІННЯ

Спеціальність 081 – Право
Галузь знань 08 – Право

Подається на здобуття наукового ступеня доктора філософії.

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ **Д. І. Костюк**

Науковий керівник: **Теремецький Владислав Іванович**,
доктор юридичних наук, професор,
заслужений юрист України

Київ – 2026

АННОТАЦІЯ

Костюк Д. І. **Адміністративно-правове забезпечення захисту персональних даних в умовах цифровізації публічного управління**. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 – «Право». Науково-дослідний інститут приватного права і підприємництва імені академіка Ф. Г. Бурчака НАПрН України, Київ, 2026.

Дисертацію присвячено комплексному дослідженню адміністративно-правового забезпечення захисту персональних даних в умовах цифровізації публічного управління.

В першому розділі *«Загальна характеристика адміністративно-правового забезпечення захисту персональних даних у сфері публічного управління»* досліджено концептуальні основи захисту персональних даних як об’єкта адміністративно-правової охорони, розкрито вплив цифровізації на трансформацію правовідносин у цій сфері та визначено механізми впливу міжнародних стандартів на національне адміністративне законодавство.

Обґрунтовано, що персональні дані є специфічним об’єктом адміністративно-правової охорони, відмінним від об’єктів конституційно-правового і цивільно-правового регулювання. Проаналізовано основні наукові підходи до визначення персональних даних і встановлено, що жоден із них не враховує повною мірою специфіки обробки даних у сфері публічного управління. Доведено, що саме адміністративне право здатне забезпечити необхідні виміри охорони – нормативний, інституційний та юрисдикційний. Право на захист персональних даних охарактеризовано як самостійне публічне суб’єктивне право з власною структурою правомочностей. Запропоновано авторське визначення персональних даних у контексті публічного управління, яке враховує специфіку суб’єктів обробки, правову підставу та дуальну мету реалізації публічно-владних повноважень і забезпечення прав особи, а також відображає реальність обробки через цифрові технології та інтегровані інформаційні системи.

Цифровізація публічного управління розглянута як чинник якісної трансформації правовідносин у сфері захисту персональних даних, що охоплює зміну суб'єктного складу правовідносин, природи їх об'єкта, змісту прав і обов'язків сторін та характеру правового зв'язку між державою і громадянином. Виявлено два принципово нові типи правовідносин: відносини між суб'єктом даних і алгоритмом як суб'єктом автоматизованого управлінського рішення та відносини в умовах структурної інформаційної асиметрії, за якої держава акумулює комплексний цифровий профіль громадянина незалежно від його активних звернень. Аналіз функціонування платформи «Дія», системи «Трембіта» та реєстру «Оберіг» підтвердив реальність виявлених ризиків і необхідність їх адміністративно-правового врегулювання.

Досліджено архітектуру міжнародних та наднаціональних стандартів захисту персональних даних, що охоплює Конвенцію 108+ як інструмент міжнародного права та акти вторинного права ЄС – GDPR, Директиву 2016/680, Data Governance Act і EU AI Act – як взаємопов'язані інструменти. Обґрунтовано класифікацію нормативного, адаптаційного, юрисдикційного та орієнтувального механізмів їхнього впливу на національне адміністративне законодавство, кожен із яких має відмінну юридичну природу і порядок реалізації. Проаналізовано практику ЄСПЛ у справах про порушення права на приватність публічними органами і встановлено, що сформульовані у ній принципи є обов'язковими для органів публічного управління України незалежно від їх закріплення у національному законодавстві. Виявлено системний характер прогалин імплементації міжнародних стандартів і обґрунтовано необхідність комплексного реформування адміністративного законодавства у цій сфері.

У другому розділі *«Зміст адміністративно-правового забезпечення захисту персональних даних в умовах цифровізації публічного управління»* досліджено нормативно-правову основу, суб'єктний склад та процедурні

елементи механізму захисту персональних даних у сфері цифрового публічного управління.

Охарактеризовано нормативно-правове регулювання захисту персональних даних у сфері цифрового публічного управління і встановлено його структурний дисбаланс між стрімким розвитком законодавства про цифрові публічні послуги та реєстри і хронічним відставанням спеціального законодавства про захист персональних даних. Закони про електронні публічні послуги, публічні електронні реєстри, електронну ідентифікацію та електронні комунікації формують розгалужену нормативну рамку цифрового публічного управління, проте жоден із них не містить комплексного регулювання захисту персональних даних, обмежуючись бланкетними нормами до Закону № 2297-VI. Виявлені прогалини мають системний характер і охоплюють відсутність правового визначення статусу оператора цифрових платформ як контролера персональних даних, відсутність вимог до оцінки впливу на захист даних при впровадженні нових цифрових сервісів та відсутність механізму прозорості алгоритмічних рішень.

Досліджено систему суб’єктів забезпечення захисту персональних даних у сфері публічного управління та проведено їх класифікацію за функціональним критерієм з урахуванням специфіки цифрового публічного управління. Виявлено системну прогалину у розподілі відповідальності між суб’єктами в умовах платформної моделі надання публічних послуг, яка полягає у тому, що чинне законодавство не визначає, хто і в якому обсязі несе відповідальність за захист персональних даних у ситуаціях множинності суб’єктів обробки. Обґрунтовано, що ключовою інституційною прогалиною є відсутність спеціалізованого незалежного наглядового органу, а чинна модель покладення відповідних функцій на Уповноваженого Верховної Ради України з прав людини не забезпечує необхідного рівня спеціалізації та операційної спроможності для ефективного нагляду за обробкою персональних даних у масштабах цифрового публічного управління.

Розкрито зміст адміністративних процедур обробки персональних даних у системах цифрового публічного управління і встановлено їхню якісну відмінність від традиційних адміністративних процедур. Ключовими ознаками цих процедур є автоматизований характер обробки без безпосередньої участі посадової особи, множинність суб'єктів у рамках однієї процедури та динамічне розширення обсягу даних внаслідок міжреєстрової взаємодії. Визначено, що правове регулювання таких процедур має ґрунтуватись на вимогах прозорості алгоритмічних рішень, підзвітності всіх суб'єктів обробки та реальної доступності механізмів захисту прав суб'єктів персональних даних відповідно до стандартів GDPR і практики ЄСПЛ.

У третьому розділі *«Удосконалення адміністративно-правового забезпечення захисту персональних даних в умовах цифровізації публічного управління»* досліджено практичні проблеми правозастосування у сфері захисту персональних даних, виявлено системні правові прогалини у регулюванні електронних публічних послуг та визначено механізми і пріоритети гармонізації українського законодавства із правом Європейського Союзу.

Проаналізовано стан правозастосування у сфері адміністративної відповідальності за порушення законодавства про захист персональних даних і встановлено феномен «мертвої норми», який полягає у тому, що за наявності тисяч звернень суб'єктів персональних даних реальне притягнення до відповідальності є поодиноким. Системними причинами цього визначено вузький суб'єктний склад відповідальності, що виключає юридичних осіб, невідповідність розміру санкцій масштабу порушень та процедурну обтяженість провадження. Обґрунтовано пропозиції щодо реформування системи адміністративної відповідальності за моделлю дворівневої структури GDPR з диференціацією санкцій залежно від тяжкості порушення та одночасним запровадженням спрощеного провадження і спеціального порядку збирання цифрових доказів.

Охарактеризовано правовий режим захисту персональних даних у системах електронних публічних послуг і встановлено, що проблеми платформи «Дія», системи «Трембіта» та реєстру «Оберіг» мають спільну системну причину – відсутність превентивних правових інструментів на етапі проектування та запуску публічних цифрових сервісів. Обґрунтовано пропозиції щодо законодавчого закріплення обов'язкових вимог privacy by design і проведення оцінки впливу на захист персональних даних як передумов введення в експлуатацію нових державних інформаційних систем, а також щодо доповнення законопроєкту № 8153 нормою про спільне контролерство із солідарною відповідальністю суб'єктів перед суб'єктами персональних даних.

Визначено пріоритети та механізми гармонізації адміністративного законодавства України у сфері захисту персональних даних із правом ЄС і доведено її багатовимірний характер, що виходить за межі імплементації GDPR і охоплює Директиву 2016/680 у правоохоронній сфері та EU AI Act у частині систем штучного інтелекту у публічному секторі. Обґрунтовано пріоритетну послідовність законодавчих та інституційних змін і сформульовано три взаємопов'язані критерії оцінки досягнутого рівня відповідності (нормативний, інституційний та практичний), сукупне виконання яких свідчить про реальну гармонізацію в умовах цифровізації публічного управління.

Ключові слова: персональні дані, захист персональних даних, цифрова трансформація, цифрові ринки, право власності, засоби, суб'єкт владних повноважень, Ukraine Facility Plan, захист даних, діджиталізація, цифровізація, GDPR, цифрові технології, інформаційна безпека, конфіденційність.

SUMMARY

Kostiuk D .I. **Administrative and legal protection of personal data in the context of digitalization of public administration**. – *Qualification scientific work on the rights of the manuscript.*

Dissertation for obtaining the degree of Doctor of Philosophy in specialty 081 – Law. Academician F. H. Burchak Scientific Research Institute of Private Law and Entrepreneurship of National Academy of Law Sciences of Ukraine, Kyiv, 2026.

The dissertation is dedicated to a comprehensive study of the administrative and legal protection of personal data in the context of digitalization of public administration.

The first chapter «*General characteristics of administrative and legal provision for the protection of personal data in the field of public administration*» examines the conceptual foundations of personal data protection as an object of administrative and legal protection, reveals the impact of digitalization on the transformation of legal relations in this field, and identifies the mechanisms of influence of international standards on national administrative legislation.

It is substantiated that personal data constitutes a specific object of administrative and legal protection, distinct from the objects of constitutional and civil law regulation. The main scientific approaches to the definition of personal data have been analyzed and it has been established that none of them fully accounts for the specifics of data processing in the sphere of public administration. It is proven that administrative law is capable of ensuring the necessary dimensions of protection – normative, institutional and jurisdictional. The right to personal data protection is characterized as an independent public subjective right with its own structure of legal powers. An authorial definition of personal data in the context of public administration is proposed, which takes into account the specifics of processing subjects, the legal basis and the dual purpose of exercising public authority and ensuring the rights and legitimate interests of individuals, and also reflects the reality of processing through digital technologies and integrated information systems.

Digitalization of public administration is examined as a factor of qualitative transformation of legal relations in the field of personal data protection, encompassing changes in the subject composition of legal relations, the nature of their object, the content of the rights and obligations of the parties, and the nature of the legal connection between the state and the citizen. Two fundamentally new types of legal relations have been identified: relations between a data subject and an algorithm as the subject of an automated management decision, and relations under conditions of structural information asymmetry, whereby the state accumulates a comprehensive digital profile of a citizen regardless of their active requests. Analysis of the functioning of the Diia platform, the Trembita system and the Oberih register confirmed the reality of the identified risks and the need for their administrative and legal regulation.

The architecture of international and national personal data protection standards is examined, encompassing Convention 108+ as an instrument of international law and acts of secondary EU law – GDPR, Directive 2016/680, Data Governance Act and EU AI Act – as interrelated instruments. A classification of normative, adaptive, jurisdictional and orientational mechanisms of their influence on national administrative legislation has been substantiated, each having a distinct legal nature and order of implementation. The case law of the ECtHR in cases concerning violations of the right to privacy by public authorities has been analyzed, and it has been established that the principles formulated therein are binding on Ukrainian public administration bodies regardless of their entrenchment in national legislation. The systemic nature of the gaps in the implementation of international standards has been identified and the need for comprehensive reform of administrative legislation in this field has been substantiated.

The second chapter «*The content of administrative and legal provision for personal data protection in the context of public administration digitalization*» examines the regulatory framework, subject composition and procedural elements of the personal data protection mechanism in the sphere of digital public administration.

The regulatory framework for personal data protection in the sphere of digital public administration has been characterized and its structural imbalance identified between the rapid development of legislation on digital public services and registers and the chronic lag of special legislation on personal data protection. The laws on electronic public services, public electronic registers, electronic identification and electronic communications form an extensive regulatory framework for digital public administration, however none of them contains comprehensive regulation of personal data protection, being limited to referral provisions to Law No. 2297-VI. The identified gaps are systemic in nature and encompass the absence of a legal definition of the status of digital platform operators as personal data controllers, the absence of requirements for data protection impact assessment when introducing new digital services, and the absence of a mechanism for transparency of algorithmic decisions.

The system of subjects responsible for ensuring personal data protection in the sphere of public administration has been studied and classified according to a functional criterion taking into account the specifics of digital public administration. A systemic gap has been identified in the distribution of responsibility between subjects under the platform model of public service delivery, consisting in the fact that current legislation does not determine who and to what extent bears responsibility for personal data protection in situations of multiple processing subjects. It is substantiated that the key institutional gap is the absence of a specialized independent supervisory authority, while the current model of assigning relevant functions to the Ukrainian Parliament Commissioner for Human Rights does not ensure the necessary level of specialization and operational capacity for effective supervision of personal data processing at the scale of digital public administration.

The content of administrative procedures for personal data processing in digital public administration systems has been revealed and their qualitative distinction from traditional administrative procedures established. The key characteristics of these procedures are the automated nature of processing without

the direct participation of an official, the multiplicity of subjects within a single procedure, and the dynamic expansion of data volume as a result of inter-register interaction. It has been determined that the legal regulation of such procedures must be based on requirements of transparency of algorithmic decisions, accountability of all processing subjects and real accessibility of mechanisms for protecting the rights of personal data subjects in accordance with GDPR standards and ECtHR case law.

The third chapter «*Improvement of administrative and legal provision for personal data protection in the context of public administration digitalization*» examines the practical problems of law enforcement in the field of personal data protection, identifies systemic legal gaps in the regulation of electronic public services, and determines the mechanisms and priorities for harmonization of Ukrainian legislation with the law of the European Union.

The state of law enforcement in the field of administrative liability for violations of personal data protection legislation has been analyzed and the phenomenon of a "dead norm" established, consisting in the fact that despite thousands of appeals from personal data subjects, actual prosecution remains isolated. The systemic causes thereof have been identified as the narrow subject composition of liability, which excludes legal entities, the discrepancy between the size of sanctions and the scale of violations, and the procedural burden of proceedings. Proposals have been substantiated for reforming the system of administrative liability based on the model of the two-tier structure of GDPR with differentiation of sanctions depending on the severity of the violation and the simultaneous introduction of simplified proceedings and a special procedure for collecting digital evidence.

The legal regime of personal data protection in electronic public service systems has been characterized and it has been established that the problems of the Diia platform, the Trembita system and the Oberih register share a common systemic cause – the absence of preventive legal instruments at the stage of design and launch of public digital services. Proposals have been substantiated for the legislative

entrenchment of mandatory requirements for privacy by design and the conduct of data protection impact assessments as prerequisites for the commissioning of new state information systems, as well as for supplementing Draft Law No. 8153 with a provision on joint controllership with joint and several liability of subjects before personal data subjects.

The priorities and mechanisms for harmonization of Ukrainian administrative legislation in the field of personal data protection with EU law have been determined and its multidimensional nature proven, extending beyond the implementation of GDPR to encompass Directive 2016/680 in the law enforcement sphere and the EU AI Act with regard to artificial intelligence systems in the public sector. A priority sequence of legislative and institutional changes has been substantiated and three interrelated criteria for assessing the achieved level of compliance formulated — normative, institutional and practical — the cumulative fulfilment of which indicates genuine harmonization in the context of digitalization of public administration.

Keywords: personal data, personal data protection, digital transformation, digital markets, property rights, means, subject of authority, Ukraine Facility Plan, data protection, digitalization, digitalization, GDPR, digital technologies, information security, confidentiality.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Костюк Д. І. Адміністративні процедури обробки персональних даних у системах міжвідомчого електронного обміну. *Приватне право і підприємництво*. 2026. Вип. 26. С. 178–185. DOI: https://doi.org/10.32849/2409-9201.2026.26.19. URL: https://ppp-journal.kiev.ua/index.php/26-2026

2. Костюк Д. І. Нормативно-правове регулювання обробки персональних даних у публічних електронних реєстрах України. *Актуальні проблеми правознавства*. 2026. № 1 (45). С. 98–105. DOI: https://doi.org/10.35774/app2026.01.098. URL: https://appj.wunu.edu.ua/index.php/appj/article/view/2265

3. Костюк Д. І. Правовий статус платформи «Дія» як суб'єкта обробки персональних даних. *Журнал східноєвропейського права*. 2026. № 145. С. 321–328. DOI: https://doi.org/10.71404/2409-6415.145.36. URL: https://easternlaw.com.ua/wp-content/uploads/2026/04/kostiuk_145.pdf

Наукові праці, які засвідчують апробацію матеріалів дисертації:

4. Костюк Д. І. Імплементація стандартів конвенції 108+ та GDPR в адміністративне законодавство України. *Україна в умовах реформування правової системи: сучасні реалії та міжнародний досвід*: матеріали IX Міжнародної науково-практичної конференції (м. Тернопіль, 2–3 травня 2025 р.). Тернопіль: ЗУНУ, 2025. С. 346–348. URL: https://confuf.wunu.edu.ua/index.php/confuf/article/view/1732/1711

5. Костюк Д. І. Наглядовий орган у сфері захисту персональних даних: стандарти незалежності та перспективи інституційної реформи в Україні. *Людина, суспільство, держава: актуальні питання правового регулювання взаємодії*: тези доп. учасників. II наук.-практ. конф. (Київ, 21 лист. 2025 р.). Київ: 2025. С. 65–67. DOI: https://doi.org/10.71404/PPSS.2025.3.18. URL: https://library.pp-ss.pro/index.php/ndippsn_20251121/article/view/kostiuk/pdf

6. Костюк Д. І. Персональні дані як об’єкт адміністративно-правової охорони. *Актуальні проблеми приватного та публічного права* : матеріали VIII Міжнародної науково-практичної конференції присвяченої 97-річчю від дня народження члена-кореспондента НАПрН України, академіка Міжнародної кадрової академії, заслуженого діяча науки України, доктора юридичних наук, професора О. І. Процевського, Харків, 27 березня 2026 року. Харківський національний педагогічний університет імені Г. С. Сковороди, Україна. Видавництво: ХНПУ імені Г. С. Сковороди, 2026. С. 505–507.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ВПО – Внутрішньо переміщені особи

ВРУ – Верховна рада України

GDPR – Загальний регламент про захист даних (General Data Protection Regulation)

DPIA – Оцінка впливу на захист персональних даних (Data Protection Impact Assessment)

DPO – Спеціаліст із захисту даних (Data Protection Officer)

EDPB – Європейська рада із захисту даних (European Data Protection Board)

ЄС – Європейський союз

ЄСПЛ – Європейський суд з прав людини

ЕСОЗ – Електронна система охорони здоров'я

ІКТ – Інформаційно-комунікаційні технології

КАС України – Кодекс адміністративного судочинства України

КМУ – Кабінет Міністрів України

КПК України – Кримінальний процесуальний кодекс України

КСЗІ – Комплексна система захисту інформації

КСУ – Конституційний Суд України

КУпАП – Кодекс України про адміністративні правопорушення

ККУ – Кримінальний кодекс України

НСЗУ – Національна служба здоров'я України

ФОП – Фізична особа-підприємець

ШІ – Штучний інтелект

eIDAS – Регламент про електронну ідентифікацію та довірчі послуги (Electronic Identification and Trust Services)

EU AI Act – Регламент ЄС про штучний інтелект

X-Road – Платформа електронної взаємодії державних реєстрів (Естонія)

ВСТУП

Обґрунтування вибору теми дослідження. Цифровізація публічного управління докорінно змінила характер взаємодії між державою та громадянином, перетворивши персональні дані на центральний ресурс адміністративних процедур. Масштабне впровадження електронних публічних послуг, інтегрованих реєстрів і систем міжвідомчого обміну даними створило принципово нові ризики для прав суб'єктів персональних даних, адекватна відповідь на які потребує системного переосмислення адміністративно-правового забезпечення їх захисту.

Чинне законодавство України у сфері захисту персональних даних суттєво відстає від реалій цифрового публічного управління, зокрема стосовно урахування специфіки агрегованої обробки даних через інтегровані платформи, закріплення механізмів превентивного захисту і відповідності міжнародним стандартам у частині інституційного забезпечення нагляду. Ця невідповідність набуває особливого значення в умовах набуття Україною статусу кандидата на членство в Європейському Союзі, що покладає конкретні зобов'язання щодо гармонізації законодавства із стандартами GDPR, Директиви 2016/680 і Конвенції 108+.

Повномасштабна збройна агресія додала до цієї проблематики безпековий вимір. Персональні дані стали стратегічним ресурсом, а їх неналежний захист загрозою національній безпеці. Сукупність зазначених чинників зумовлює актуальність комплексного дослідження адміністративно-правового забезпечення захисту персональних даних в умовах цифровізації публічного управління та визначає науково-практичну значущість обраної теми.

Дослідженню питань обробки і захисту персональних даних присвятили свої роботи І. Арістова, О. Баранов, О. Гіляка, М. Бем, Ю. Бездецький, М. Бліхар, В. Брижко, І. Городиський, С. Гусаров, О. Заярний, К. Мельник, М. Пальчик, В. Пилипчук, В. Пішта, І. Похиленко, К. Шкрібляк та багато інших правників. Серед зарубіжних дослідників проблематику визначення

персональних даних та їх правового режиму розробляли Б. Паркінсон, М. Філліпс, К. Ірті, Р. Ґеллерт, К. Єнг, Л. Бігрейв, Р. Уолтерс та інші.

Питання цифровізації публічного управління та її правових наслідків досліджували Н. Атаманова, М. Білецький, М. Дубняк, Р. Кірін, А. Крулевський, Г. Крушельницька, І. Луняченко, В. Медяник, С. Ненько, О. Савченко, Т. Плугатар, С. Пороскун, К. Рябець, В. Рядінська, Н. Сорокіна, М. Тимченко, О. Тур, В. Філатов та інші науковці. Проблематику електронних публічних послуг, цифрових платформ і систем електронної взаємодії розробляли В. Клочан, Х. Кметик-Подубінська, І. Петрів, В. Полюхович, Ю. Хохлачова та інші вчені.

Адміністративно-правові аспекти захисту персональних даних, системи суб'єктів і механізмів відповідальності вивчали К. Головко, Д. Деркач, О. Дяковський, Н. Загребельна, В. Кірієнко, М. Колотило, В. Коновалова, В. Кравчук, А. Мерник, Р. Мигаль, А. Михайлик, Є. Остіян, І. Савельєва, Н. Семчук, В. Світличний, В. Стратонов, В. Теремецький, Я. Худолєй та інші.

Питання гармонізації українського законодавства з міжнародними стандартами захисту персональних даних та євроінтеграційні аспекти цієї проблематики розробляли К. Гуртова, Ю. Коваленко, О. Кожухар, А. Лабик, П. Мелотікова, Н. Расторгуєва, О. Шпакович, О. Шевчук, О. Яворська та інші. Серед зарубіжних дослідників зазначеної тематики слід відзначити внесок Н. Ботчорічвілі, С. Міккелссона, Ю. Руоганена, Д. Шинкунієне.

Незважаючи на значний науковий доробок у цій сфері, комплексного дослідження адміністративно-правового забезпечення захисту персональних даних в умовах цифровізації публічного управління з урахуванням сучасних викликів євроінтеграції, воєнного стану та стрімкого розвитку цифрових технологій у вітчизняній науці адміністративного права досі не проводилось, що зумовлює актуальність і наукову новизну цього дослідження.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертацію виконано відповідно до положень Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським

співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, зокрема ст. 15 щодо співробітництва у сфері забезпечення належного рівня захисту персональних даних відповідно до європейських і міжнародних стандартів, а також з урахуванням положень Плану України для Ukraine Facility на 2024–2027 роки, які передбачають цифровізацію публічних послуг, розвиток безпечної цифрової інфраструктури, удосконалення електронної ідентифікації, модернізацію державних реєстрів та інтеграцію України до Єдиного цифрового ринку ЄС. Тематика дисертації відповідає пунктам 3.5.2, 3.5.5, 3.5.6, 3.5.24 та 3.12.26 Основних наукових напрямів та найважливіших проблем фундаментальних досліджень у галузі природничих, технічних, суспільних і гуманітарних наук Національної академії наук України на 2024–2028 роки, затверджених постановою Президії НАН України від 10.01.2024 № 8.

Дисертацію підготовлено в межах теми фундаментальних досліджень «Правове забезпечення ринкових відносин в умовах євроінтеграції» (РК УкрІНТЕІ № 0123U100002), яка виконується в Науково-дослідному інституті приватного права і підприємництва імені академіка Ф. Г. Бурчака Національної академії правових наук України. Тему дисертаційного дослідження затверджено вченою радою Науково-дослідного інституту приватного права і підприємництва імені академіка Ф. Г. Бурчака Національної академії правових наук України (протокол № 2 від 22.02.2023), а згодом уточнено (протокол № 3 від 25.03.2026).

Мета і завдання дослідження. *Мета* дисертаційної роботи полягає у здійсненні комплексного дослідження адміністративно-правового забезпечення захисту персональних даних в умовах цифровізації публічного управління, виявленні системних прогалин чинного законодавства та визначенні перспективних шляхів його вдосконалення з урахуванням міжнародних стандартів і досвіду держав-членів Європейського Союзу.

Для досягнення поставленої мети необхідно вирішити такі *завдання*:

– розкрити поняття та правову природу персональних даних як об’єкта адміністративно-правової охорони, обґрунтувати їх місце у системі об’єктів публічного суб’єктивного права та обґрунтувати авторське визначення персональних даних у контексті цифровізації публічного управління;

– розглянути цифровізацію публічного управління як чинник якісної трансформації правовідносин у сфері захисту персональних даних, визначити нові типи правовідносин, що виникають внаслідок цифровізації, та виявити системні правові ризики, пов’язані з масштабною обробкою персональних даних у цифровому публічному управлінні;

– описати міжнародно-правові стандарти захисту персональних даних, визначити механізми їхнього впливу на національне адміністративне законодавство та виявити системні прогалини імплементації цих стандартів в Україні;

– охарактеризувати нормативно-правове регулювання захисту персональних даних у сфері цифрового публічного управління, визначити його структуру та виявити прогалини, що потребують законодавчого усунення;

– дослідити систему суб’єктів забезпечення захисту персональних даних у сфері публічного управління, визначити їхній правовий статус, повноваження та взаємодію;

– розкрити зміст адміністративних процедур обробки персональних даних у системах цифрового публічного управління та визначити вимоги до їх правового регулювання;

– проаналізувати стан і проблеми правозастосування у сфері адміністративної відповідальності за порушення законодавства про захист персональних даних та обґрунтувати пропозиції щодо реформування системи санкцій і процедурного механізму притягнення до відповідальності;

– виявити правові проблеми захисту персональних даних у системах електронних публічних послуг та сформулювати пропозиції щодо вдосконалення правового регулювання у цій сфері;

– визначити пріоритети та механізми гармонізації адміністративного законодавства України у сфері захисту персональних даних із правом Європейського Союзу в умовах євроінтеграції та обґрунтувати послідовність необхідних законодавчих та інституційних змін.

Об'єктом дослідження є суспільні відносини, що виникають у процесі забезпечення захисту персональних даних в умовах цифровізації публічного управління.

Предметом дослідження є адміністративно-правове забезпечення захисту персональних даних в умовах цифровізації публічного управління.

Методи дослідження. Досягнення поставлених наукових завдань і формулювання висновків, що розкривають наукову новизну роботи, забезпечено завдяки комплексному застосуванню загальнонаукових, конкретно-наукових та спеціально-юридичних методів наукового пізнання.

Діалектичний метод наукового пізнання став основою для розгляду всіх аспектів дослідження в їх взаємозв'язку та взаємообумовленості. Метод аналізу та синтезу застосовано при дослідженні поняття та правової природи персональних даних (підрозділ 1.1) і виявленні системних прогалин адміністративної відповідальності за їх порушення (підрозділ 3.1). Формально-юридичний метод використано при характеристиці нормативно-правового регулювання захисту персональних даних (підрозділ 2.1), адміністративних процедур їх обробки (підрозділ 2.3) та правових проблем у системах електронних публічних послуг (підрозділ 3.2). Системний аналіз застосовано для характеристики адміністративно-правового механізму захисту персональних даних (розділ 2) та міжнародно-правових стандартів і механізмів їхнього впливу на національне законодавство (підрозділ 1.3). Метод абстрагування та конкретизації використано при дослідженні цифровізації публічного управління як чинника трансформації правовідносин у сфері захисту персональних даних (підрозділ 1.2). Порівняльно-правовий метод застосовано при аналізі механізмів гармонізації українського законодавства із правом ЄС (підрозділ 3.3). Історико-правовий метод

використано при дослідженні генези нормативно-правового регулювання захисту персональних даних і етапів цифровізації публічного управління (підрозділи 1.1, 1.2). Метод прогнозування використано при визначенні пріоритетів і послідовності кроків гармонізації адміністративного законодавства із правом ЄС (підрозділ 3.3). Імперативний метод застосовано при дослідженні системи суб'єктів забезпечення захисту персональних даних та їхніх повноважень (підрозділ 2.2). Метод юридичної герменевтики використано при тлумаченні норм міжнародних стандартів та їхньому співвідношенні з нормами національного адміністративного законодавства (підрозділ 1.3).

Науковим та теоретичним підґрунтям дисертації стали праці вітчизняних і зарубіжних фахівців у галузі адміністративного права та інформаційного права, загальної теорії держави і права, інших галузевих правових і суміжних наук.

Нормативною основою дисертації є Конституція України, чинні міжнародно-правові договори, закони України, підзаконні нормативно-правові акти, які закріплюють правові засади забезпечення захисту персональних даних в умовах цифровізації публічного управління.

Наукова новизна отриманих результатів визначається тим, що дисертація є комплексним дослідженням, у якому розроблено концептуальне, теоретико-правове та прикладне розуміння особливостей адміністративно-правового забезпечення захисту персональних даних в умовах цифровізації публічного управління. До найважливіших наукових положень, що містять наукову новизну та виносяться на захист, належать такі:

вперше:

– здійснено комплексний аналіз феномену «мертвої норми» у сфері адміністративної відповідальності за порушення законодавства про захист персональних даних, що дозволило виявити системні причини неефективності чинного механізму, зокрема відсутність відповідальності юридичних осіб, невідповідність розміру санкцій масштабу порушень та процедурні бар'єри

притягнення до відповідальності, а також обґрунтувати пропозиції щодо реформування системи санкцій з орієнтацією на дворівневу модель адміністративних штрафів, передбачену GDPR, із диференціацією відповідальності залежно від тяжкості порушення та з урахуванням особливостей вітчизняної правової системи;

– обґрунтовано кваліфікацію правовідносин між суб'єктами обробки персональних даних у системах електронних публічних послуг «Дія» та «Трембіта» як відносин спільного контролерства за критеріями, закріпленими у ст. 26 GDPR, що, на відміну від чинного Закону № 2297-VI, який оперує лише конструкціями «володільця» і «розпорядника» персональних даних, дозволило виявити нормативну прогалину в розподілі відповідальності між платформою-посередником і органом-надавачем послуги та обґрунтувати необхідність доповнення законопроєкту № 8153 положенням про солідарну відповідальність спільних контролерів перед суб'єктом персональних даних;

– розроблено класифікацію механізмів впливу міжнародних і наднаціональних стандартів захисту персональних даних на національне адміністративне законодавство шляхом розмежування нормативного, адаптаційного, юрисдикційного та орієнтувального механізмів залежно від їхньої юридичної природи і порядку реалізації, що дозволило диференційовано оцінити ступінь обов'язковості відповідних стандартів для органів публічного управління України та визначити пріоритетні напрями адаптації національного законодавства до acquis ЄС у сфері захисту персональних даних;

удосконалено:

– науково-теоретичне обґрунтування адміністративно-правової природи захисту персональних даних шляхом виокремлення трьох його необхідних вимірів: нормативного (встановлення обов'язкових правил обробки для суб'єктів публічного адміністрування), інституційного (визначення наглядових органів і механізмів контролю) та юрисдикційного (система адміністративної відповідальності та порядок оскарження), що, на відміну від

наявних підходів, які розглядають захист персональних даних переважно в контексті інформаційного або конституційного права, дозволяє довести центральну роль адміністративного права у регулюванні відносин між суб'єктами публічного адміністрування і громадянином у цій сфері;

– розуміння цифровізації публічного управління як чинника якісної трансформації правовідносин у сфері захисту персональних даних шляхом виокремлення чотирьох взаємопов'язаних вимірів: зміни суб'єктного складу, об'єкта, змісту прав і обов'язків, а також характеру правового зв'язку між державою і громадянином, що дозволило визначити її системний вплив на архітектуру адміністративно-правових відносин;

– характеристику нормативно-правового регулювання захисту персональних даних у сфері цифрового публічного управління шляхом виявлення його структурного дисбалансу між стрімким розвитком законодавства про цифрові публічні послуги і реєстри та відставанням спеціального законодавства про захист персональних даних, що дозволило обґрунтувати системний характер прогалин і визначити пріоритетні напрями їх законодавчого усунення;

– систематизацію суб'єктів забезпечення захисту персональних даних у сфері публічного управління шляхом їх класифікації за функціональним критерієм з урахуванням специфіки цифрового публічного управління, що, дозволило виявити прогалини у розподілі відповідальності між суб'єктами в умовах платформної моделі надання публічних послуг та обґрунтувати необхідність запровадження спеціалізованого наглядового органу;

– розуміння правових проблем захисту персональних даних у системах електронних публічних послуг шляхом виявлення їхньої спільної системної причини, яка полягає у відсутності превентивних правових інструментів на етапі проектування та запуску публічних цифрових сервісів, що, на відміну від підходів, які аналізують окремі недоліки правового регулювання платформи «Дія» чи системи «Трембіта», дозволило обґрунтувати необхідність запровадження обов'язкових вимог privacy by design і DPIA як передумов

введення в експлуатацію нових державних інформаційних систем, що обробляють персональні дані громадян;

– підхід до гармонізації адміністративного законодавства України у сфері захисту персональних даних із правом Європейського Союзу шляхом обґрунтування її багатовимірного характеру, що виходить за межі адаптації до acquis ЄС у сфері захисту персональних даних і охоплює Директиву 2016/680 у правоохоронній сфері та EU AI Act у частині систем штучного інтелекту в публічному секторі, що дозволило визначити пріоритетну послідовність законодавчих та інституційних змін і сформулювати критерії оцінки досягнутого рівня відповідності національного законодавства стандартам ЄС в умовах євроінтеграційного процесу;

дістали подальшого розвитку:

– визначення поняття персональних даних у контексті публічного управління, яке запропоновано трактувати як будь-які відомості чи сукупність (прямих або опосередкованих) відомостей про фізичну особу, яка ідентифікована або може бути ідентифікована, що збираються, зберігаються та обробляються суб’єктами публічного адміністрування в межах адміністративних процедур, зокрема із застосуванням цифрових технологій та інтегрованих інформаційних систем, на підставі та у спосіб, визначені законом, з метою реалізації публічно-владних повноважень та забезпечення прав і законних інтересів особи, що дозволяє відобразити специфіку персональних даних як об’єкта адміністративно-правової охорони в умовах цифровізації публічного управління;

– розуміння права на захист персональних даних у контексті адміністративно-правових відносин шляхом його характеристики як самостійного публічного суб’єктивного права з тривимірною структурою правомочностей: права вимагати законності обробки персональних даних від суб’єктів публічного адміністрування, права на реалізацію суб’єктивних прав щодо власних даних та права на захист у разі їх порушення, що дозволило чітко визначити зміст, суб’єктний склад і механізм реалізації цього права в

адміністративно-правових відносинах, на відміну від підходів, які розглядають його виключно як елемент права на приватність;

– наукове розуміння правовідносин у сфері захисту персональних даних в умовах цифрового публічного управління шляхом виявлення двох нових типів таких правовідносин: відносин між суб'єктом даних і алгоритмом як суб'єктом автоматизованого управлінського рішення та відносин в умовах структурної інформаційної асиметрії, за якої держава формує комплексний цифровий профіль громадянина з множини реєстрів незалежно від його активних звернень;

– виокремлення прогалин імплементації міжнародних і наднаціональних стандартів захисту персональних даних шляхом виявлення системного характеру невідповідності національного законодавства цим стандартам у термінологічному, інституційному та процедурному вимірах, що дозволило обґрунтувати необхідність комплексного, а не точкового реформування адміністративного законодавства;

– наукове розуміння проблеми здійснення адміністративних процедур обробки персональних даних у системах цифрового публічного управління шляхом виявлення їхньої специфіки порівняно з традиційними адміністративними процедурами, зокрема автоматизованого характеру обробки, відсутності безпосередньої участі посадової особи та множинності суб'єктів у межах однієї процедури, що дозволило сформулювати вимоги до правового регулювання таких процедур з урахуванням стандартів прозорості, підзвітності та захисту прав суб'єктів персональних даних.

Практичне значення отриманих результатів. Практичне значення отриманих результатів полягає у тому, що дисертаційне дослідження має теоретико-прикладний характер, а сформульовані у ньому висновки та пропозиції можуть бути використані у:

– *науково-дослідній діяльності* – для подальшого вивчення адміністративно-правових аспектів захисту персональних даних в умовах цифровізації публічного управління, розроблення концептуальних засад

реформування законодавства у цій сфері, а також у порівняльно-правових дослідженнях механізмів захисту персональних даних у державах-членах Європейського Союзу (*акт впровадження НДІ публічної політики і соціальних наук від 07.05.2026*);

– *правотворчій діяльності* – під час удосконалення положень законодавства України про захист персональних даних, зокрема при підготовці законопроєкту № 8153 до другого читання, розробленні спеціального законодавства про захист персональних даних у правоохоронній сфері відповідно до Директиви (ЄС) 2016/680, а також у процесі гармонізації національного адміністративного законодавства з правом Європейського Союзу в рамках євроінтеграційного процесу;

– *правозастосовній діяльності* – у практиці органів публічної влади при здійсненні обробки персональних даних у системах електронних публічних послуг, діяльності Уповноваженого Верховної Ради України з прав людини як наглядового органу у сфері захисту персональних даних, а також при вирішенні адміністративними судами спорів, пов’язаних із порушенням прав суб’єктів персональних даних у сфері публічного управління;

– *освітньому процесі закладів вищої освіти* – під час викладання та методичного забезпечення навчальних дисциплін «Адміністративне право», «Інформаційне право», «Право кібербезпеки», а також при підготовці навчально-методичних матеріалів і проведенні лекційних та практичних занять.

Особистий внесок здобувача. Дисертаційне дослідження виконано здобувачем самостійно. Сформульовані у роботі висновки, рекомендації та пропозиції є результатом особистого аналізу наукових джерел, міжнародних документів, актів права Європейського Союзу, нормативно-правових актів України та практики правозастосування у сфері захисту персональних даних в умовах цифровізації публічного управління.

Апробація матеріалів дисертації. Основні положення й висновки дисертації були обговорені та оприлюднені на міжнародних і всеукраїнських

науково-практичних конференціях, семінарах, круглих столах, а саме: «Україна в умовах реформування правової системи: сучасні реалії та міжнародний досвід» (м. Тернопіль, 2–3 травня 2025 р.), «Актуальні проблеми приватного та публічного права » (м. Харків, 27 березня 2026 р.), «Людина, суспільство, держава: актуальні питання правового регулювання взаємодії» (м. Київ, 21 листопада 2025 р.).

Публікації. Основні результати дисертаційного дослідження відображено в 6 наукових працях за темою дисертації, із яких 3 статті опубліковано у виданнях, внесених до переліку фахових наукових видань України, а 3 праці засвідчують апробацію матеріалів дисертації.

Структура та обсяг дисертації. Дисертація складається з вступу, трьох розділів, кожен із яких містить три підрозділи, висновків, списку використаних джерел (186 найменування на 24 сторінках) та двох додатків на 4 сторінках. Повний обсяг кваліфікаційної наукової праці становить 215 сторінок, із них 171 сторінка – основного тексту.

РОЗДІЛ 1
ЗАГАЛЬНА ХАРАКТЕРИСТИКА АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ПУБЛІЧНОГО УПРАВЛІННЯ

1.1. Поняття персональних даних як об'єкта адміністративно-правової охорони

Стрімке поширення інформаційно-комунікаційних технологій, автоматизація процесів публічного управління та розбудова електронних сервісів держави зумовили перетворення відомостей про фізичну особу на ресурс стратегічного значення, і визначили персональні дані як одне із центральних понять сучасного інформаційного та адміністративного права Як слушно зазначає М. Бліхар, поряд із зростанням використання Інтернету «зростає і рівень небезпеки для користувачів, а найбільшою загрозою постає недостатній рівень захисту персональних даних» [14]. Масштаби обробки персональних даних органами публічної влади невпинно зростають, оскільки державні реєстри, електронні адміністративні послуги, автоматизовані системи передбачають акумулювання значного обсягу відомостей про фізичних осіб. Р. Ґеллерт констатує, що обсяг поняття «персональні дані» постійно розширюється із впливом цифрового суспільства, зокрема в умовах «розумних» середовищ (smart environments), де нові технології генерують безпрецедентні масиви даних про особу [174]. Водночас правова доктрина досі не виробила єдиного підходу до визначення цього поняття, що ускладнює формування ефективного механізму регулювання та захисту прав громадян.

Б. Андрусишин та Є. Білозьоров на основі порівняльного аналізу українського та європейського законодавства, а також практики ЄСПЛ, доходять висновку, що в національному праві відсутнє єдине розуміння поняття «персональні дані», що суттєво ускладнює механізм їх захисту та гарантування [164]. Водночас комплексне визначення персональних даних у

контексті публічного управління залишається недостатньо розробленим, значна кількість досліджень зосереджена на загальних питаннях інформаційного права або на захисті персональних даних у окремих сферах (трудовому, медичному, конституційному праві тощо), тоді як специфіка обробки даних суб'єктами публічного адміністрування потребує окремого обґрунтування.

Чинний Закон України «Про захист персональних даних» від 1 червня 2010 року № 2297-VI визначає персональні дані як «відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована» [118]. Це офіційне визначення побудоване на двох базових критеріях: факт ідентифікації особи та можливість такої ідентифікації. І. Похиленко підкреслює, що ідентифікація може бути безпосередньою (за прізвищем, номером паспорта) або опосередкованою (за допомогою додаткової інформації у розпорядженні володільця), і наводить конкретні приклади: ідентифікаційні дані, контактні, біометричні, медичні, фінансові, дані про освіту та онлайн-активність [97, с. 96]. М. Колотило вважає зазначене визначення вичерпним і достатнім для правозастосування [59, с. 240]. Однак вважаємо таку позицію дискусійною, оскільки визначення не містить прикладів ідентифікаторів, не розмежовує типи даних і не враховує можливостей сучасних технологій ідентифікації.

Регламент (ЄС) 2016/679 (GDPR) визначає персональні як будь-яку інформація, що стосується ідентифікованої або такої, що може бути ідентифікована, фізичної особи. Причому Регламент прямо перелічує приклади ідентифікаторів: ім'я, ідентифікаційний номер, дані про місцезнаходження, онлайн-ідентифікатор, а також фізичні, фізіологічні, генетичні, психічні, економічні, культурні або соціальні ознаки [180]. Така конкретизація відображає технологічну реальність, де IP-адреса, cookies або цифровий відбиток браузера слугують засобом ідентифікації. Зазначимо, що навіть у європейській доктрині визнається неможливість точного та надійного визначення меж поняття «персональні дані», і дослідники констатують, що

через нечіткість концепції захисту наразі неможливо визначити точний та надійний спосіб, коли саме особа є ідентифікованою [144]. К. Ірті підкреслює динамічну природу персональних даних, і зазначає, що межа між персональними та неперсональними даними не є сталою, оскільки анонімізовані дані за певних умов можуть бути реідентифіковані, а псевдонімізовані зберігають потенціал ідентифікації [175]. Ця невизначеність має прямі наслідки для публічного управління, де органи влади змушені приймати рішення про режим обробки даних в умовах правової неоднозначності.

Аналіз наукових праць дозволяє систематизувати існуючі підходи до визначення персональних даних у кілька груп.

Інформаційний підхід розглядає персональні дані як різновид інформації. А. Кебус визначає їх як «будь-які відомості, що стосуються фізичної особи, на підставі яких ця особа може бути ідентифікована» [48, с. 203], акцентуючи на інформаційній природі та зв’язку з правом на інформацію. Р. Ґеллерт у контексті цього підходу досліджує співвідношення понять «дані» та «інформація» у праві захисту персональних даних і доходить висновку, що визначення «будь-яка інформація» у ст. 4 GDPR охоплює як синтаксичний вимір інформації (цифрові дані, зображення, голосові записи), так і семантичний (інтерпретація даних через їх співвіднесення з конкретною особою) [173].

Функціональний підхід конкретизує зміст персональних даних залежно від сфери правовідносин: С. Гусаров та К. Мельник визначають персональні дані працівника як «будь-яку інформацію про конкретну фізичну особу, яка працює на підставі трудового договору, надану роботодавцю або зібрану ним відповідно до закону» [26, с. 133], а І. Діордіца, І. Коваленко та О. Коваль наголошують на необхідності розглядати персональні дані у контексті широкого спектру культурних, соціальних і релігійних традицій [32, с. 141]. Такий підхід засвідчує, що зміст персональних даних не є статичним, він трансформується залежно від конкретних правовідносин.

Атрибутивний підхід визначає персональні дані через систему обов'язкових ознак. М. Пальчик, К. Шкрібляк та Ю. Березделецький виокремлюють три такі ознаки, а саме: персональні дані становлять окремий вид інформації, зазвичай фіксуються у документах, що надаються особою, а їх основною метою є ідентифікація фізичної особи [89, с. 431].

Критеріальний підхід будується через перелік видів даних та критеріїв ідентифікації. М. Бем, І. Городиський та співавтори зазначають, що у міжнародних актах (Конвенція 108, Директива 95/46/ЄС, GDPR) поняття персональних даних означено приблизно однаково, тобто будь-яка інформація, яка стосується ідентифікованої особи або особи, яка може бути ідентифікованою [11, с. 16]. М. Філліпс підтверджує цю тенденцію, простежуючи еволюцію міжнародних норм обміну даними від Керівних принципів ОЕСР до GDPR і констатуючи послідовне розширення обсягу поняття «персональні дані» у кожному наступному міжнародному документі [179]. Цей підхід є найближчим до офіційного визначення і найчастіше використовується у правозастосовній практиці.

М. Різак визначає персональні дані як об'єкт посягання: «виражену в об'єктивній матеріальній формі охоронювану законом інформацію або масив інформації, за допомогою якої можна чітко ідентифікувати конкретну особу та щодо якої вчинені протиправні дії» [134, с. 119], акцентуючи на охоронному аспекті даних.

Окремої уваги заслуговує позиція В. Пилипчука та В. Брижка, які пропонують розглядати персональні дані як «особливий вид умовно визначеної власності», що юридично виступає у формі права приватної власності людини та ототожнює собою право на її самовизначення [91, с. 45]. Зазначимо, що ця концепція була закладена ще у проекті Закону 2006 року, однак Президент застосував право «вето» саме через норму щодо права власності людини на свої персональні дані. Погоджуємося із застереженням О. Гиляки, який попереджає, що при такому підході «конфіденційність є виключно предметом торгу», а наслідком може стати декларативність права

на недоторканність приватного життя [19, с. 25]. Ця дискусія є важливою для публічного управління, проте незалежно від обраної концепції захист персональних даних у цій сфері здійснюється переважно адміністративно-правовими засобами, а не засобами приватного права.

Множинність підходів до визначення зумовлена складністю самого об'єкта. А. Михайлик констатує, що «українське законодавство про захист персональних даних складається з більше ніж 20 нормативно-правових актів, які не мають чіткого та скорельованого з європейським законодавством визначення» [83, с. 83]. М. Бем та І. Городиський фіксують важливу прогалину про те, що у національному законодавстві відсутнє чітке визначення поняття «захист персональних даних» [10, с. 243-244]. Р. Уолтерс акцентує увагу на значній фрагментарності підходів до визначення персональних даних і в інших країнах, оскільки одні держави використовують узагальнене визначення, що охоплює будь-яку інформацію, за допомогою якої можна ідентифікувати особу, тоді як інші розмежовують загальні, медичні, чутливі та біометричні дані у самостійні правові категорії з різним рівнем захисту [185]. Така фрагментарність ускладнює обмін даними та уніфікацію правозастосовної практики, що є актуальним і для України. Отже, проблема полягає не лише у визначенні самого поняття «персональні дані», а й у відсутності нормативного визначення принципів їх обробки і захисту як правової категорії.

Поняття «персональні дані» функціонує в нормативному полі поряд із кількома суміжними категоріями, розмежування з якими має не лише теоретичне, а й безпосередньо практичне значення для правозастосування. Передусім ідеться про поняття «інформація про фізичну особу», «конфіденційна інформація про особу» та «таємниця приватного життя». Закон України «Про інформацію» від 2 жовтня 1992 року вперше запровадив категорію «інформація про фізичну особу», визначивши її як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [119]. Це формулювання стало попередником сучасної дефініції «персональні дані» у Законі № 2297-VI, який фактично

запозичив його дослівно [118]. Водночас між цими поняттями існує функціональна відмінність: «інформація про фізичну особу» є загальноправовою категорією інформаційного законодавства, тоді як «персональні дані» є спеціальною категорією, що підпадає під окремий правовий режим обробки та захисту. Якщо перше поняття фіксує об'єкт (відомості про особу), то друге додає правовий режим (правила збирання, зберігання, використання, вилучення та відповідальність за порушення).

Стаття 32 Конституції України оперує категорією «конфіденційна інформація про особу», забороняючи її збирання, зберігання, використання та поширення без згоди особи [63]. Конституційний Суд України у Рішенні у справі К. Устименка від 30 жовтня 1997 року № 5-зп роз'яснив зміст цього поняття зазначивши, що до конфіденційної інформації належать «свідчення про особу (освіта, сімейний стан, релігійність, стан здоров'я, дата і місце народження, майновий стан та інші персональні дані)» [137]. Це рішення є ключовим для розуміння співвідношення категорій, при чому КСУ фактично визнав персональні дані складовою конфіденційної інформації про особу, але не тотожною їй. М. Пальчик та співавтори підтверджують таке розмежування і зазначають, що «конфіденційна інформація, як і персональні дані, це інформація про фізичну особу, зокрема її національність, дату та місце народження, освіту. Водночас до конфіденційної інформації може належати, наприклад, інформація статистичного характеру або відомості про результати перевірки контролюючим органом» [89, с. 431]. Отже, конфіденційна інформація є ширшою категорією, яка включає персональні дані, але не зводиться до них. Статистична інформація чи результати відомчих перевірок є конфіденційними, проте не є персональними даними, оскільки самі по собі не ідентифікують конкретну фізичну особу.

Окремої уваги заслуговує категорія «таємниця приватного (особистого) життя», яка має конституційне підґрунтя (ст. 32 Конституції) і ширший зміст, ніж поняття персональних даних. Таємниця приватного життя охоплює сферу особистих стосунків, сімейного життя, побуту, листування, яка може й не

фіксуватися у вигляді конкретних даних. Персональні дані, натомість, завжди мають фіксовану форму та відображені у документах, реєстрах, базах даних, цифрових системах. Серед обов'язкових властивостей персональних даних зазначають саме «фіксовану форму та відображення у певному джерелі (носії даних)» [89, с. 431]. Вважаємо, що персональні дані є формалізованою частиною інформації про приватне життя, яка підлягає правовому режиму обробки.

Закон України «Про доступ до публічної інформації» вносить ще один вимір у це співвідношення. О. Гиляка зазначає, що положення трьох законів («Про інформацію», «Про доступ до публічної інформації» та «Про захист персональних даних») «передбачають режим доступу до публічної інформації, захист персональних даних та юридичні механізми для пошуку балансу між правом знати та правом на приватність» [19, с. 20-21]. Частина 2 статті 6 Закону «Про доступ до публічної інформації» містить трискладовий тест, обов'язковий при обмеженні доступу до інформації: обмеження має переслідувати легітимну мету; розголошення може спричинити істотну шкоду; шкода від оприлюднення переважає суспільний інтерес у її отриманні [107]. Для сфери публічного управління цей баланс є повсякденною дилемою, оскільки державні реєстри одночасно є джерелом публічної інформації та містять персональні дані, і визначення межі між відкритістю та захистом потребує застосування саме цього трискладового тесту.

Таким чином, у системі суміжних категорій «персональні дані» займають специфічне місце. Вони є вужчим поняттям порівняно з «конфіденційною інформацією про особу» та «таємницею приватного життя», але ширшим за галузеві категорії (персональні дані працівника, пацієнта тощо). Водночас саме поняття «персональні дані» має найбільш розвинений правовий режим, що включає визначення підстав обробки, прав суб'єкта, обов'язків володільця, механізм контролю та відповідальності.

З точки зору теорії адміністративного права персональні дані є об'єктом публічного суб'єктивного права – права на захист персональних даних. У

науці адміністративного права публічне суб'єктивне право визначається як юридично закріплена і гарантована державою можливість особи вимагати від суб'єктів публічного адміністрування певної поведінки у сфері реалізації публічно-владних повноважень. В. Галунько та співавтори визначають людиноцентристську теорію адміністративного права як таку, за якою публічна адміністрація має якнайповніше задовольняти права, свободи й законні інтереси приватних осіб [3]. Саме через цю призму право на захист персональних даних постає не як елемент ширшого права на приватність, а як самостійне публічне суб'єктивне право з власним змістом, суб'єктним складом і механізмом реалізації. Цю позицію підтверджує і сучасне право ЄС. Хартія основних прав ЄС закріплює право на захист персональних даних у ст. 8 окремо від права на приватність (ст. 7), що є свідченням їхньої самостійної юридичної природи [155]. О. Гиляка у дослідженні права на приватність та захист персональних даних в умовах цифровізації підтверджує, що право на захист персональних даних набуло самостійного конституційного статусу і не може розглядатися лише як похідне від права на приватне життя, оскільки має власний предмет [19].

Публічне суб'єктивне право на захист персональних даних включає три взаємопов'язані складових: право вимагати від суб'єктів публічного адміністрування законності обробки персональних даних, тобто дотримання встановлених підстав, мети та принципів; право на реалізацію суб'єктивних прав щодо власних даних, що охоплює доступ, виправлення, видалення та заперечення проти обробки; право на захист у разі порушення, що включає звернення до наглядового органу і до суду. Саме ця тривимірна структура відрізняє право на захист персональних даних від загального права на приватність і визначає його як самостійний об'єкт адміністративно-правової охорони. Більш детально про це нами описано у [68].

Цифровізація публічного управління структурно змінює природу персональних даних як об'єкта адміністративно-правової охорони. В умовах аналогового управління персональні дані існували переважно як статичний

об’єкт, зафіксований у конкретному документі з визначеним колом осіб, що мали до нього доступ. Цифровізація перетворює персональні дані на динамічний об’єкт, що безперервно генерується, агрегується з різних джерел і змінює свій правовий режим залежно від контексту обробки. Р. Ґеллерт констатує, що поняття «персональні дані» постійно розширюється під впливом цифрового суспільства, де нові технології генерують безпрецедентні масиви даних про особу, причому жодне окреме значення саме по собі може не ідентифікувати особу, але їхня сукупність робить ідентифікацію неминучою [173]. Цей феномен агрегації є ключовою характеристикою цифрового публічного управління, де державні реєстри, платформи електронних послуг і системи міжвідомчого обміну даними фактично формують цифровий образ громадянина шляхом поєднання відомостей, кожне з яких окремо є нейтральним, але в сукупності розкриває повну картину приватного життя особи. К. Ірті підкреслює динамічну природу цього процесу, і зазначає, що межа між персональними та неперсональними даними не є сталою, оскільки анонімізовані дані за певних умов можуть бути реідентифіковані, а псевдонімізовані зберігають потенціал ідентифікації [175]. Б. Паркінсон описує це через поняття цифрової мозаїки, сформованої сукупністю усіх цифрових слідів особи, яку держава акумулює через множину адміністративних процедур і яка є значно більш інформативною та потенційно небезпечною, ніж будь-який окремий масив даних [177]. Саме ця трансформація об’єкта від статичного до динамічного, від локального до агрегованого, від однозначно ідентифікованого до потенційно реідентифікованого визначає принципово нові вимоги до адміністративно-правової охорони персональних даних в умовах цифровізації публічного управління і обумовлює необхідність переосмислення традиційних правових інструментів їх захисту.

Перелік видів персональних даних не є вичерпним, оскільки будь-яка інформація, яка дозволяє однозначно визначити особу, може бути віднесена

до цієї категорії. Водночас для цілей правового регулювання необхідна систематизація. На основі аналізу [89] складено наступну класифікацію.

Таблиця 1

Класифікація персональних даних

Критерій класифікації	Види персональних даних
за сферою використання	звичайні; працівників; публічних осіб; військовослужбовців та учасників збройного конфлікту; призовників, військовозобов'язаних і резервістів; медичні; у цифровому середовищі
за можливістю поширення	відкриті; конфіденційні
за визначенням приватності	звичайні; чутливі
за правовими режимами захисту	у звичайному стані; у надзвичайному стані; у воєнному стані
за підставами обробки	за згодою суб'єкта; без згоди (відповідно до закону)
за метою обробки	у сфері охорони здоров'я; для ведення військового обліку; для захисту життєво важливих інтересів

*складено самостійно на основі [89]

М. Різак пропонує більш лаконічний поділ на загальні дані (прізвище, ім'я, дата народження), вразливі (расове походження, політичні переконання, дані про здоров'я) та спеціальні (межі обігу яких визначаються самим суб'єктом) [134]. В. Теремецький обґрунтовано зазначає, що базу персональних даних доцільно розглядати у широкому та вузькому значеннях: як будь-які бази персональних даних та як спеціально створені локальні бази персональних даних відповідно [151, с. 5]. В. Балацька пропонує диференціацію за рівнем чутливості:

– ідентифікаційні, фінансові та медичні дані мають високий рівень;

– біометричні потребують критично високого рівня захисту;

– контактні дані та дані про онлайн-активність (IP-адреса, cookies) відповідають середньому;

– соціально-демографічні (вік, стать, освіта) потребують базового [8].

Така градація має практичне значення для сфери публічного управління, оскільки дозволяє визначати відповідні інструменти залежно від характеру даних, що обробляються у конкретній адміністративній процедурі.

Б. Паркінсон пропонує альтернативний підхід до систематизації персональних даних, побудований не на рівні чутливості, а на способі формування даних. Дослідник виокремлює п’ять категорій: digital footprint (дані, свідомо залишені самою особою), third party digital footprint (дані, створені третіми особами), digital mosaic (сукупність усіх слідів), digital persona (профіль, сформований внаслідок аналізу даних) та digitally extended self (повна цифрова репрезентація особи) [177]. Вважаємо цей підхід продуктивним для сфери публічного управління, де державні реєстри фактично формують цифровий образ громадянина шляхом агрегації даних з різних джерел та процедур.

А. Цьоменко пропонує класифікацію за критеріями змістового наповнення та рівня встановленої «доступності», виокремлюючи три групи: загальні (загальнодоступні), спеціальні та біометричні [158, с. 43]. До загальних авторка відносить базові дані про носія як прізвище, ім’я, по батькові, місце реєстрації та проживання, паспортні дані, відомості про освіту, місце роботи, доходи, тобто інформацію, яку можна знайти в публічно доступних базах даних, каталогах, довідковій документації, засобах масової інформації. Спеціальними персональними даними пропонується вважати інформацію щодо участі в політичних партіях та громадських організаціях, віросповідання, переконання світоглядно-філософського характеру, наявність судимості, аспекти інтимного та сексуального життя, дані з реєстрів нерухомого майна. Біометричні персональні дані характеризують носія за біологічним та фізіологічним принципом (дактилоскопічні дані, аналіз ДНК, група крові, зріст, колір очей), при цьому їх різновидами виступають генетичні дані та медичні персональні дані. Такий підхід має практичне значення для сфери публічного управління, оскільки дозволяє диференціювати правовий режим обробки залежно від категорії даних. Органи публічної влади

одночасно оперують усіма трьома групами: загальними (реєстри виборців), спеціальними (реєстри судимостей, дані НАЗК) та біометричними (ID-картки, закордонні паспорти тощо), і кожна група потребує різного рівня організаційного та технічного захисту. Окремо А. Цьоменко пропонує класифікацію за співвідношенням із метою використання на повні персональні дані (що дозволяють з високою ймовірністю ідентифікувати особу), неповні (що відображають лише окремі складові, наприклад, лише номер телефону або адресу проживання) та надмірні (що містять як ідентифікуючу інформацію, так і відомості, які виходять за межі визначеної мети обробки) [158, с. 43]. Цей критерій кореспондує з принципом ненадмірності обробки, закріпленим у частині третій статті 6 Закону № 2297-VI та статті 5 GDPR, саме поняття «надмірних» персональних даних позначає порушення цього принципу.

Пропонуємо доповнити наведені класифікації такими параметрами:

– за характером ідентифікації: прямі (що безпосередньо дозволяють ідентифікувати особу: ім’я, номер паспорта, РНОКПП) та опосередковані (що у поєднанні з іншими даними можуть призвести до ідентифікації: IP-адреса, cookies, геолокація);

– за суб’єктом обробки: публічні (що обробляються органами влади в рамках адміністративних процедур) та приватні (що обробляються суб’єктами господарювання). Таке доповнення має практичне значення, оскільки правовий режим обробки суттєво відрізняється залежно від того, хто є володільцем даних і яким чином здійснюється ідентифікація.

Ефективність процесів збирання, обробки та захисту персональних даних залежить не лише від чіткості понятійного апарату, а й від стану його законодавчого забезпечення. Формування нормативно-правової бази захисту персональних даних в Україні мало тривалу передісторію. Можна виокремити чотири етапи цього процесу: фундаментальний період (1991-2010 рр.), пов’язаний із формуванням базових юридичних положень; етап систематизації (2010-2014 рр.), що характеризується впровадженням спеціального Закону та первинних регуляторних механізмів; період

трансформації інституційної архітектури (2014-2018 рр.), коли контрольні функції було делеговано Уповноваженому ВРУ; етап гармонізації з європейськими нормативами (з 2018 р.), зумовлений синхронізацією з вимогами GDPR.

Відправною точкою формування законодавчої бази щодо персональних даних стали положення Конституції України 1996 року. Стаття 32 визначає, що не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом [63]. Закон України «Про інформацію» вперше запровадив поняття «інформація про фізичну особу», що стало основою сучасної дефініції «персональні дані» [119]. У Рішенні Конституційного Суду України у справі К. Устименка було визначено, що до конфіденційної інформації належать «свідчення про особу (освіта, сімейний стан, релігійність, стан здоров'я, дата і місце народження, майновий стан та інші персональні дані)» [137]. Це рішення фактично створило правову підставу для подальшого нормативного закріплення поняття. В. Пилипчук та В. Брижко зазначають, що протягом 1996-2010 років було опрацьовано вісім версій проекту Закону «Про захист персональних даних», який неодноразово розглядався центральними органами виконавчої влади [91, с. 37]. Лише 1 червня 2010 року Верховна Рада ухвалила Закон № 2297-VI, що дало Україні підстави ратифікувати Конвенцію Ради Європи № 108.

Закон визначив ключові поняття (персональні дані, база персональних даних, володілець, розпорядник, суб'єкт персональних даних), закріпив принципи та умови обробки, окреслив права суб'єктів та обов'язки володільців, передбачив механізм державного контролю [118]. Одним із нововведень стало створення Державної служби України з питань захисту персональних даних на підставі Указу Президента від 9 грудня 2010 року. Ця інституція відповідала за ведення Національного реєстру персональних даних, розгляд скарг, проведення перевірок. Паралельно до Кодексу про адміністративні правопорушення було внесено статтю 188-39, що передбачила

адміністративну відповідальність за порушення законодавства про захист персональних даних. Однак, практична імплементація виявила суттєві проблеми. М. Колотило констатує «надмірну бюрократизацію процедурних аспектів реєстрації баз персональних даних та недостатню ефективність державного контролю» [59, с. 242]. В. Пилипчук та В. Брижко більш категорично характеризуючи ситуацію відзначають, що практика тих років засвідчила «тотальну недієвість закону, відсутність централізованого регулювання, абсолютну нежиттєздатність Державної служби з питань захисту персональних даних» [91, с. 39]. У 2014 році Державну службу було ліквідовано, а функції передано Уповноваженому ВРУ з прав людини. Ключовою зміною стала елімінація обов'язкової реєстрації баз персональних даних, що зменшило адміністративне навантаження на суб'єктів обробки.

Дослідження правової природи персональних даних неможливе без урахування міжнародно-правових стандартів, ратифікованих Україною. О. Гиляка зазначає, що «вперше нормативне закріплення норм з правового регулювання захисту персональних даних відбулося в тих положеннях міжнародних договорів з прав людини, які гарантували право на приватність» [19, с. 19]. Першим юридично зобов'язальним документом у цій сфері стала Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року (ETS № 108). Конвенція надала визначення поняттю «персональні дані», а у ст. 7 зобов'язала сторони вживати заходів безпеки, спрямованих на запобігання випадковому чи несанкціонованому знищенню, доступу, зміні або поширенню [166]. Стаття 5 закріпила базові вимоги стосовно того, що персональні дані мають здобуватися добросовісно і на законних підставах, зберігатися для визначених і законних цілей, бути адекватними, відповідними та ненадмірними, бути точними та актуальними [166]. Україна ратифікувала Конвенцію на підставі Закону від 6 липня 2010 року № 2438-VI, що стало передумовою для прийняття Закону № 2297-VI.

У праві ЄС право на захист персональних даних визнано основоположним, і воно закріплене у Договорі про функціонування ЄС (ст. 16) та Хартії основних прав ЄС (ст. 8). Ці акти є внутрішніми установчими документами ЄС, обов'язковими лише для держав-членів. «Пакет захисту даних» ЄС 2016 року, окрім GDPR, включає Директиву (ЄС) 2016/680 про захист фізичних осіб при обробці даних правоохоронними органами та Директиву (ЄС) 2016/681 про використання даних пасажирів. Директива 2016/680 має особливе значення для нашого дослідження, оскільки регулює обробку персональних даних саме суб'єктами публічного адміністрування, встановлюючи спеціальний правовий режим. Зазначені директиви не є юридично обов'язковими для України, проте їх імплементація є частиною євроінтеграційних зобов'язань, передбачених Угодою про асоціацію та підтверджених набуттям Україною статусу кандидата на членство в ЄС. Стаття 15 розділу III Угоди про асоціацію між Україною та ЄС передбачає співробітництво з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів [154]. Ю. Коваленко підкреслює, що «забезпечення належного рівня захисту персональних даних безпосередньо випливає як з Угоди про асоціацію, так і з набуття Україною офіційного статусу кандидата на членство в ЄС» [53, с. 138]. Починаючи з 2013 року ООН прийняла дві резолюції «Право на приватність у цифрову еру», запровадивши посаду Спеціального доповідача ООН щодо права на приватне життя [184].

Зазначені міжнародні зобов'язання та очевидна невідповідність чинного Закону № 2297-VI європейським стандартам зумовили підготовку нового законопроекту, спрямованого на комплексну імплементацію вимог GDPR у національне законодавство. 25 жовтня 2022 року до Верховної Ради було подано проект Закону «Про захист персональних даних» № 8153, який став чи не найбільш масштабною спробою наблизити українське законодавство до вимог GDPR.

Сформована нормативно-правова база визначає не лише інституційну архітектуру захисту, а й встановлює правила поводження з персональними даними на кожному етапі їх життєвого циклу. Стаття 2 Закону № 2297-VI визначає обробку персональних даних як «будь-яку дію або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем» [118]. Це визначення охоплює весь життєвий цикл даних, від моменту збирання до знищення. Закон визначає три ключових суб'єкти: суб'єкт персональних даних (фізична особа, дані якої обробляються), володілець (визначає мету обробки, встановлює склад даних) і розпорядник (обробляє від імені володільця) [118]. У публічному управлінні вступ у правовідносини часто має обов'язковий характер, оскільки громадянин не може відмовитися від надання даних при зверненні за адміністративними послугами. Орган публічної влади як володілець перебуває у домінуючому становищі, а суб'єкт даних у залежному. Така асиметрія обумовлює необхідність посиленого адміністративно-правового захисту.

Стаття 8 Закону закріплює наступні права суб'єкта: знати про джерела збирання та мету обробки; доступ до своїх даних; внесення змін, блокування або видалення; захист від незаконної обробки; оскарження [118]. О. Гиляка вказує на суттєвий недолік: «закон передбачає можливість видалення персональних даних, але не допускає можливості це зробити особою самостійно. Підставами для видалення можуть бути лише рішення суду або припис Уповноваженого» [19, с. 21]. GDPR суттєво розширив права суб'єктів, закріпивши право на забуття (ст. 17), право на перенесення даних (ст. 20), право на заперечення проти автоматизованого прийняття рішень (ст. 22) [21]. Ці права мають значення для публічного управління, де дедалі більше рішень приймається з використанням автоматизованих систем. А. Гачкевич зазначає, що при навчанні автоматизованих систем та моделей штучного інтелекту

«перетворення персональних даних за допомогою анонімізації, псевдонімізації та синтезації набуває особливого значення» [18, с. 30].

Стаття 11 Закону встановлює наступні підстави для обробки персональних даних: згода суб'єкта; дозвіл відповідно до закону для здійснення повноважень володільця; укладення та виконання правочину; захист життєво важливих інтересів; необхідність захисту законних інтересів володільця персональних даних; необхідність виконання обов'язку, встановленого законом [118]. У сфері публічного управління найбільш поширеною підставою є виконання повноважень, установлених законом. У листі Державної служби з питань захисту персональних даних від 31 грудня 2013 року роз'яснюється: «процеси обробки персональних даних, що здійснюються у випадках, передбачених законами України, не потребують отримання згоди від фізичних осіб» [75]. Це суттєво відрізняє публічну сферу від приватної, де переважає обробка на підставі згоди.

Стаття 7 Закону № 2297-VI забороняє обробку персональних даних про «расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних» [118]. Водночас частина друга цієї статті містить вичерпний перелік винятків, за наявності яких обробка допускається, а саме: за однозначною згодою суб'єкта; для здійснення прав та виконання обов'язків володільця у сфері трудових правовідносин; для захисту життєво важливих інтересів суб'єкта або іншої особи; релігійними організаціями, громадськими організаціями та політичними партіями щодо даних їх членів; для обґрунтування або захисту правової вимоги; в цілях охорони здоров'я (встановлення діагнозу, лікування, функціонування електронної системи охорони здоров'я); для ведення військового обліку призовників, військовозобов'язаних та резервістів; у зв'язку з виконанням завдань оперативно-розшукової чи контррозвідувальної діяльності; а також якщо дані були явно оприлюднені самим суб'єктом. Стаття

9 GDPR встановлює аналогічну заборону обробки чутливих даних, однак містить суттєві змістовні відмінності порівняно з українським законодавством. Зазначимо, що GDPR передбачає окрему підставу для обробки з причин суттєвого суспільного інтересу (п. «g» ст. 9), яка є принципово важливою для сфери публічного управління, оскільки дозволяє обробляти чутливі дані без згоди суб'єкта за умови пропорційності та наявності спеціальних гарантій [180]. Чинний Закон № 2297-VI такої підстави не містить, що створює правову невизначеність у діяльності органів публічної влади, які об'єктивно потребують обробки чутливих даних для виконання своїх функцій. Окремо GDPR виділяє підставу для обробки в цілях суспільного здоров'я, зокрема захисту від серйозних транскордонних загроз (п. «i» ст. 9), а також для наукових, історичних та статистичних досліджень (п. «j» ст. 9). В українському законодавстві обробка медичних даних врегульована значно вужче і прив'язана до конкретного кола суб'єктів: медичних працівників, працівників НСЗУ, Пенсійного фонду та Фонду соціального захисту осіб з інвалідністю [118]. Зауважимо також, що GDPR наскрізно закріплює вимогу пропорційності кожного винятку визначеній меті та передбачає «належні та спеціальні заходи для захисту фундаментальних прав» суб'єкта. Закон № 2297-VI формулює винятки без такої вимоги, що знижує рівень гарантій прав суб'єктів персональних даних. Зазначені розбіжності підтверджують необхідність імплементації у проекті нового Закону не лише нових категорій даних, а й оновленої системи підстав обробки чутливих даних з обов'язковим закріпленням принципу пропорційності.

Аналіз наукових підходів та нормативного регулювання дозволяє обґрунтувати адміністративно-правову природу охорони персональних даних у сфері публічного управління. Конституційно-правова охорона забезпечує фундаментальний рівень захисту. Стаття 32 Конституції України гарантує право на недоторканність приватного життя [63], однак вона визначає тільки загальне явище захисту. Цивільно-правова охорона ефективна у відносинах між приватними особами і орієнтована на компенсацію шкоди після факту

порушення. Жоден із цих підходів не є достатнім для сфери публічного управління, де органи влади є домінуючим суб'єктом обробки персональних даних, а правовідносини між ними і громадянином є за своєю природою владно-управлінськими, а не рівноправними. Саме адміністративне право як галузь, що регулює відносини у сфері публічного управління, здатне забезпечити три необхідних виміри охорони: нормативний через встановлення обов'язкових правил обробки даних для суб'єктів публічного адміністрування; інституційний через визначення наглядових органів та механізмів контролю; та юрисдикційний через систему адміністративної відповідальності і порядок оскарження неправомірних дій. Це і визначає персональні дані у сфері публічного управління як специфічний об'єкт адміністративно-правової охорони, що відрізняє їх від об'єктів конституційно-правового чи цивільно-правового регулювання.

Сформована система принципів, разом із проаналізованим понятійним апаратом, дозволяє перейти до формулювання визначення персональних даних у контексті публічного управління. Публічне управління (адміністрування), за визначенням В. Галунька, є діяльністю уповноважених суб'єктів щодо практичної реалізації функцій виконавчої влади [3, с. 103]. Н.Т. Головацький стверджує, що «публічна адміністрація відіграє ключову роль у цій сфері, адже саме вона володіє персональними даними своїх громадян» [22, с. 331]. Адміністративно-правова природа обробки і захисту персональних даних у сфері публічного управління обумовлена багатьма факторами.

На підставі проведеного аналізу доктринальних підходів, нормативних визначень та специфіки обробки даних як об'єкта адміністративно-правової охорони пропонуємо таке визначення: персональні дані у контексті публічного управління це будь-які відомості чи сукупність відомостей (прямих або опосередкованих) про фізичну особу, яка ідентифікована або може бути ідентифікована, що збираються, зберігаються та обробляються суб'єктами публічного адміністрування в рамках адміністративних процедур, у тому числі із застосуванням цифрових технологій та інтегрованих

інформаційних систем, на підставі та у спосіб, визначені законом, з метою реалізації публічно-владних повноважень та забезпечення прав і законних інтересів особи. Таке визначення враховує широкий підхід до ідентифікації, специфіку суб'єктів, процедурні особливості, правову підставу та дуальну мету (реалізація публічно-владних повноважень та забезпечення прав особи).

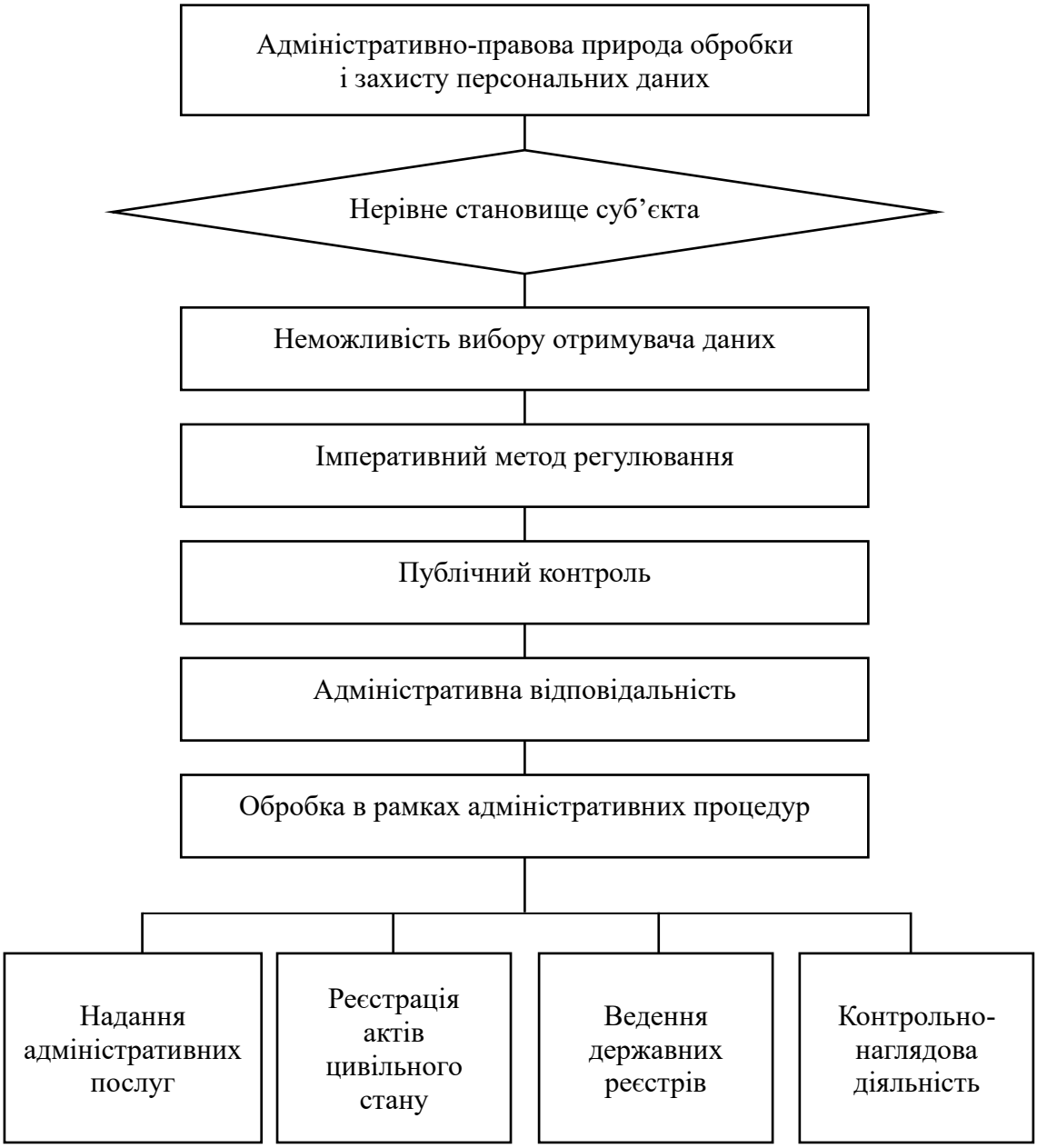

Рис. 1.1. Адміністративно-правова природа обробки і захисту персональних даних у сфері публічного управління (розроблено автором)

О. Дяковський зазначає, що стан захищеності персональних даних є «юридично забезпеченим рівнем безпеки персональної інформації, при якому гарантується її конфіденційність, цілісність, доступність, а також дотримання прав суб'єктів даних» [35]. Досягнення такого стану потребує консолідації зусиль щодо персональної безпеки володільця даних, організаційних і правових заходів держави, діяльності громадських організацій. Важлива проблема у сфері захисту персональних даних в Україні полягає у відсутності ефективної загальнодержавної системи захисту, належного організаційно-правового механізму регулювання відносин та відповідальності за правопорушення. Подальше вдосконалення адміністративно-правового регулювання потребує врахування викликів цифрової трансформації, інтенсифікації міжнародної співпраці та розбудови інструментів як державного нагляду, так і саморегулювання у сфері обробки персональних даних. К. Бершадська обґрунтовано зазначає, що без комплексного захисту персональних даних від незаконного доступу особа не зможе повноцінно реалізувати свої права [12]. У публічному управлінні ця теза набуває додаткового виміру, так як персональні дані є не лише засобом ідентифікації, а й інструментом реалізації владних повноважень, що покладає на державу підвищену відповідальність за їх захист.

Пропонуємо захист персональних даних у сфері публічного управління визначити як систему адміністративно-правових засобів (норм, процедур, інституцій, заходів контролю та відповідальності), спрямованих на забезпечення конфіденційності, цілісності та доступності персональних даних, що обробляються суб'єктами публічного адміністрування, з метою недопущення їх незаконного збирання, використання, поширення або знищення та гарантування прав суб'єктів персональних даних. Це визначення відображає комплексний характер захисту та його адміністративно-правову природу.

Воєнний стан, введений Указом Президента України від 24 лютого 2022 року № 64/2022, суттєво трансформував правовий режим персональних даних

як об’єкта охорони [101]. Персональні дані набули стратегічного виміру національної безпеки. З одного боку, держава розширила підстави для їх обробки без згоди суб’єкта, з іншого усвідомлення їх цінності для противника зумовило посилення фактичного захисту. Ця суперечність між необхідністю обмеження прав суб’єктів в умовах збройного конфлікту та вимогами пропорційності, що випливають із міжнародних стандартів, є одним із ключових викликів для адміністративно-правового регулювання і детально розглядається у наступних розділах цієї роботи.

1.2. Цифровізація публічного управління як чинник трансформації правовідносин у сфері захисту персональних даних

Системний аналіз цифровізації публічного управління як чинника трансформації правовідносин у сфері захисту персональних даних потребує попереднього з’ясування змісту базового поняття «управління», оскільки саме воно визначає предметні межі дослідження та конкретизує суб’єктний склад відповідних правовідносин.

Етимологічно поняття «управління» у найширшому сенсі означає цілеспрямований вплив суб’єкта на об’єкт з метою досягнення визначеного результату. У теорії держави і права управління традиційно розглядається як різновид соціального управління, або свідомої, організованої діяльності людей, спрямованої на впорядкування суспільних відносин. Загальна теорія управління виокремлює три його ключові ознаки, а саме: наявність суб’єкта та об’єкта управлінського впливу, цілеспрямованість такого впливу та наявність зворотного зв’язку між суб’єктом і об’єктом [37].

У правовій науці поняття «управління» набуває специфічного змісту залежно від того, хто виступає суб’єктом управлінської діяльності. Саме за цим критерієм традиційно розмежовуються поняття «державне управління» та «публічне управління». Державне управління як категорія пострадянської

адміністративно-правової доктрини охоплює діяльність органів виконавчої влади щодо практичного виконання законів та реалізації державної політики. В. Авер'янов визначав державне управління як «підзаконну, юридично владну діяльність органів виконавчої влади, яка полягає у практичній реалізації завдань і функцій держави шляхом безпосереднього керівництва економічною, соціально-культурною та адміністративно-політичною сферами суспільного життя» [1, с. 262]. Ця концепція відображала модель, за якої держава є єдиним джерелом публічної влади, а управлінська функція зосереджена виключно в апараті виконавчої влади.

Водночас сучасна адміністративно-правова доктрина дедалі більше оперує поняттям «публічне управління», яке є ширшим за змістом і відображає демократичну модель організації влади. Публічне управління охоплює не лише діяльність органів виконавчої влади, а й діяльність органів місцевого самоврядування, а також інших суб'єктів, наділених публічно-владними повноваженнями. Тобто публічним управлінням є організуючий вплив усієї системи органів публічної влади на суспільну життєдіяльність людей з метою її впорядкування та збереження або перетворення, що спирається на владні повноваження [2].

Таким чином, співвідношення понять «публічне управління» та «державне управління» будується за принципом «ціле та його частина», де державне управління є складовою публічного управління, здійснюваною органами державної виконавчої влади, тоді як публічне управління охоплює також управлінську діяльність органів місцевого самоврядування та інших суб'єктів, що реалізують публічно-владні функції. Для цілей цього дослідження важливим є те, що обробка персональних даних здійснюється всіма суб'єктами публічного управління у широкому розумінні, як органами виконавчої влади, так і органами місцевого самоврядування, що й зумовлює вибір категорії «публічне управління» як аспекту дослідження.

Зазначена концептуальна основа є необхідною передумовою для розуміння того, яким чином цифровізація впливає на зміст, суб'єктний склад

та характер правовідносин у сфері захисту персональних даних у системі публічного управління.

Цифровізація публічного управління є явищем, що докорінно змінює не лише форму, а й зміст взаємодії між державою та громадянином. Цифрові технології виступають каталізатором підвищення ефективності та прозорості публічного адміністрування, дозволяючи зменшити транзакційні витрати, мінімізувати корупційні ризики та забезпечити передбачуваність адміністративних процедур [84, с. 164]. На відміну від суто технічної модернізації, яка передбачає автоматизацію окремих операцій, цифровізація трансформує саму архітектуру владних відносин через спосіб прийняття управлінських рішень, механізми надання публічних послуг, обсяг і характер даних, що циркулюють у системі публічного адміністрування. Це має важливе значення, оскільки саме цифровізація створила передумови для якісної зміни характеру, масштабу та ризиків обробки персональних даних у сфері публічного управління, що, своєю чергою, зумовлює необхідність відповідного адміністративно-правового забезпечення.

Термін «цифровізація» був уведений у науковий обіг у 1995 році Н. Негропонте, який обґрунтував неминучість переходу від матеріального («атомного») до цифрового («бітового») виміру суспільних процесів [176]. О. Савченко, систематизуючи наукові підходи до поняття «цифровізація у публічному управлінні», зазначає, що у вузькому сенсі цифровізація означає перетворення інформації у цифрову форму, тоді як у широкому є трендом ефективного світового розвитку, що охоплює як виробництво, бізнес і науку, так і соціальну сферу та публічне управління [145, с. 73]. Дослідник пропонує визначення цифровізації публічного управління як «використання цифрових технологій, можливостей онлайн-комунікацій у системі прийняття та реалізації державно-управлінських рішень, надання адміністративних послуг, формування дієвих державних механізмів реалізації державної політики у всіх сферах життєдіяльності суспільства» [145, с. 74]. Н. Атаманова та І. Луняченко підкреслюють, що цифровізація публічного управління не зводиться до

запровадження електронних сервісів, а передбачає комплексну трансформацію правовідносин у сфері публічної адміністрації, охоплюючи впровадження електронних адміністративних послуг, створення єдиних електронних реєстрів, розвиток цифрової ідентифікації та довірчих сервісів, формування стандартів кібербезпеки і механізмів автоматизованого прийняття управлінських рішень [5, с. 7].

На нашу думку, принципово важливим є розмежування понять «інформатизація» та «цифровізація», оскільки вони відображають різний рівень технологічного рівня публічного управління і, відповідно, неоднаковий характер впливу на правовідносини у сфері персональних даних.

О. Нестеренко констатує, що попри прийняття ще у 1998 році Закону «Про Національну програму інформатизації» та початок створення інформаційних систем як інфраструктурних елементів, ці кроки залишались фрагментарними через відсутність фінансування та суперечливість нормативно-правової бази, що засвідчило існуючий розрив між потребами суспільства та станом інформатизації державного управління [86, с. 9]. Інформатизація передбачала оцифрування існуючих паперових процесів, тобто перехід від паперових носіїв до електронних без зміни самої логіки управління. Проте, обробка персональних даних залишалася обмеженою рамками конкретного органу, а обсяг оброблюваних відомостей визначався функціональними потребами конкретної управлінської процедури.

Н. Сорокіна та В. Філатов, досліджуючи теоретичні підходи до цифровізації публічного управління, обґрунтовують розмежування двох підходів: технічного, що зосереджується на впровадженні цифрових технологій як інструменту автоматизації існуючих процесів, та трансформаційного, що розглядає цифровізацію як процес кардинальної зміни моделі публічного управління [150, с. 78]. Автори наголошують, що цифровізація публічного управління є системним трансформаційним процесом, який передбачає інтеграцію цифрових технологій в усі аспекти діяльності органів публічної влади з метою не лише автоматизації та

оптимізації управлінських процесів, а й глибокої зміни самої моделі управління. На такому рівні з'являється можливість електронної взаємодії між органами влади, що передбачає обмін персональними даними між різними суб'єктами публічної адміністрації, що працює у системі «паперового управління».

С. Ненько уточнює, що правове регулювання цифровізації публічного адміністрування в Україні формується на конституційному, законодавчому та підзаконному рівнях [84, с. 162]. Цифровізація, як зауважує М. Дубняк, передбачає не просто електронну форму реалізації існуючих процедур, а переосмислення самих процедур, їх реінжиніринг на основі можливостей цифрових технологій, включаючи впровадження штучного інтелекту, автоматизованого прийняття рішень та Smart-управління [33]. На такому рівні персональні дані стають не допоміжним елементом, а центральним ресурсом управлінського процесу, оскільки без доступу до даних з множини реєстрів, без їх агрегації та аналітичної обробки цифрове публічне управління неможливе. В. Медяник обґрунтовує, що цифрова трансформація соціальної сфери є «не просто запровадженням нових технологій, а фундаментальною зміною змісту та форм здійснення публічної влади, і пропонує розглядати цифровізацію як прояв нового етапу еволюції адміністративного права, що полягає у переході від паперово-орієнтованої моделі до цифрової адміністративно-правової парадигми» [80, с. 226].

Описані технологічні зміни тягнуть за собою якісну трансформацію структури адміністративно-правових відносин у сфері захисту персональних даних. Насамперед змінюється суб'єктний склад, і поряд із традиційними суб'єктами (органом публічної влади і громадянином) з'являються нові учасники правовідносин (оператори цифрових платформ, адміністратори реєстрів, треті особи, що отримують доступ до даних через системи міжвідомчого обміну), кожен із яких має власний правовий статус, обсяг повноважень і міру відповідальності, що у чинному законодавстві чітко не визначена. Трансформується і сам об'єкт правовідносин, оскільки персональні

дані перестають бути статичним масивом відомостей у конкретній базі і перетворюються на динамічний ресурс, що безперервно агрегується, передається і змінює свій правовий режим залежно від контексту обробки. Якісно змінюється і зміст прав та обов'язків сторін. Суб'єкт даних формально зберігає права, закріплені у Законі № 2297-VI, проте реальна можливість їх реалізації в умовах інтероперабельних реєстрів і автоматизованих рішень є суттєво обмеженою порівняно з традиційною моделлю. Нарешті, змінюється сам характер правового зв'язку між державою і громадянином. Якщо в умовах паперового управління взаємодія була епізодичною і прив'язаною до конкретної адміністративної процедури, то цифрове публічне управління формує постійний і багатовимірний інформаційний зв'язок, за якого держава акумулює відомості про громадянина з множини джерел незалежно від його активних звернень. Ця трансформація вимагає відповідного переосмислення адміністративно-правового інструментарію захисту персональних даних.

Зазначена трансформація породжує питання, яке традиційна теорія адміністративного права не розглядала, а саме чи зберігається класична конструкція адміністративних правовідносин як владно-управлінського зв'язку між суб'єктом публічної адміністрації і приватною особою в умовах, коли держава акумулює персональні дані громадянина не лише у рамках конкретної адміністративної процедури, а безперервно і з множини джерел. Правовий статус суб'єкта даних у цифровому публічному управлінні набуває принципово нових характеристик. З пасивного учасника окремих адміністративних процедур він перетворюється на постійний об'єкт інформаційної присутності держави, що суттєво змінює баланс між публічним інтересом і правом на приватність. Окрім того, цифровізація породжує новий тип правовідносин, якого не знало традиційне адміністративне право, а саме відносини між суб'єктом даних і алгоритмом, що приймає управлінське рішення без участі посадової особи. У цих відносинах відсутній традиційний суб'єкт владних повноважень у розумінні людини, яка несе персональну

відповідальність за рішення, що суттєво ускладнює реалізацію права на оскарження і захист.

Структурною характеристикою правовідносин у цифровому публічному управлінні, що залишається поза увагою чинного законодавства, є феномен інформаційної асиметрії між державою і громадянином. В умовах традиційного паперового управління обсяг відомостей, якими держава володіла про конкретного громадянина, був обмежений рамками окремих адміністративних процедур і розпорошений між різними органами. Цифровізація принципово змінила цей баланс, оскільки агрегація даних з множини реєстрів через інтероперабельні системи дозволяє державі формувати комплексний цифровий профіль громадянина, тоді як сам громадянин, як правило, не знає, які саме органи, коли і з якою метою отримували доступ до його відомостей. Вважаємо, що ця асиметрія є не технічною випадковістю, а структурною характеристикою цифрового публічного управління, і саме вона визначає необхідність закріплення права громадянина на повну прозорість щодо обробки його персональних даних.

Таким чином, пропонуємо визначити цифровізацію публічного управління як комплексний правовий та організаційно-технологічний процес трансформації діяльності суб’єктів публічної адміністрації, що полягає у системному впровадженні цифрових технологій у прийняття та реалізацію управлінських рішень, надання адміністративних послуг та взаємодію з громадянами, передбачаючи перехід від паперово-орієнтованої до цифрової моделі публічного адміністрування. Істотною ознакою дефініції є те, що персональні дані громадян перестають бути допоміжним елементом управлінського процесу і перетворюються на його центральний ресурс, без якого функціонування цифрового публічного управління стає неможливим. Це визначення відрізняється від існуючих тим, що акцентує увагу не лише на технологічному, а й на правовому аспекті трансформації, підкреслюючи зміну ролі персональних даних у системі публічного управління.

Для розуміння того, як саме цифровізація трансформувала правовідносини у сфері захисту персональних даних, варто простежити етапи її формування в Україні. Р. Кірін, розробляючи дворівневу модель періодизації розвитку законодавства про е-урядування, виокремлює кілька послідовних етапів:

– інформаційний (підготовчий) етап 1992-1998 рр.;

– етап першої Національної програми інформатизації 1998-2010 рр. (з періодами інформатизації, інтернетизації, телекомунікації та електронізації);

– етап першої Концепції розвитку е-урядування 2010-2017 рр. (з періодами формування та сталого розвитку);

– етап другої Концепції розвитку е-урядування 2017-2023 рр. (з періодами євроінтеграційного розвитку та цифровізації економіки) та етап другої Національної програми інформатизації 2023-2025 рр. [50, с.23].

Ця періодизація дозволяє простежити еволюцію нормативної бази, що регулює обробку персональних даних у публічному управлінні. На інформаційному етапі (1992-1998 рр.) було закладено конституційні основи захисту інформації про особу. Закон України «Про інформацію» від 2 жовтня 1992 року вперше запровадив категорію «інформація про фізичну особу» та визначив основні засади інформаційних відносин. Стаття 32 Конституції України 1996 року закріпила заборону збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди. Водночас органи публічної влади здійснювали обробку даних громадян переважно у паперовій формі, а обсяг такої обробки був обмежений функціональними потребами конкретного органу. Кожен орган влади вів власні картотеки, журнали, реєстри, які не були інтегровані між собою, що природним чином обмежувало масштаб і ризики обробки персональних даних. Характерною рисою цього періоду була відсутність спеціального закону про захист персональних даних, а норми ст. 32 Конституції мали загальний характер і не деталізували механізмів захисту.

Етап першої Національної програми інформатизації (1998-2010 рр.) ознаменувався початком системного впровадження інформаційних технологій у публічне управління. Закон України «Про Національну програму інформатизації» від 4 лютого 1998 року № 74/98-ВР (на сьогодні втратив чинність) визначив стратегічні напрями інформатизації державних органів [120]. Закон України «Про електронні документи та електронний документообіг» від 22 травня 2003 року № 851-IV встановив правовий режим електронних документів, визнавши їх юридичну силу рівнозначною паперовим. При цьому обов'язковою умовою є дотримання вимог до електронного підпису [108]. Цей закон фактично легалізував електронну обробку персональних даних в органах влади, проте не передбачив спеціальних вимог до захисту таких даних при електронному документообігу. На цьому етапі почали створюватися перші електронні бази даних та реєстри: Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців, Державний реєстр фізичних осіб-платників податків, Єдиний державний демографічний реєстр. С. Крамський, О. Дарушин та О. Захарченко, простежуючи еволюцію електронного урядування, відзначають, що саме у цей період відбувся перехід від епізодичного використання комп'ютерних технологій до формування цілісної інфраструктури електронного урядування [72]. Для правовідносин у сфері захисту персональних даних цей етап став переломним, оскільки тепер уперше виникла ситуація, коли персональні дані громадян стали зберігатися у централізованих електронних базах, доступних для значної кількості державних службовців, що створило принципово нові ризики несанкціонованого доступу, витоку та неконтрольованого поширення. Показово, що спеціальний закон щодо персональних даних було прийнято лише у 2010 році, тобто після більш ніж десятиліття функціонування електронних реєстрів без належного правового режиму захисту.

Якісно новий етап розпочався з прийняттям Концепції розвитку електронного урядування в Україні, схваленої розпорядженням Кабінету Міністрів України від 13 грудня 2010 року № 2250-р [126]. Концепція

визначила стратегічні пріоритети електронного урядування, зокрема створення єдиного веб-порталу адміністративних послуг, забезпечення електронної взаємодії між органами влади та впровадження електронного документообігу. Саме у цей період було прийнято два ключові закони: «Про захист персональних даних» № 2297-VI, який уперше запровадив спеціальний правовий режим обробки персональних даних [118], та «Про адміністративні послуги» від 6 вересня 2012 року № 5203-VI, який визначив правові засади надання адміністративних послуг через центри надання адміністративних послуг (ЦНАПи) та закріпив принцип «єдиного вікна» [99]. Хронологія прийняття цих актів та Концепції е-урядування відображає усвідомлення того, що розширення електронної взаємодії між державою та громадянином потребує відповідних правових гарантій. Водночас Р. Кірін слушно зауважує, що на етапі формування е-урядування (2010-2014 рр.) нормативне регулювання мало переважно рамковий характер і не враховувало специфіки масштабної цифрової обробки даних [50]. Закон № 2297-VI був орієнтований на традиційну модель, за якої володілець бази даних чітко ідентифікований, обсяг даних обмежений, а процеси обробки є лінійними і прогнозованими. Закон «Про адміністративні послуги» не містив спеціальних норм щодо захисту персональних даних при наданні послуг у електронному форматі, обмежившись загальним посиланням на законодавство про захист інформації.

Період сталого розвитку е-урядування (2014-2017 рр.) збігся з підписанням Угоди про асоціацію між Україною та ЄС, яка у ст. 15 розділу III передбачає співробітництво з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів [154]. Цей період характеризувався активним розвитком електронних публічних послуг, зокрема запроваджено систему електронних петицій, розпочато роботу Єдиного державного порталу адміністративних послуг, створено систему ProZorro. Закон України «Про електронну ідентифікацію та електронні довірчі послуги» від 5 жовтня 2017 року № 2155-VIII (у первісній редакції – «Про електронні довірчі послуги») визначив

правові засади електронної ідентифікації та надання довірчих послуг, замінивши попередній Закон «Про електронний цифровий підпис» [110]. Цей закон створив правову основу для подальшого впровадження кваліфікованого електронного підпису та дистанційної ідентифікації, які згодом стали технологічним фундаментом платформи «Дія». К. Нестеренко зазначає, що саме у цей час закладалися підвалини для переходу від окремих електронних сервісів до інтегрованої цифрової екосистеми [85]. У 2016 році Постановою Кабінету Міністрів України від 8 вересня 2016 року № 606 було затверджено Положення про систему електронної взаємодії державних електронних інформаційних ресурсів «Трембіта» [28], яка стала технологічною основою для міжреєстрового обміну даними. Одночасно зростав і масштаб обробки персональних даних, за якого кожна нова електронна послуга передбачала збирання, зберігання та передачу відомостей про громадян між різними суб’єктами публічної адміністрації.

Якісний стрибок у цифровізації публічного управління відбувся у 2019-2020 роках із створенням Міністерства цифрової трансформації України та запуском екосистеми «Дія». Портал та мобільний застосунок «Дія» стали інтегрованою платформою, через яку громадяни отримують електронні документи, адміністративні послуги та здійснюють юридично значущі дії. М. Тимченко, досліджуючи розвиток сервісу «Дія» в умовах війни, констатує, що екосистема «Дія» перетворилася на основний інструмент реалізації принципу «сервісної держави», забезпечуючи безперервність надання публічних послуг навіть в умовах повномасштабної збройної агресії [152]. Для правовідносин у сфері захисту персональних даних поява «Дії» означала принципову зміну парадигми. Якщо раніше кожен орган публічної влади обробляв персональні дані автономно в межах своєї компетенції, то інтегрована платформа передбачає агрегацію даних з різних джерел в єдиному цифровому просторі.

Функціонування «Дії» безпосередньо залежить від правового режиму електронної ідентифікації. Закон № 2155-VIII (у редакції Закону від 1 грудня 2022 року № 2801-IX) запровадив триступеневу систему рівнів довіри до

засобів ідентифікації (низький, середній, високий), кожен з яких передбачає різний обсяг ідентифікаційних даних та різний ступінь їх верифікації [110]. Для отримання більшості публічних послуг через «Дію» необхідний середній або високий рівень довіри, що передбачає обробку значного обсягу персональних даних, включаючи біометричні. Закон визначає ідентифікаційні дані особи як набір даних, які дають змогу встановити фізичну або юридичну особу, проте не містить вичерпного переліку таких даних та не встановлює спеціальних обмежень щодо їх обсягу, що створює ситуацію, коли обсяг оброблюваних даних визначається не законом, а технічними рішеннями розробників. Закон також запровадив поняття гаманець з цифровою ідентифікацією як «засіб ідентифікації, що дає змогу користувачу надавати на запит третіх осіб інформацію про ідентифікаційні дані, здійснювати електронну ідентифікацію та автентифікацію для надання послуги, створювати кваліфіковані електронні підписи та/або печатки» [110]. Фактично мобільний застосунок «Дія» виконує функції такого гаманця, агрегуючи ідентифікаційні документи, засоби підпису (Дія.Підпис) та механізми автентифікації.

Сервіс «Дія.Підпис» є кваліфікованим електронним підписом, що формується за допомогою мобільного застосунку без зовнішніх носіїв ключів. Для його створення та використання здійснюється обробка біометричних даних (фотозображення обличчя для фотоверифікації), ідентифікаційних даних з Єдиного державного демографічного реєстру та даних електронних документів. Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» від 20 листопада 2012 року № 5492-VI визначає правові засади функціонування цього реєстру, який містить оцифроване зображення обличчя, відбитки пальців рук, демографічні дані та відомості про документи громадянина [111]. «Дія» отримує доступ до цих даних через систему «Трембіта», що означає передачу біометричних і демографічних даних між реєстрами, кожна з яких є окремою операцією обробки персональних даних.

Ні Закон № 2155-VIII, ні Закон № 5492-VI не містять спеціальних норм щодо захисту даних, що обробляються через інтегровані цифрові платформи, обмежуючись відсилкою (бланкетною нормою) до загального Закону № 2297-VI.

Аналіз архітектури екосистеми «Дія» засвідчує, що українська модель цифрового публічного управління будувалася переважно за принципом максимальної ефективності та зручності для громадянина (efficiency by design), а не за принципом захисту персональних даних за замовчуванням (privacy by design). Принцип privacy by design, закріплений у ст. 25 GDPR та визнаний одним із ключових стандартів сучасного законодавства про захист даних, передбачає, що технічні та організаційні заходи захисту персональних даних мають бути інтегровані у систему на етапі її проєктування, а не додаватися постфактум. В українському законодавстві цей принцип не закріплений ні у чинному Законі № 2297-VI, ні у спеціальних актах про цифрове публічне управління, однак його запровадження пропоноване проектом Закону № 8153.

Наочною ілюстрацією підходу efficiency by design є комплексна послуга «єМалятко», запроваджена через «Дію» для автоматичної реєстрації новонародженої дитини. При зверненні за цією послугою відбувається одночасний обмін даними між кількома реєстрами: пологовий будинок передає медичні дані, органи РАЦС здійснюють державну реєстрацію народження, Пенсійний фонд присвоює реєстраційний номер облікової картки платника податків, органи соціального захисту оформлюють допомогу при народженні. Весь цей процес відбувається автоматично, без окремих звернень батьків до кожного органу. З точки зору зручності це є безумовним досягненням, проте з точки зору захисту персональних даних виникає низка питань, чи надається батькам повна інформація про те, між якими саме реєстрами відбувається обмін даними їхньої дитини; чи мають батьки можливість обмежити обсяг даних, що передаються окремим органам; чи існує механізм контролю за подальшим використанням цих даних кожним із

реципієнтів. Аналогічні питання виникають щодо сервісу share-ID у «Дії», який дозволяє громадянам надавати доступ до своїх ідентифікаційних даних третім особам (банкам, страховим компаніям, операторам зв'язку). Хоча цей сервіс передбачає надання згоди, механізм відкликання згоди та видалення даних, що вже були передані третій особі, залишається нормативно невизначеним.

Масштаб обробки персональних даних в екосистемі «Дія» стає очевидним при аналізі конкретних сервісів, запроваджених протягом 2020-2025 років. Цифрові документи (електронний паспорт, посвідчення водія, свідоцтво про реєстрацію транспортного засобу, студентський квиток, довідка ВПО) передбачають обробку ідентифікаційних та біометричних даних, що верифікуються через Єдиний державний демографічний реєстр. Програма «єПідтримка» передбачає обробку фінансових даних, зокрема банківських реквізитів та історії транзакцій. Програма «єВідновлення» оперує даними про адресу об'єкта нерухомості, характер та обсяг пошкоджень, правовстановлюючі документи, фотографічну та відеофіксацію. Сервіс реєстрації внутрішньо переміщених осіб обробляє відомості про попереднє та актуальне місце проживання, склад сім'ї, наявність малолітніх дітей, інвалідність, належність до вразливих категорій. Сервіс «єВорог» передбачає фіксацію свідчень про воєнні злочини, що включає геолокаційні дані, фотографії, відео та текстові описи подій, тобто виключно чутливу інформацію, розголошення якої може створити загрозу для життя осіб, що її надали. Отже, сукупність сервісів екосистеми «Дія» фактично перетворила державу на найбільшого агрегатора персональних даних в Україні.

Система електронної взаємодії державних електронних інформаційних ресурсів «Трембіта», побудована на удосконаленій естонській платформі X-Road. Правовий режим «Трембіти» визначається Положенням, затвердженим Постановою Кабінету Міністрів України від 8 вересня 2016 року № 606 [28]. Система є децентралізованою, тобто вона не передбачає централізації даних та зміни їх власника, забезпечуючи доступ до даних державних реєстрів

різними установами відповідно до визначених повноважень. Ю. Хохлачова та співавтори, аналізуючи моделі цифрових платформ, підкреслюють, що вибір архітектурної моделі визначає не лише технічні характеристики, а й ступінь інтеграції даних та можливості реінжинірингу бізнес-процесів [156]. С. Пороскун зазначає, що «Трембіта» дає змогу реалізувати принцип «тільки раз», за яким громадянин не зобов'язаний надавати одні й ті самі дані різним органам влади [95]. Зручність цього принципу є безсумнівною, проте його реалізація породжує питання. Суб'єкт даних у цій ситуації не може контролювати, які саме органи, з якою метою та в якому обсязі отримують доступ до його персональних даних через систему міжреєстрової взаємодії.

Первісна редакція Постанови № 606 про Деякі питання електронної взаємодії електронних інформаційних ресурсів, містила лише загальні вимоги щодо захисту інформації, не передбачаючи спеціальних механізмів контролю за обробкою персональних даних. Фактично суб'єкт даних не мав правових інструментів для з'ясування того, які органи, коли та з якою метою отримували доступ до його відомостей. Цю прогалину було частково усунено Постановою Кабінету Міністрів України від 1 жовтня 2025 року № 1244, якою запроваджено підсистему моніторингу доступу до персональних даних [105]. Відповідно до оновленої редакції, суб'єкти електронної взаємодії зобов'язані здійснювати реєстрацію декларацій про мету передачі персональних даних, передавати унікальний ідентифікатор декларації суб'єкту, який планує отримувати інформацію, та забезпечувати обмін даними виключно із застосуванням підсистеми моніторингу. Запровадження цього механізму засвідчує визнання державою проблеми неконтрольованого обігу персональних даних. Водночас механізм має суттєві обмеження: він запроваджений на рівні підзаконного акту, тоді як питання фундаментальних прав мають регулюватися законом; не передбачено прямого права громадянина переглядати журнал доступу до своїх даних; не визначено правових наслідків порушення вимог реєстрації декларацій; перехідні положення дозволяють обмін без підсистеми моніторингу до забезпечення

практичної технічної сумісності, тобто повне впровадження відтерміновано на невизначений строк.

Проблема неконтрольованого обігу даних набуває особливої гостроти в контексті принципу пропорційності, закріпленого Законом України «Про адміністративну процедуру» від 17 лютого 2022 року № 2073-IX [100]. Пропорційність передбачає, що обробка персональних даних має бути адекватною, відповідною та не надмірною стосовно мети. О. Тур, досліджуючи цифровізацію на рівні територіальних громад, констатує, що органи місцевого самоврядування отримують через «Трембіту» доступ до даних центральних реєстрів, проте рівень їх технічної та організаційної спроможності забезпечити захист цих даних суттєво відрізняється від рівня центральних органів [153].

Ще одним складним питанням є цифрова нерівність та її вплив на захист персональних даних. Попри стрімкий розвиток цифрових послуг, значна частина громадян не має можливості або навичок для самостійного користування електронними сервісами. До них відносяться літні особи, мешканці територій з низьким рівнем інтернет-покриття, жителі окупованих та прифронтових територій, почасту особи з інвалідністю. В. Клочан та І. Петрів фіксують, що процес цифровізації стикається з об’єктивними бар’єрами, а саме нестачею фінансування, недостатньою кваліфікацією персоналу та низькою цифровою спроможністю окремих громад [52, с. 167]. Громадяни, які не можуть самостійно скористатися електронними послугами, змушені звертатися до працівників ЦНАПів або родичів, передаючи облікові дані, коди доступу та конфіденційну інформацію. Посередник отримує фактичний доступ до всього цифрового профілю громадянина в «Дії», а правовий режим такого делегованого доступу залишається нормативно невизначеним. К. Рябець підтверджує, що навіть масштабні освітні ініціативи не здатні повністю усунути цифровий розрив у короткостроковій перспективі [142]. Адміністративно-правове забезпечення захисту персональних даних повинно передбачати спеціальні механізми для осіб, які здійснюють доступ

через посередників, зокрема обов'язкову фіксацію факту делегованого доступу, обмеження обсягу доступних посереднику даних та відповідальність за їх неправомірне використання.

Окремою проблемою, що виникає внаслідок цифровізації, є автоматизоване прийняття рішень на основі алгоритмів та систем штучного інтелекту. О. Бугай, досліджуючи можливості та обмеження алгоритмічного прийняття рішень, зазначає, що серед переваг є підвищення ефективності та зниження витрат, отримання інформації з великих баз даних, покращення взаємодії між громадянами й урядами, водночас основними обмеженнями є неякісні дані, дискримінація, непрозорість рішень та високі вимоги до кібербезпеки [16, с. 144]. Алгоритмічне рішення у публічному управлінні за своєю природою передбачає обробку значних масивів персональних даних, а результат безпосередньо впливає на права та законні інтереси громадян. Окремі елементи автоматизованого прийняття рішень вже функціонують в екосистемі «Дія», зокрема автоматичне визначення права на соціальні виплати, автоматична верифікація ідентифікаційних даних, автоматичне формування електронних документів на підставі даних з реєстрів. У кожному з цих випадків алгоритм обробляє персональні дані громадянина та ухвалює рішення, що впливає на його права, без безпосередньої участі посадової особи.

С. Пороскун обґрунтовує, що цифрова форма процедури забезпечує високий рівень прозорості шляхом фіксації кожного етапу прийняття рішення у формі незмінних цифрових слідів, проте одночасно акцентує увагу на проблемі «чорної скриньки» через непрозорість алгоритмів, що ускладнює розуміння логіки адміністративних актів та обмежує можливості їх оскарження [95, с. 82]. Дослідник формулює важливу тезу про те, що правова визначеність у цифрову добу має включати стандарт «зрозумілості», відповідно до якого будь-який алгоритм, що впливає на права особи, повинен бути зрозумілим та верифікованим.

М. Дубняк, аналізуючи проблеми правового забезпечення цифровізації, встановлює, що Стратегія цифрового розвитку WinWin закладає прогресивні

цілі щодо розвитку штучного інтелекту, проте її операційні завдання орієнтовані на формування іміджу цифрової держави, а не на системне вирішення правових викликів, пов’язаних із безпекою персональних даних [33].

Окремого аналізу потребує інституційний вимір захисту персональних даних у цифровому публічному управлінні, а саме питання про те, хто і яким чином здійснює нагляд за обробкою даних у системі, що об’єднує десятки державних реєстрів та обслуговує мільйони громадян. Відповідно до чинного Закону № 2297-VI, парламентський контроль за додержанням прав у сфері захисту персональних даних здійснює Уповноважений Верховної Ради України з прав людини [118]. Водночас Уповноважений виконує ці функції паралельно з численними іншими повноваженнями, що об’єктивно обмежує його спроможність здійснювати ефективний нагляд за обробкою даних у складній системі цифрового публічного управління. Ефективна реалізація цифрової трансформації потребує ухвалення комплексного закону «Про цифрове врядування» та розбудови спеціалізованої системи нагляду. Відсутність спеціалізованого наглядового органу є критичною прогалиною, оскільки масштаб і складність обробки персональних даних у цифровому публічному управлінні потребують постійного, професійного та технічно обізнаного нагляду, який за чинної інституційної моделі забезпечити неможливо.

М. Білецький констатує прямий зв’язок між цифровою трансформацією та якістю врядування, наголошуючи, що забезпечення безпеки цифрової інфраструктури є важливим завданням державних інститутів [13, с. 64]. Повномасштабна збройна агресія російської федерації стала каталізатором цифровізації та водночас відобразила її правові вразливості. Екосистема «Дія» не лише продовжила функціонування, а й значно розширила перелік послуг у воєнний час.

Проте, Л. Малюга та К. Шкрібляк підтверджують, що правове регулювання захисту персональних даних в Україні залишається

концептуально застарілим, оскільки не враховує реалій цифрової трансформації [78, с. 114]. Р. Кірін, досліджуючи правові засади євроінтеграційного розвитку законодавства про е-урядування у воєнний та повоєнний час, систематизує нормативно-правові акти цього періоду і констатує необхідність кодифікації цифрового законодавства у формі Цифрового кодексу України [51, с. 258]. В. Клочан та І. Петрів зазначають, що воєнний стан поставив органи місцевого самоврядування перед безпрецедентними викликами, і цифрова трансформація стала засобом виживання місцевих інституцій, що суттєво прискорило впровадження цифрових інструментів, нерідко без належного правового забезпечення захисту персональних даних [52, с. 160].

Аналіз етапів цифровізації публічного управління засвідчує системну невідповідність між темпами технологічного розвитку та рівнем правового забезпечення захисту персональних даних. Закон України «Про особливості надання публічних (електронних публічних) послуг» від 15 липня 2021 року № 1689-IX визначив правові засади надання публічних послуг в електронній формі [123]. Закон України «Про публічні електронні реєстри» від 18 листопада 2021 року № 1907-IX встановив вимоги до створення, ведення та взаємодії реєстрів [125]. Закон «Про електронні комунікації» від 16 грудня 2020 року № 1089-IX регулює обробку даних у сфері електронних комунікацій, проте його дія не поширюється на обробку даних при наданні електронних публічних послуг [109]. Ці акти формують нормативну рамку цифрового публічного управління, проте жоден не містить комплексного регулювання захисту персональних даних, обмежуючись відсилкою (бланкетною нормою) до Закону № 2297-VI. Так, і досі відсутнє визначення правового статусу «Дії» як контролера або процесора даних, не передбачено вимог до оцінки впливу на захист даних при впровадженні нових цифрових сервісів, не створено правового механізму прозорості алгоритмічних рішень.

Закон України № 3633-IX від 11 квітня 2024 року передбачив розширення обсягу збору і обробки персональних даних у контексті

мобілізаційних процедур [104]. Зазначений Закон зобов'язав військовозобов'язаних оновлювати персональні дані через територіальні центри комплектування або електронний кабінет «Резерв+», що призвело до масштабного накопичення чутливих відомостей (місце проживання, стан здоров'я, сімейний стан, місце роботи) в єдиній інформаційній системі, водночас питання захисту цих даних від несанкціонованого доступу та їх цільового використання залишилося врегульованим лише на рівні загальних норм Закону № 2297-VI. Проте формування адміністративно-правового забезпечення захисту персональних даних повинно враховувати не лише типовий режим функціонування, а й кризові сценарії, передбачаючи чіткі критерії та процедури тимчасового обмеження прав із гарантіями їх відновлення.

Специфіка публічного управління зумовлює необхідність окремого правового регулювання захисту персональних даних у цифровому просторі. Масштаб обробки в єдиній системі «Дія», є значним і передбачає збір даних з десятків реєстрів від паспортних до медичних, майнових, податкових. Така агрегація не була передбачена розробниками окремих реєстрів. К. Рябець, досліджуючи вебпортал «Дія. Цифрова освіта», зазначає, що ця платформа акумулює дані про рівень цифрових компетентностей населення [142], які у сукупності з іншими відомостями з екосистеми «Дія» можуть використовуватися для профілювання профілів громадян.

Міжнародний досвід цифровізації публічного управління засвідчує, що проблема захисту персональних даних є невід'ємною складовою архітектурних рішень, а не факультативним доповненням. Естонська модель, що стала прототипом для української системи «Трембіта», заслуговує на особливу увагу саме у контексті захисту даних. Платформа X-Road, запроваджена у 2001 році, забезпечує міжреєстрову взаємодію понад 900 організацій та оперує більш ніж 3000 сервісів обміну даними. Принципова відмінність естонської моделі від української полягає у тому, що з 2015 року в Естонії функціонує інтегрований механізм забезпечення прозорості доступу

до персональних даних. Кожен громадянин має право у режимі реального часу переглядати журнал доступу до своїх відомостей (data tracker) та з'ясовувати, який саме орган, коли та з якою метою звертався до його даних. У разі виявлення необґрунтованого доступу суб'єкт даних може подати скаргу безпосередньо через державний портал. В Україні аналогічний механізм, як було зазначено, запроваджений лише у 2025 році Постановою № 1244 і досі перебуває на етапі технічної імплементації, причому право громадянина на перегляд журналу доступу прямо не закріплено [105].

Іншим аспектом, що відрізняє естонську модель, є принцип декларованої мети. В Естонії кожен міжреєстровий запит супроводжується обов'язковою декларацією мети, а система автоматично перевіряє, чи відповідає запитуваний обсяг даних заявленій меті. У Регламенті (ЄС) № 910/2014 (eIDAS) у поєднанні з GDPR закріплено комплексний підхід до цифрової ідентифікації та захисту даних: електронна ідентифікація розглядається не ізольовано, а у нерозривному зв'язку з правами суб'єктів даних, включаючи право на інформацію про обробку (ст. 13-14 GDPR), право на доступ (ст. 15), право на виправлення (ст. 16) та право на обмеження обробки (ст. 18) [180]. М. Білецький, аналізуючи досвід Сінгапуру, Республіки Корея, Данії та Естонії, констатує, що країни-лідери цифрового врядування досягли високих показників завдяки комплексному та стратегічному підходу до цифровізації, орієнтації на потреби громадян, інвестиціям в інфраструктуру та людський капітал, а також забезпеченню безпеки та прозорості [13, с. 63]. В Україні ж, як засвідчив проведений аналіз, цифрова інфраструктура значно випередила правове забезпечення захисту персональних даних, що створює структурний дисбаланс, характерний для моделей наздоганяючої цифровізації.

Проведений аналіз засвідчує, що ефективність цифрового публічного управління перебуває у прямій залежності від рівня цифрової довіри громадян, яка формується на основі впевненості у надійності захисту їхніх персональних даних. М. Білецький, аналізуючи проблеми публічного управління, зазначає,

що процес цифровізації призводить до зростання обсягів даних, які потребують надійного захисту, а на державу покладається відповідальність за розробку законодавчих механізмів щодо збору, зберігання та обробки даних для захисту права громадян на приватність [13, с. 64]. Для України ця проблема набуває додаткового виміру, оскільки в умовах триваючої збройної агресії довіра до державних цифрових систем є не лише питанням зручності, а й елементом соціальної стійкості та національної безпеки. Громадяни, які не довіряють механізмам захисту своїх даних у «Дії», можуть утримуватися від отримання електронних послуг, що підриває саму ідею цифрового урядування. В. Медяник, досліджуючи адміністративно-правовий вектор цифровізації соціальної сфери, обґрунтовує, що перехід до цифрової моделі публічного управління створює нові правові ризики у сфері захисту персональних даних, відповідальності за технічні помилки та кібербезпеки, а відсутність чіткої законодавчої архітектури цифрових процедур породжує правову невизначеність як для громадян, так і для виконавців послуг [80]. По суті, цифровізація формує нову модель взаємовідносин між державою та громадянином, що має ознаки соціального контракту. Громадянин надає персональні дані для отримання публічних послуг, а держава бере на себе зобов’язання щодо їх належного захист. Порушення цього контракту з боку держави, наприклад через недостатній рівень захисту, відсутність прозорості або безвідповідальне поводження з даними, підриває легітимність цифрового публічного управління як такого. Тому формування адекватного адміністративно-правового забезпечення захисту персональних даних є не лише правовою, а й політичною необхідністю, що визначає перспективи подальшої цифровізації публічного управління в Україні.

Таким чином, цифровізація публічного управління є не лише технологічним процесом, а також чинником якісної трансформації правовідносин у сфері захисту персональних даних. Перехід від паперового до цифрового адміністрування змінив суб’єктний склад правовідносин (з’явилися оператори цифрових платформ та інтероперабельних реєстрів),

обсяг обробки даних (від локальних архівів до централізованих баз з мільйонами записів), характер ризиків (від фізичної втрати документів до кібератак, масових витоків та алгоритмічної дискримінації) та саму природу управлінського рішення (від індивідуального рішення посадової особи до автоматизованого рішення алгоритму). Ці зміни вимагають формування окремого адміністративно-правового режиму захисту персональних даних у сфері цифрового публічного управління, який враховував би нерівне становище суб'єкта даних, масштаб і складність обробки, інтероперабельність реєстрів, автоматизацію прийняття рішень та необхідність забезпечення прозорості і підзвітності цифрових систем.

1.3. Сучасний стан адміністративно-правового забезпечення захисту персональних даних

Міжнародно-правові стандарти захисту персональних даних не є сукупністю ізольованих актів. Вони утворюють багаторівневу архітектуру, елементи якої перебувають у ієрархічному зв'язку, доповнюють та обумовлюють один одного. Розуміння цієї архітектури є необхідною передумовою для оцінки того, яким саме чином міжнародні стандарти впливають на національне адміністративне законодавство України, і які з них справляють юридично зобов'язальний, а які лише рекомендуючий вплив.

Першим рівнем є універсальні стандарти Ради Європи. Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 року (ETS № 108) та її оновлена редакція (Конвенція 108+ 2018 року) є єдиним юридично зобов'язальним міжнародним договором у сфері захисту персональних даних, що має відкритий характер і допускає ратифікацію державами поза межами ЄС. Україна ратифікувала Конвенцію 108 у 2010 році, що породило конкретні міжнародно-правові зобов'язання у сфері захисту персональних даних. Ключовою відмінністю Конвенції 108+ від

її попередньої редакції є запровадження принципу підзвітності контролера, вимоги щодо DPIA у випадках підвищеного ризику, а також посилення незалежності наглядових органів [166]. Для України ратифікація оновленої Конвенції 108+ є окремим завданням, що безпосередньо впливає на зміст національного адміністративного законодавства, оскільки відповідно до ст. 9 Конституції України чинні міжнародні договори, згода на обов'язковість яких надана Верховною Радою, є частиною національного законодавства [63]. Ю.О. Коваленко у дослідженні євроінтеграційних зобов'язань України у сфері захисту персональних даних підкреслює, що ратифікація оновленої Конвенції 108+ є не лише формальним кроком, а й сигналом про реальну готовність держави дотримуватись міжнародних стандартів захисту персональних даних на рівні, що відповідає сучасним технологічним реаліям [54].

Другим рівнем є стандарти ЄС як євроінтеграційне зобов'язання. GDPR і Директива 2016/680 не є юридично зобов'язальними для України як для держави, що не є членом ЄС, однак набувають обов'язкового характеру через євроінтеграційні зобов'язання через ст. 15 Угоди про асоціацію [154] та переговорну рамку кандидата на членство в ЄС [167]. Цей механізм впливу є принципово відмінним від прямої дії міжнародного договору, оскільки стандарти ЄС впливають на національне законодавство через зобов'язання адаптації acquis, тобто через законодавчий процес, а не через безпосереднє застосування. Наслідком є те, що будь-яка невідповідність українського законодавства стандартам GDPR є одночасно порушенням євроінтеграційних зобов'язань і підставою для оцінки прогресу в рамках переговорного процесу. О. Шпакович із співавторами у порівняльному дослідженні захисту персональних даних в Україні і Чеській Республіці констатують, що держави-кандидати на членство в ЄС перебувають у специфічній правовій ситуації, коли вони зобов'язані відтворити зміст acquis у національному законодавстві ще до вступу, хоча до моменту вступу відповідні акти ЄС не матимуть прямої дії на їхній території [183]. Окремі аспекти імплементації стандартів конвенції 108+ та GDPR в адміністративне законодавство України описано нами у [64].

Третім рівнем є нові регуляторні інструменти ЄС у сфері захистуданих. Починаючи з 2022 року архітектура регулювання даних в ЄС суттєво розширилась за межі GDPR. Регламент (ЄС) 2022/868 (Data Governance Act) набув чинності у вересні 2023 року і регулює повторне використання даних публічного сектору, механізми посередництва у сфері даних та добровільне надання даних в суспільних інтересах, так зване data altruism [181]. Для сфери захисту персональних даних у публічному управлінні Data Governance Act є важливим з огляду на те, що він встановлює умови, за яких органи публічної влади можуть надавати доступ до наявних у них даних, включаючи дані з державних реєстрів, для повторного використання третіми особами, і при цьому вимагає забезпечення відповідності такого повторного використання вимогам GDPR щодо захисту персональних даних. Ю. Руоганен та С. Міккелссон у коментарі до Data Governance Act зазначають, що цей акт будується на двох ключових ідеях (повторному використанні даних публічного сектору і добровільному наданні даних) і що його взаємодія з GDPR є однією з центральних регуляторних проблем, яка потребує вирішення на рівні національного законодавства кожної держави [182].

Ця архітектура впливає на національне адміністративне законодавство України через чотири взаємопов’язані механізми:

– нормативний, через ратифікацію міжнародних договорів, що безпосередньо включаються до системи національного законодавства;

– адаптаційний, через зобов’язання привести національне законодавство у відповідність до acquis ЄС у рамках євроінтеграційного процесу;

– юрисдикційний, через практику ЄСПЛ, яка тлумачить ст. 8 Конвенції про захист прав людини у справах про порушення права на приватність і є обов’язковою для України як держави-члена Ради Європи;

– орієнтувальний, через добровільне запозичення стандартів, що не є юридично зобов’язальними для України, але слугують орієнтиром для вдосконалення законодавства.

Розмежування цих чотирьох механізмів є принципово важливим для адміністративного права, оскільки кожен із них має різну юридичну силу і різний порядок імплементації у систему національних норм.

Стаття 8 Конвенції про захист прав людини і основоположних свобод гарантує право на повагу до приватного і сімейного життя, до житла та кореспонденції і є основним конвенційним інструментом захисту персональних даних у відносинах між особою і публічними органами [173]. ЄСПЛ послідовно тлумачить ст. 8 як таку, що охоплює право на захист персональних даних: будь-яке зберігання, використання або розкриття інформації про особу органами публічної влади підпадає під сферу дії цієї статті і потребує обґрунтування з точки зору законності, необхідності і пропорційності втручання. О. Гіляка та А. Мерник у дослідженні практики ЄСПЛ і Суду ЄС у сфері цифрових технологій констатують, що саме практика ЄСПЛ сформувала базові принципи захисту персональних даних ще до прийняття GDPR і Конвенції 108, і що ці принципи залишаються обов'язковим мінімумом, нижче якого не може опускатися жодна держава-член Ради Європи [20].

Далі розглянемо знакові справи, що визначили принципи обробки персональних даних.

Справа «Леандер проти Швеції» (Leander v. Sweden, 1987) заклала фундаментальний принцип: зберігання державою відомостей про особу у таємних реєстрах без її відома є втручанням у право на приватність, гарантоване ст. 8 Конвенції, яке потребує чіткої законної підстави і реальних гарантій проти зловживань. Хоча у цій справі ЄСПЛ визнав втручання виправданим з міркувань національної безпеки, він уперше чітко встановив, що сам факт зберігання та використання державним органом інформації про приватне життя особи, поєднаний з відмовою надати їй можливість оскаржити таку інформацію, підпадає під сферу дії ст. 8 Конвенції [171]. Для українського адміністративного права цей принцип має пряме значення у контексті функціонування державних реєстрів, де мільйони громадян не мають реальної

можливості дізнатись про зміст відомостей, що зберігаються про них, і тим більше заперечити їхню достовірність або правомірність зберігання.

Справа «S. і Марпер проти Сполученого Королівства» (S. and Marper v. United Kingdom, 2008) є одним з найважливіших рішень ЄСПЛ у сфері захисту персональних даних, що стосується дій публічних органів. ЄСПЛ встановив, що безстрокове зберігання біологічних зразків і ДНК-профілів осіб, щодо яких кримінальне провадження завершилось виправданням або закриттям, порушує ст. 8 Конвенції. Суд підкреслив, що зростаюче використання автоматизованої обробки персональних даних вимагає посилених гарантій, а загальна і невибіркова природа зберігання даних сама по собі є порушенням принципу пропорційності [170]. Для України це рішення є орієнтиром у контексті правового режиму реєстру «Оберіг» і загалом зберігання даних у правоохоронній сфері, де Закон № 2297-VI не встановлює конкретних строків зберігання і не передбачає автоматичного видалення даних після відпадіння підстав для їхньої обробки.

Справа «M.K. проти Франції» (M.K. v. France, 2013) стосувалась збирання відбитків пальців особи під час кримінального провадження і подальшого їх безстрокового зберігання у поліцейській базі даних незалежно від результату провадження. ЄСПЛ констатував порушення ст. 8 і підкреслив, що система зберігання, яка не розрізняє осіб залежно від тяжкості правопорушення і не встановлює строків зберігання, не відповідає принципу пропорційності [172]. Цей принцип безпосередньо кореспондує з принципом цільового обмеження, закріпленим у ст. 5 GDPR, але у чинному Законі № 2297-VI він відсутній у чіткому вигляді стосовно органів публічної влади.

Справа «Аман проти Швейцарії» (Amann v. Switzerland, 2000) розширила розуміння поняття «приватне життя» у контексті ст. 8, встановивши, що навіть зберігання інформації, яка не є чутливою за своїм характером, але може бути використана на шкоду особі, є втручанням у приватність, що потребує виправдання [169]. ЄСПЛ зазначив, що поняття «приватне життя» охоплює також професійну діяльність і соціальне життя

людини, що суттєво розширює коло відомостей, стосовно яких публічні органи зобов'язані дотримуватись вимог ст. 8. Для українського адміністративного права це означає, що захист персональних даних у публічному управлінні не обмежується чутливими категоріями даних – він поширюється на будь-які відомості, що циркулюють в адміністративних процедурах і можуть вплинути на права особи.

Україна є стороною Конвенції про захист прав людини і основоположних свобод з 1997 року, а рішення ЄСПЛ є обов'язковими для виконання відповідно до ст. 46 Конвенції [61]. Це означає, що принципи, сформовані у практиці ЄСПЛ щодо захисту персональних даних, мають пряму юридичну силу в Україні і є обов'язковим орієнтиром для адміністративного законодавства і правозастосовної практики. Водночас порівняння стандартів ЄСПЛ з чинним Законом № 2297-VI виявляє системну розбіжність у тому, що вимога законної підстави для зберігання персональних даних, принцип пропорційності такого зберігання, вимога строковості і принцип визначеності мети є стандартами ЄСПЛ, які в українському законодавстві або відсутні, або закріплені у надто загальній формі без конкретних механізмів реалізації. Ця розбіжність є не лише теоретичною прогалиною, а й джерелом потенційної відповідальності держави за порушення Конвенції, і саме усунення цієї розбіжності є одним із завдань реформування адміністративного законодавства у сфері захисту персональних даних.

Встановлення того, що міжнародні стандарти впливають на національне законодавство, зумовлює дослідження такого впливу. Принципово важливим є характеристика того, яким саме чином відбувається цей вплив, через які правові механізми, з якою юридичною силою і які практичні наслідки це має для системи адміністративного законодавства України.

Першим є нормативний механізм, який передбачає пряму дію міжнародних договорів. Відповідно до ч. 1 ст. 9 Конституції України чинні міжнародні договори, згода на обов'язковість яких надана Верховною Радою, є частиною національного законодавства України [63]. Це означає, що

Конвенція Ради Європи № 108, ратифікована у 2010 році, безпосередньо входить до системи національного законодавства і має переважну силу перед підзаконними актами у разі колізії. Водночас практичне значення цього механізму обмежене тим, що Конвенція містить загальні принципи, а не конкретні правила поведінки, а її норми потребують законодавчої деталізації для практичного застосування органами публічного управління. Суттєвою прогалиною є те, що Україна досі не ратифікувала оновлену Конвенцію 108+, яка набула чинності у жовтні 2023 року після досягнення необхідної кількості ратифікацій. Ратифікація 108+ є не лише формальним кроком, а й умовою повноцінного членства в системі Ради Європи у сфері захисту даних і одним із сигналів готовності до отримання рішення про адекватність від Єврокомісії. С. Мазепа у дослідженні імплементації європейських стандартів інформаційної безпеки в Україні фіксує, що однією з ключових проблем є невідповідність термінологічного апарату українського законодавства європейським стандартам та недостатня розвиненість інституційних механізмів реалізації міжнародних зобов'язань [77].

Адаптаційний механізм визначає зобов'язання відповідності acquis ЄС. Цей механізм є якісно відмінним від нормативного, оскільки він не передбачає прямої дії актів ЄС, а зобов'язує Україну привести своє законодавство у відповідність до їхнього змісту. Юридична природа цього зобов'язання ґрунтується одночасно на ст. 15 Угоди про асоціацію [154], переговорній рамці кандидата на членство [167] і прийнятих у рамках переговорного процесу індивідуальних зобов'язаннях. Практичний наслідок адаптаційного механізму полягає в тому, що будь-яка невідповідність українського законодавства стандартам GDPR або Директиви 2016/680 є одночасно порушенням міжнародно-правових зобов'язань і підставою для оцінки прогресу в рамках переговорного процесу. Це принципово відрізняє адаптаційний механізм від нормативного, оскільки невиконання нормативного зобов'язання тягне юридичну відповідальність перед міжнародними інстанціями, тоді як невиконання адаптаційного зобов'язання визначає переговорні наслідки у

вигляді призупинення або уповільнення процесу вступу. О. Яворська підкреслює, що GDPR вже зараз справляє реальний вплив на українські суб'єкти обробки персональних даних, оскільки його дія поширюється на всіх контролерів, які обробляють дані громадян ЄС, незалежно від місцезнаходження контролера [163]. Це означає, що адаптаційний механізм для України є не лише перспективним завданням євроінтеграції, а й поточним регуляторним реаліям для значної частини суб'єктів господарювання.

Юрисдикційний механізм передбачає урахування практики ЄСПЛ як обов'язкового правового орієнтиру. Рішення ЄСПЛ є обов'язковими для виконання Україною відповідно до ст. 46 Конвенції про захист прав людини і основоположних свобод [61]. Однак вплив практики ЄСПЛ на адміністративне законодавство виходить за межі виконання конкретних рішень, і він має системний характер. Принципи, сформульовані ЄСПЛ у практиці, розглянутій нами раніше (законність зберігання державою персональних даних, пропорційність і строковість зберігання, конкретність і незмінність мети збирання, широке тлумачення поняття «приватне життя») є обов'язковими правовими стандартами для всього законодавства і правозастосування в Україні. Це означає, що органи публічного управління зобов'язані керуватись цими стандартами незалежно від того, чи відтворені вони у національному законодавстві. Проте відсутність їх законодавчого закріплення створює правову невизначеність у правозастосуванні і ускладнює захист прав суб'єктів персональних даних у практиці адміністративних судів.

Орієнтувальний механізм полягає у добровільному запозиченні стандартів. Поряд із юридично зобов'язальними механізмами і орієнтувальний, який характеризує вплив, який здійснюється через добровільне запозичення найкращих практик і стандартів, що не є юридично обов'язковими для України. Йдеться насамперед про Рекомендації Комітету Міністрів Ради Європи у сфері захисту персональних даних, що охоплюють обробку даних у поліцейській сфері, у медицині, в трудових відносинах, а також стандарти Робочої групи ст. 29 та Керівні настанови EDPB щодо

окремих аспектів застосування GDPR. Хоча ці документи не є юридично зобов'язальними, їх дотримання є індикатором реальної, а не лише формальної відповідності стандартам ЄС і враховується при оцінці рівня захисту персональних даних Єврокомісією в рамках процедури adequacy. Н. Расторгуєва у дослідженні систем органів, відповідальних за імплементацію acquis в Україні, наголошує, що ефективна адаптація потребує не лише законодавчих змін, а й системного інституційного забезпечення, здатного відстежувати зміни в практиці застосування стандартів ЄС і своєчасно відображати їх у національному регулюванні [131].

Чотири описані механізми діють не ізольовано, а у взаємодії, що формує комплексне правове середовище. Нормативний механізм задає мінімальний юридично зобов'язальний стандарт; адаптаційний визначає цільовий орієнтир, до якого має прагнути законодавство; юрисдикційний формує практичний правовий стандарт, яким мають керуватись органи влади вже сьогодні; орієнтувальний окреслює динамічний орієнтир, що відображає поточний стан розвитку стандартів. Для адміністративного законодавства України ця взаємодія означає, що реформування у сфері захисту персональних даних не може обмежуватись прийняттям одного закону, а має охоплювати одночасне виконання зобов'язань за Конвенцією 108+, адаптацію до acquis ЄС, урахування практики ЄСПЛ і добровільне запровадження найкращих практик ЄС у сферах, де юридично зобов'язальні норми ще відсутні.

Відповідність національного адміністративного законодавства міжнародним стандартам у сфері захисту персональних даних не є питанням, що вичерпується констатацією наявності або відсутності окремих норм. Системна оцінка цієї відповідності потребує виявлення прогалин у їхній взаємозв'язаності та системній природі, оскільки саме ця системність визначає характер і масштаб завдань, що стоять перед адміністративно-правовим регулюванням у сфері захисту персональних даних.

Вагомою прогалиною є невідповідність термінологічного апарату. С. Мазепа констатує, що невідповідність термінологічного апарату українського

законодавства до європейських стандартів є однією з ключових перешкод ефективної імплементації [77]. Чинний Закон № 2297-VI оперує поняттями «володілець» і «розпорядник», тоді як міжнародні стандарти GDPR і Конвенція 108+ використовують «контролер» і «процесор». Ця відмінність є не суто термінологічною, оскільки поняття «контролер» і «процесор» у праві ЄС мають чітко окреслений зміст, що визначає розподіл відповідальності, обсяг обов'язків і механізми звітності. Перенесення цих понять з іноземного права без відповідного змістовного наповнення може призвести до ситуації, коли нові терміни вживатимуться, але їхній зміст залишатиметься невизначеним у правозастосовній практиці. О. Яворська підкреслює, що GDPR пропонує ширше та деталізованіше визначення персональних даних, до яких включаються як традиційні ідентифікатори, так і більш чутливі категорії, тоді як українське законодавство залишає окремі аспекти, зокрема щодо біометричних, медичних та генетичних даних, менш регламентованими, що створює правові прогалини, особливо у випадках міжнародної обробки даних [163].

Ще однією прогалиною є відсутність принципу підзвітності. Конвенція 108+ і GDPR закріплюють принцип підзвітності (accountability) як самостійний принцип, відповідно до якого контролер не лише зобов'язаний дотримуватись вимог законодавства, а й повинен бути здатним продемонструвати це дотримання. Цей принцип є якісно відмінним від простого обов'язку дотримання, оскільки він передбачає ведення документації, проведення внутрішніх аудитів, призначення відповідальних осіб і звітування перед наглядовим органом. У чинному Законі № 2297-VI принцип підзвітності у такому розумінні відсутній. Закон встановлює вимоги до обробки, але не зобов'язує суб'єктів обробки документувати відповідність цим вимогам. Це означає, що навіть за умови фактичного дотримання закону суб'єкт обробки позбавлений правових інструментів для підтвердження такого дотримання перед наглядовим органом, що суттєво ускладнює як здійснення нагляду, так і захист власних інтересів у разі спору. О. Шпакович,

О. Шевчук та П. Мелотікова наголошують, що саме відсутність принципу підзвітності є однією з принципових відмінностей між українським законодавством і стандартами ЄС, і що без його закріплення будь-які інші реформи залишатимуться неповними [183].

Інституційна прогалиною є відсутність спеціалізованого наглядового органу. Конвенція 108+ у ст. 15 і GDPR у ст. 51 однозначно вимагають існування незалежного спеціалізованого наглядового органу у сфері захисту персональних даних. Виконання цієї вимоги є не факультативним елементом адаптації, а обов'язковою умовою як ратифікації Конвенції 108+ в її оновленій редакції, так і отримання рішення про адекватність від Єврокомісії. Чинна модель, за якої функції наглядового органу покладено на Уповноваженого Верховної Ради України з прав людини, не відповідає жодному з чотирьох вимірів незалежності, визначених ст. 52 GDPR: ні функціональному, ні фінансовому, ні кадровому, ні операційному. Це є не просто організаційним недоліком, а системною прогалиною, що унеможливлює реальну імплементацію міжнародних стандартів незалежно від того, наскільки досконалим буде зміст нового закону.

Ще однією є прогалина у сфері транскордонної передачі даних. Міжнародні стандарти, зокрема ст. 14 Конвенції 108+ і глава V GDPR, встановлюють детальний режим транскордонної передачі персональних даних, що включає механізми adequacy, стандартні договірні застереження і обов'язкові корпоративні правила. Чинний Закон № 2297-VI містить лише загальну норму про те, що передача даних за кордон допускається за умови відповідного рівня захисту у країні-отримувачі, без деталізації механізмів підтвердження такого рівня і без визначення правових інструментів, що можуть замінити механізм adequacy. Це є практично значущою прогалиною з огляду на масштаби транскордонної передачі даних в умовах воєнного стану, та зберігання реєстрів у хмарних сховищах, передача даних органам влади іноземних держав, взаємодія з міжнародними гуманітарними організаціями.

Інструменти усунення визначених прогалин будуть наведені у наступний розділах.

Таким чином, невідповідність українського адміністративного законодавства міжнародним стандартам у сфері захисту персональних даних не є сукупністю ізольованих недоліків, а системною характеристикою, що відображає об’єктивний розрив між рівнем розвитку міжнародних стандартів і станом національного законодавства. Подолання цього розриву є завданням не одного законодавчого акта, а комплексного реформування, що охоплює матеріальне право, інституційну архітектуру і механізми правозастосування.

Висновки до розділу 1

Персональні дані у контексті публічного управління є специфічним об’єктом адміністративно-правової охорони, що відрізняється від об’єктів конституційно-правового і цивільно-правового регулювання. Саме адміністративне право здатне забезпечити три необхідних виміри охорони (нормативний, інституційний та юрисдикційний), що обумовлює його центральну роль у регулюванні відносин між суб’єктами публічного адміністрування і громадянином у сфері обробки персональних даних. Право на захист персональних даних є самостійним публічним суб’єктивним правом із власним змістом, суб’єктним складом і механізмом реалізації, що охоплює три взаємопов’язані правомочності, а саме: вимагати законності обробки, реалізовувати суб’єктивні права щодо власних даних і отримувати захист у разі порушення.

Цифровізація публічного управління якісно трансформувала правовідносини у сфері захисту персональних даних, розвинувши їх суб’єктний склад, об’єкт, зміст прав і обов’язків та характер правового зв’язку між державою і громадянином. Агрегація персональних даних з множини реєстрів формує стійку інформаційну асиметрію на користь держави, а

автоматизоване прийняття управлінських рішень породжує новий тип правовідносин, відмінний від традиційного адміністративного права.

Міжнародно-правові стандарти захисту персональних даних впливають на національне адміністративне законодавство через чотири механізми (нормативний, адаптаційний, юрисдикційний та орієнтувальний), кожен з яких має відмінну юридичну природу і різний порядок імплементації. Практика ЄСПЛ формує обов'язкові правові стандарти, що вже сьогодні є обов'язковими для органів публічного управління незалежно від їхнього закріплення у національному законодавстві. Системний аналіз прогалин імплементації виявляє невідповідність у чотирьох взаємопов'язаних вимірах (термінологічному, принциповому, інституційному та процедурному), що визначає комплексний характер завдань реформування адміністративного законодавства у сфері захисту персональних даних.

РОЗДІЛ 2
ЗМІСТ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ ЦИФРОВІЗАЦІЇ ПУБЛІЧНОГО УПРАВЛІННЯ

2.1. Нормативно-правове регулювання захисту персональних даних у сфері цифрового публічного управління

Адміністративно-правовий механізм як юридична категорія розглядається у науковій літературі через взаємопов'язану систему нормативно-правових, інституційних та процедурних елементів [1]. Власне через них держава в особі уповноважених суб'єктів забезпечує захист персональних даних, у тому числі у сфері цифровізації публічного управління. Нормативна складова охоплює систему правових норм, які регулюють відносини у сфері захисту персональних даних; інституційна – права та обов'язки суб'єктів, наділених відповідними повноваженнями; процедурна – порядок здійснення діяльності із захисту персональних даних. Саме така архітектоніка і визначає підхід до побудови структури даного розділу. Нормативна складова є базовою, оскільки від якості правового регулювання залежить повнота повноважень суб'єктів захисту, а також ефективність застосовуваних визначених процедур [3]. Саме тому дослідження чинного правового регулювання у цій сфері є початковою точкою аналізу всього механізму забезпечення захисту персональних даних в умовах цифровізації публічного управління. Без з'ясування того, що і як врегульовано на нормативному рівні, неможливо ні оцінити інституційну спроможність суб'єктів захисту даних, ні виявити системні прогалини, що потребують усунення.

Нормативно-правове регулювання захисту персональних даних у сфері публічного управління не є однорідним, а складається з кількох взаємопов'язаних рівнів: конституційного, законодавчого та підзаконного.

Кожен із цих рівнів виконує власну функцію: конституційні норми закріплюють основоположні гарантії права на приватність; закони визначають загальні та спеціальні правила обробки персональних даних суб'єктами публічного управління; підзаконні акти конкретизують ці правила стосовно окремих систем, реєстрів і процедур. Методологічно дослідження нормативної бази саме через цей трирівневий підхід дозволяє отримати цілісну картину правового регулювання та виявити прогалини на кожному з рівнів.

Сучасний стан нормативно-правового регулювання в сфері захисту персональних даних характеризується суттєвою асиметрією між темпами цифровізації публічного управління та розвитком відповідного законодавства. З одного боку, за останнє десятиліття в Україні сформувалася розгалужена система цифрової публічної інфраструктури – від порталу «Дія» до численних державних реєстрів, що об'єднують масиви персональних даних мільйонів громадян. З іншого боку, базовий Закон України «Про захист персональних даних», прийнятий ще у 2010 році [118], не зазнав суттєвого оновлення й значною мірою не відповідає вимогам сучасного цифрового середовища та стандартам, закладеним у Регламенті (ЄС) 2016/679 (GDPR) [180]. Наслідком цього є фрагментарне, а подекуди й суперечливе правове регулювання, яке не забезпечує належного рівня захисту персональних даних у публічній цифровій сфері.

Зазначені обставини зумовлюють необхідність системного аналізу чинної нормативної бази з метою встановлення її реального змісту, виявлення внутрішніх суперечностей та прогалин. Даний аналіз нами буде здійснюватись послідовно від конституційних засад, а саме через базове і спеціальне законодавство, і до підзаконного регулювання, з окремою увагою до специфіки правового регулювання в умовах воєнного стану.

Конституційні засади правового регулювання захисту персональних даних у сфері публічного управління визначаються межами допустимого

втручання держави у приватне життя особи. Конституція України містить кілька ключових положень, що формують відповідні засади.

Центральне місце посідає стаття 32 Конституції України, відповідно до якої «не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини» [63]. У контексті публічного управління ця норма набуває особливого значення, оскільки саме органи державної влади та місцевого самоврядування є основними суб'єктами, що акумулюють і обробляють персональні дані громадян у процесі реалізації своїх функцій [40]. Відповідно, стаття 32 Конституції встановлює не лише право особи, а й конституційне обмеження повноважень публічної адміністрації щодо поводження з персональними даними.

Поряд із статтею 32 важливу роль відіграє стаття 31 Конституції, яка гарантує таємницю листування, телефонних розмов та іншої кореспонденції. В умовах цифровізації ця норма поширюється на електронні комунікації громадян з органами публічної влади, зокрема в системах електронного урядування та при наданні електронних публічних послуг [58].

Важливим є положення статті 22 Конституції України про те, що конституційні права і свободи не можуть бути звужені при прийнятті нових законів. Ця норма формує конституційну вимогу до законодавця: будь-яке розширення повноважень публічних органів щодо збору та обробки персональних даних в умовах цифровізації має здійснюватися з дотриманням принципу пропорційності та не може призводити до звуження гарантованого конституційного права на приватність [34, с. 94].

Водночас у науковій літературі справедливо зазначається, що конституційні норми у цій сфері сформульовані на достатньо загальному рівні й не враховують специфіки цифрового середовища, зокрема масштабів автоматизованої обробки персональних даних у публічних реєстрах, ризиків профілювання особи через міжвідомчий обмін даними та загроз, пов'язаних з

алгоритмічним прийняттям рішень [6]. Це зумовлює необхідність розвитку конституційних гарантій на рівні галузевого законодавства, насамперед адміністративного.

Основу законодавчого регулювання захисту персональних даних в Україні становить Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI [118]. Він є центральним у системі нормативно-правового регулювання досліджуваної сфери, оскільки визначає поняття персональних даних, підстави та умови їх обробки, права суб'єктів даних, а також обов'язки осіб, що здійснюють обробку. Закон поширюється на діяльність як приватних, так і публічних суб'єктів, що робить його ключовим інструментом регулювання відносин у сфері публічного управління.

Закон було прийнято у 2010 році передусім з метою виконання зобов'язань України за Конвенцією Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108) 1981 року [166], до якої Україна приєдналася у 2010 році. Відповідно, структура і термінологія Закону значною мірою відображають підходи, закладені саме в цьому міжнародному документі, а не у GDPR, який на момент прийняття Закону ще не існував. Це принципова обставина, яка пояснює значну частину сучасних проблем із застосуванням Закону в умовах цифрової трансформації суспільних відносин.

Стаття 6 Закону закріплює загальні вимоги до обробки персональних даних, з яких доктринально виводяться такі принципи: законність обробки, визначеність та обмеження мети, адекватність і ненадмірність даних, відкритість і прозорість обробки. Закон також містить окремі норми щодо точності даних (ст. 19–20) та обмеження строків їх зберігання (ст. 13) [118]. Водночас аналіз цих принципів у порівнянні з аналогічними положеннями GDPR [180] виявляє суттєві відмінності як у рівні деталізації, так і у механізмах забезпечення їх дотримання. Зокрема, GDPR прямо закріплює принцип підзвітності, який покладає на контролера даних обов'язок не лише дотримуватися принципів обробки, а й бути спроможним продемонструвати

їх дотримання. Закон України аналогічного положення не містить, що суттєво послаблює відповідальність публічних органів як операторів персональних даних [88].

Окремої уваги заслуговує питання сфери застосування Закону щодо суб'єктів публічного управління. Закон визначає поняття «володільця» та «розпорядника» персональних даних, однак не містить спеціальних норм, які б враховували особливості обробки даних саме органами державної влади та місцевого самоврядування. Між тим обробка персональних даних у публічній сфері має принципові відмінності від приватної: вона здійснюється на підставі владних повноважень, часто є обов'язковою для суб'єкта даних, а відмова від надання даних може унеможливити реалізацію особою своїх прав. GDPR враховує цю специфіку, передбачаючи окрему правову підставу обробки для виконання завдань в публічних інтересах (ст. 6(1)(e)), а також низку спеціальних гарантій для такої обробки. Закон України подібної диференціації не проводить.

Найбільш очевидними прогалинами Закону в контексті цифровізації публічного управління є такі. По-перше, Закон не містить жодних положень щодо автоматизованого прийняття рішень та профілювання, тоді як GDPR присвячує цьому питанню окрему статтю 22, що є критично важливим в умовах розширення практики алгоритмічного прийняття адміністративних рішень. По-друге, Закон не передбачає обов'язку проведення оцінки впливу на захист даних (Data Protection Impact Assessment, DPIA) перед запуском нових систем обробки даних, що є обов'язковим за GDPR для операцій з підвищеним ризиком. По-третє, відсутні вимоги до реалізації принципу «захист даних за замовчуванням та за проектом» (privacy by design and by default), що означає відсутність нормативного зобов'язання для розробників публічних цифрових систем враховувати вимоги захисту даних вже на етапі їх проектування [19]. По-четверте, санкції за порушення Закону є явно непропорційно низькими порівняно з міжнародними стандартами. Більш детально це буде розглянуто у підрозділі 3.1.

Таким чином, Закон України «Про захист персональних даних» виконував свою функцію на етапі початкового формування правової бази у цій сфері, однак сьогодні є очевидно недостатнім для регулювання відносин, що виникають в умовах масштабної цифровізації публічного управління. Його збереження як базового акта без суттєвого оновлення є однією з ключових системних проблем, що визначають незадовільний стан захисту персональних даних у вітчизняній публічній цифровій інфраструктурі.

Поряд із загальним Законом «Про захист персональних даних» у сфері цифрового публічного управління діє розгалужена система спеціального законодавства, яке регламентує обробку персональних даних у конкретних цифрових системах і реєстрах. Це законодавство формувалося переважно у 2012-2021 роках і відображає різні етапи цифровізації публічного управління в Україні. Його аналіз є принципово важливим, оскільки саме у спеціальних актах сконцентровані найбільш суттєві прогалини у сфері захисту персональних даних. При цьому слід підкреслити, що між загальним і спеціальним законодавством існує суттєвий методологічний розрив: якщо базовий Закон № 2297-VI будувався передусім навколо захисту персональних даних як такого, то спеціальне законодавство у сфері цифрового публічного управління розроблялося переважно з позицій забезпечення функціональних потреб цифрової трансформації, і питання захисту даних у ньому нерідко залишалося на другому плані.

Закон України «Про публічні електронні реєстри» від 18.11.2021 № 1907-IX [125] є одним із ключових актів спеціального законодавства, що визначає правові засади функціонування публічних електронних реєстрів як основних інструментів цифрового публічного управління. Реєстри є центральним елементом цифрової публічної інфраструктури, оскільки в Україні функціонує значна кількість державних реєстрів і баз даних, які у сукупності акумулюють персональні дані практично всього дорослого населення країни [38]. Закон встановлює загальні вимоги до створення, ведення, захисту та взаємодії реєстрів, визначає права суб’єктів даних щодо

доступу до реєстрових відомостей, а також закріплює принцип одноразового подання даних, відповідно до якого громадянин не зобов'язаний надавати одні й ті самі дані різним органам публічної влади [125].

Закон № 1907-IX також вперше на законодавчому рівні закріпив вимоги до захисту інформації в реєстрах, зокрема щодо розмежування доступу, резервного копіювання, аудиту дій з даними та захисту від несанкціонованого доступу. У цьому сенсі він є кроком уперед порівняно з попереднім станом нормативного регулювання. Водночас аналіз Закону № 1907-IX крізь призму вимог захисту персональних даних виявляє низку суттєвих проблем. Зокрема, він не встановлює єдиних критеріїв розмежування реєстрових даних за режимом доступу на рівні загального закону, делегуючи вирішення цього питання галузевим законам, відповідно до яких створено кожен окремий реєстр. Наслідком є фрагментований підхід: режим доступу до персональних даних у різних реєстрах визначається різними нормативними актами без уніфікованих стандартів захисту. Поза межами регулювання Закону № 1907-IX залишається і колізія між вимогами Закону «Про доступ до публічної інформації» щодо надання публічної інформації у формі відкритих даних та вимогами Закону «Про захист персональних даних», яка на практиці породжує правову невизначеність для адміністраторів реєстрів.

У науковій літературі підкреслюється суперечність між принципом відкритості реєстрових даних як умови прозорості публічного управління та принципом захисту персональних даних як гарантії права на приватність і зазначається, що Закон № 1907-IX не пропонує збалансованого механізму вирішення цієї суперечності, обмежуючись загальними відсилками (бланкетними нормами) до законодавства про захист персональних даних [79].

Окрім зазначеного Закон не містить спеціальних норм, які б зобов'язували адміністраторів реєстрів проводити оцінку впливу на захист даних (DPIA) перед запуском нових реєстрів або суттєвою зміною порядку обробки реєстрових даних. За стандартами GDPR проведення DPIA є обов'язковим для операцій з обробки даних, що з високою ймовірністю

можуть спричинити значний ризик для прав і свобод фізичних осіб [180], а функціонування великих публічних реєстрів беззаперечно підпадає під цей критерій. Відсутність такої вимоги в українському законодавстві означає, що нові реєстрові системи можуть запускатися без будь-якої попередньої оцінки їхнього впливу на права суб'єктів персональних даних.

Ще одним недостатньо врегульованим питанням є відповідальність адміністраторів реєстрів як операторів персональних даних. Закон визначає адміністратора реєстру як суб'єкта, відповідального за його ведення, однак не встановлює спеціальних санкцій за порушення вимог захисту персональних даних при адмініструванні реєстрів. Це ускладнює реалізацію суб'єктами даних своїх прав у разі порушень і фактично виводить адміністраторів реєстрів з-під дієвого механізму відповідальності.

Закон України «Про особливості надання публічних (електронних публічних) послуг» від 15.07.2021 № 1689-IX [122] регулює відносини у сфері надання електронних публічних послуг, зокрема через платформу «Дія». Вагомість цього Закону найкраще демонструють показники використання платформи «Дія», користувачами якої є близько 24 мільйони українців, і через платформу якої надавалося близько 100 видів публічних послуг і документів. Отже, «Дія» є найбільшим за охопленням оператором персональних даних громадян у системі публічного управління України.

З точки зору захисту персональних даних Закон № 1689-IX породжує принципову проблему невизначеності правового статусу платформи «Дія» як оператора персональних даних. Закон не дає відповіді на запитання, хто є «володільцем» персональних даних у розумінні Закону «Про захист персональних даних» при наданні електронної послуги через «Дію» – орган-надавач послуги чи Міністерство цифрової трансформації як адміністратор платформи. Ця невизначеність унеможливлює чіткий розподіл відповідальності за порушення у сфері захисту персональних даних. За стандартами GDPR у подібних ситуаціях застосовується концепція спільного контролера даних, яка передбачає солідарну відповідальність усіх суб'єктів,

що спільно визначають цілі та засоби обробки [180]. Українське законодавство аналогічної правової конструкції не передбачає.

Крім того, Закон № 1689-IX не містить спеціальних норм щодо принципу мінімізації даних при наданні електронних послуг. На практиці це призводить до того, що для отримання окремих послуг через «Дію» від громадянина запитується значно більший обсяг персональних даних, ніж це є об'єктивно необхідним для надання конкретної послуги. Такий підхід суперечить не лише стандартам GDPR, а й задекларованому самим Законом № 1689-IX принципу зручності для користувача, оскільки надмірний збір даних підвищує ризики для особи в разі витоку інформації. Проблема загострюється в умовах воєнного стану, коли витік персональних даних громадян може становити пряму загрозу їхній безпеці.

Окремо слід вказати на проблему міжвідомчого обміну даними в межах платформи «Дія». Закон № 1689-IX передбачає широку інтеграцію реєстрів для цілей надання послуг, однак не встановлює достатніх гарантій того, що дані, отримані при наданні однієї послуги, не використовуватимуться для інших цілей. Такий підхід суперечить фундаментальному принципу цільового обмеження обробки персональних даних, закріпленому як у базовому Законі № 2297-VI [118], так і у стандартах GDPR [180], і може призводити до неконтрольованого розширення цілей використання персональних даних громадян. Більш детально про це описано нами у публікації [67].

Закон України «Про адміністративні послуги» від 06.09.2012 № 5203-VI [99], хоча й передував сучасному етапу цифровізації, залишається важливим елементом нормативної бази, оскільки визначає загальні засади надання адміністративних послуг, у тому числі в електронній формі. Його положення щодо порядку подання та використання документів і відомостей при наданні послуг безпосередньо стосуються захисту персональних даних. Однак показово, що за більш ніж десять років дії цього Закону його жодного разу не було доповнено спеціальними нормами про захист персональних даних при наданні адміністративних послуг в умовах цифровізації. Закон обмежується

загальними вимогами до обробки інформації про заявника та відсилає до загального законодавства про захист персональних даних, що є недостатнім з огляду на масштаби цифровізації адміністративних послуг.

Окрему групу спеціального законодавства становлять акти, що регулюють функціонування галузевих реєстрів: електронної медичної системи (ЕСОЗ), Єдиного державного демографічного реєстру, Єдиного реєстру осіб, які вчинили корупційні або пов'язані з корупцією правопорушення, Державного реєстру виборців та інших. Спільною рисою більшості цих актів є те, що вони зосереджені на функціональній стороні реєстрів і лише побіжно торкаються питань захисту персональних даних, відсилаючи до базового Закону № 2297-VI.

Особливої уваги заслуговує правове регулювання захисту персональних даних в електронній медичній системі. Медичні дані є особливою категорією чутливих персональних даних, обробка яких потребує підвищеного рівня захисту, що зафіксовано на рівні Конвенції 108+ [166] та статті 9 GDPR [180]. Стаття 24-2 Основ законодавства України про охорону здоров'я покладає на Національну службу здоров'я України обов'язок захищати центральну базу даних ЕСОЗ від несанкціонованого доступу та забезпечувати захист персональних даних пацієнтів відповідно до вимог законодавства. Міністерство охорони здоров'я України також розробило методичні матеріали щодо захисту персональних даних пацієнтів при роботі з інформаційно-комунікаційними системами електронної охорони здоров'я [41]. Водночас спеціальне законодавство у сфері охорони здоров'я містить лише загальні норми про захист персональних даних в ЕСОЗ переважно технічного характеру без конкретних правових вимог щодо мінімізації даних, цільового обмеження та прав суб'єктів даних стосовно медичної інформації, що не відповідає стандарту ст. 9 GDPR для особливих категорій даних.

Аналогічна ситуація склалася у сфері Єдиного державного демографічного реєстру, який акумулює ключові ідентифікаційні дані про кожного громадянина України. Закон України «Про Єдиний державний

демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» [111], не передбачає спеціальних процедур сповіщення суб'єктів даних про порушення захисту персональних даних, що є стандартною вимогою сучасного законодавства про захист даних і прямим обов'язком контролера за GDPR [180].

Системний аналіз спеціального законодавства у цій сфері дає підстави для висновку, що воно формувалося переважно з позицій забезпечення функціональних потреб цифрового публічного управління, а не з позицій захисту персональних даних. Питання захисту даних у спеціальних актах нерідко вирішуються за залишковим принципом через відсилку до базового Закону, який, як було показано вище, сам потребує суттєвого оновлення. Результатом є фрагментарне регулювання, яке не забезпечує системного захисту персональних даних у цифровому публічному просторі та не відповідає сучасним міжнародним стандартам у цій сфері.

Важливим інструментом у захисті персональних даних у сфері цифрового публічного управління, що базується на законодавстві, є підзаконні нормативно-правові акти, які конкретизують законодавчі вимоги стосовно окремих систем, процедур і технічних аспектів обробки персональних даних. Саме на підзаконному рівні визначаються окремі специфічні аспекти, що дають змогу дослідити цілісність та послідовність (або непослідовність) вітчизняного регулювання у цій сфері.

Центральне місце серед підзаконних актів у сфері цифрового публічного управління посідає Постанова Кабінету Міністрів України від 08.09.2016 № 606 «Деякі питання електронної взаємодії електронних інформаційних ресурсів» [28], яка регулює порядок електронної взаємодії між державними інформаційними ресурсами, зокрема між публічними реєстрами при наданні адміністративних послуг. З точки зору захисту персональних даних Постанова № 606 є ключовим підзаконним актом, оскільки саме міжвідомчий обмін даними між реєстрами є одним із найбільш ризикових аспектів обробки персональних даних у публічній цифровій інфраструктурі.

Разом із тим аналіз Постанови № 606 виявляє суттєву прогалину: вона регулює технічні та організаційні аспекти електронної взаємодії інформаційних ресурсів, однак не містить спеціальних вимог до захисту персональних даних у процесі такої взаємодії. Зокрема, Постанова не встановлює обов'язкових вимог щодо мінімізації обсягу даних, що передаються між реєстрами, не визначає порядку ведення журналів аудиту доступу до персональних даних при міжвідомчому обміні, а також не передбачає механізму повідомлення суб'єктів персональних даних про факти такого обміну.

Слід, однак, зазначити, що Постанова № 606 не є цілковито позбавленою норм про захист персональних даних. Вона покладає на суб'єктів електронної взаємодії загальний обов'язок здійснювати обробку і забезпечувати захист персональних даних у власних інформаційно-комунікаційних системах відповідно до законодавства про захист персональних даних, а також містить спеціальну норму щодо обробки персональних даних у підсистемі моніторингу доступу системи «Трембіта» [28]. Утім ці положення мають переважно відсильний характер і не встановлюють самостійних змістовних вимог до захисту персональних даних при міжвідомчому обміні, що підтверджує загальний висновок про недостатність підзаконного регулювання у цій сфері.

Серед підзаконних актів, що регулюють технічний захист інформації в державних системах, варто зазначити «Мінімальні вимоги до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем», затверджені Постановою КМУ від 29.03.2006 № 373 [115]. Цей акт визначає організаційні та технічні вимоги до захисту державних інформаційних ресурсів і конфіденційної інформації, у тому числі персональних даних, в інформаційних системах органів державної влади та місцевого самоврядування.

Разом з тим, характерною рисою нормативних актів Мінцифри у цій сфері є їх переважна орієнтація на питання інформаційної безпеки та

кіберзахисту, а не на захист персональних даних як такий. Між цими поняттями існує принципова відмінність: інформаційна безпека спрямована на захист систем і даних від несанкціонованого доступу ззовні, тоді як захист персональних даних охоплює значно ширше коло питань, включаючи законність самої обробки, дотримання принципів мінімізації та цільового обмеження, реалізацію прав суб'єктів даних тощо. Акти Мінцифри здебільшого регулюють першу складову, залишаючи другу недостатньо врегульованою на підзаконному рівні.

Серед підзаконних актів, що безпосередньо стосуються захисту персональних даних, слід виділити Типовий порядок обробки персональних даних, затверджений Наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14 «Про затвердження документів у сфері захисту персональних даних» [114]. Цей документ конкретизує вимоги до організації обробки персональних даних володільцями баз персональних даних, зокрема органами публічної влади. Він містить вимоги до документування операцій з обробки даних, організації внутрішнього контролю, а також до технічних і організаційних заходів захисту даних.

Разом із тим Типовий порядок, прийнятий на виконання базового Закону 2010 року, успадкував його обмеження і не враховує сучасних реалій цифрового публічного управління. Зокрема, він не містить спеціальних вимог до обробки персональних даних в автоматизованих системах прийняття рішень, не передбачає процедур реагування на інциденти безпеки персональних даних, а також не встановлює вимог до призначення відповідальних осіб із захисту даних на зразок інституту Data Protection Officer, передбаченого статтею 37 GDPR [180].

Системний аналіз підзаконної нормативної бази у досліджуваній сфері засвідчує її суттєву недостатність. Підзаконні акти здебільшого дублюють або деталізують положення законів, не заповнюючи наявних у них прогалин, а між актами різних органів виконавчої влади існують колізії та неузгодженості, що ускладнює їх практичне застосування. Ця ситуація є закономірним наслідком

відсутності єдиного координуючого органу у сфері захисту персональних даних, що зумовлює формування підзаконного регулювання розрізнено, без єдиної методологічної основи. Саме інституційний вимір цієї проблеми є предметом аналізу у наступному підрозділі дисертації.

Важливим аспектом нормативно-правового регулювання захисту персональних даних у сфері публічного управління є питання функціонування цього регулювання в умовах воєнного стану. З 24 лютого 2022 року Україна перебуває в умовах правового режиму, що передбачає можливість тимчасового обмеження окремих прав і свобод громадян. Це безпосередньо стосується і права на захист персональних даних, закріпленого у статті 32 Конституції України [63], оскільки в умовах воєнного стану через створення ряду новий реєстрів масштаб обробки персональних даних публічними органами та ризики для прав суб'єктів даних суттєво зростають.

Конституційно-правовою основою для обмеження права на захист персональних даних в умовах воєнного стану є стаття 64 Конституції України, яка допускає тимчасове обмеження конституційних прав в умовах воєнного або надзвичайного стану із зазначенням строків таких обмежень. Закон України «Про правовий режим воєнного стану» від 12.05.2015 № 389-VIII [124] визначає конкретні заходи, що можуть вживатися в умовах воєнного стану, серед яких розширення повноважень правоохоронних органів щодо збору та обробки інформації про осіб. При цьому Конституційний Суд України у своїй практиці неодноразово наголошував, що будь-яке обмеження права на приватність, включаючи обробку персональних даних, має відповідати принципам законності, пропорційності та необхідності [135].

На сьогодні в Україні немає інструменту регламентування особливості обробки персональних даних саме в умовах воєнного стану. Ні базовий Закон № 2297-VI [118], ні спеціальні закони у сфері цифрового публічного управління не містить чітких положень щодо обсягу, мети, строків зберігання та порядку доступу до персональних даних в умовах надзвичайних станів. Ця прогалина створює правову невизначеність, яка на практиці породжує ризики

зловживань з боку суб’єктів публічної влади та унеможливлює ефективний захист прав громадян [148].

Практичним виявом цієї прогалини є щонайменше три проблеми. По-перше, в умовах воєнного стану суттєво розширилися повноваження правоохоронних органів щодо доступу до персональних даних громадян, однак відсутність прозорих процедур та ефективного судового контролю за такими діями створює ризики порушення права на приватність, гарантованого статтею 32 Конституції України [63]. По-друге, платформа «Дія» в умовах воєнного стану набула нових функцій, пов’язаних із безпекою та ідентифікацією, при цьому відсутність чітких правових механізмів, що регулюють обсяг, мету та строки зберігання відповідних даних, суперечить принципу мінімізації даних [148]. По-третє, державні реєстри, що акумулюють персональні дані громадян, стали об’єктами систематичних кібератак з боку агресора, тоді як законодавство не передбачає спеціальних процедур реагування на інциденти безпеки персональних даних в умовах воєнного стану [70].

Конституційний Суд України сформував важливі правові позиції, що безпосередньо стосуються допустимих меж обробки персональних даних публічними органами. У рішенні № 2-рп/2012 Суд зазначив, що обробка персональних даних має здійснюватися виключно на підставі закону, а будь-яке втручання у приватне життя особи має бути обґрунтованим, пропорційним і відповідати легітимній меті [135]. У рішенні № 7-р/2018, що стосувалося повноважень Міністерства фінансів щодо доступу до персональних даних у реєстрових системах, Суд визнав неконституційним надання публічному органу необмежених повноважень щодо обробки персональних даних без чіткого визначення обсягу даних, категорій суб’єктів, строків і порядку їх зберігання [136]. Ці позиції набувають особливого значення в умовах воєнного стану, коли держава схильна розширювати свої повноваження у сфері збору та обробки інформації.

У порівняльній перспективі показовим є досвід країн Європейського Союзу, де навіть в умовах надзвичайних ситуацій «зберігається чіткий баланс між забезпеченням безпеки та дотриманням прав людини: встановлюються суворі обмеження щодо обсягу та строків зберігання даних, а також передбачаються механізми незалежного контролю за діями державних органів» [148]. Цей підхід є важливим орієнтиром для вдосконалення українського законодавства, яке наразі не забезпечує належного рівня правових гарантій захисту персональних даних в умовах надзвичайних обставин.

Проведений аналіз нормативно-правової бази дозволяє систематизувати виявлені прогалини. На конституційному рівні це відсутність норм, що враховують специфіку цифрового середовища та масштаби автоматизованої обробки персональних даних. На законодавчому рівні це застарілість базового Закону № 2297-VI, відсутність регулювання алгоритмічних рішень, обов'язкової DPIA та вимог privacy by design, невизначеність правового статусу платформи «Дія» як оператора персональних даних, фрагментарність галузевого законодавства. На підзаконному рівні це переважна орієнтація актів на технічний захист інформації на шкоду змістовним гарантіям прав суб'єктів даних, відсутність спеціального регулювання для умов воєнного стану. Спільним знаменником усіх виявлених прогалин є відсутність в Україні спеціалізованого незалежного наглядового органу у сфері захисту персональних даних, що детально буде розглянуто у підрозділі 2.2, та невідповідність чинного законодавства стандартам GDPR, що є предметом аналізу розділу 3 дисертаційної роботи.

2.2. Система суб'єктів забезпечення захисту персональних даних у сфері публічного управління в умовах цифровізації

Дослідження інституційної складової адміністративно-правового механізму захисту персональних даних передбачає насамперед з'ясування поняття і складу суб'єктів, що беруть участь у його реалізації. Як зазначає Н. Головацький, адміністративно-правова природа сучасних відносин у сфері захисту персональних даних у публічному управлінні знаходиться у протиріччі з традиційним поняттям суб'єкта владних повноважень, що зумовлює необхідність переосмислення підходів до визначення кола відповідних суб'єктів [21]. Це методологічне завдання вимагає послідовного аналізу суміжних категорій – від загального до спеціального.

У науковій літературі з адміністративного права поняття «суб'єкт» розглядається через призму наявності правосуб'єктності у відповідній сфері. В. Колпаков та О. Кузьменко визначають суб'єктів адміністративного права як осіб, наділених правами та обов'язками у сфері публічного управління, і пропонують їх класифікацію за п'ятьма групами: Президент України, органи виконавчої влади, державні службовці, громадяни, органи місцевого самоврядування [60]. В. Галунько підкреслює, що конститутивною ознакою суб'єктів публічної адміністрації є реалізація ними функцій виконавчої влади та захист публічного інтересу [3]. Ця загальна категорія надто широка для цілей нашого дослідження і потребує звуження через більш конкретні поняття.

Важливим методологічним орієнтиром є також поділ між «суб'єктом адміністративного права» і «суб'єктом адміністративно-правових відносин», який обґрунтовують В. Колпаков та О. Кузьменко: перший є носієм потенційної здатності вступати у відповідні правовідносини, тоді як другий є фактичним їх учасником [60]. В межах даного дослідження принциповим є саме друге поняття, яке стосується суб'єктів, що реально здійснюють повноваження у сфері захисту персональних даних.

В. Брижко у своїх дослідженнях організаційно-правових питань захисту персональних даних розрізняє суб'єктів, що здійснюють обробку даних, та суб'єктів, що забезпечують контроль за дотриманням відповідного законодавства Автор зазначає, що змішування цих двох категорій є одним із ключових недоліків вітчизняного законодавства [15].

Т. Обуховська у своєму дослідженні державних механізмів захисту персональних даних констатує, що захист персональних даних виходить далеко за межі суто технічного захисту інформаційних систем і охоплює законність самої обробки, забезпечення прав суб'єктів даних та дотримання принципів мінімізації й цільового обмеження, що є предметом правового, а не лише технічного регулювання [87]. Тобто, суб'єкти кібербезпеки і суб'єкти забезпечення захисту персональних даних це суміжні, але нетотожні категорії.

Стаття 4 Закону України «Про захист персональних даних» визначає п'ять груп суб'єктів відносин, пов'язаних із персональними даними: суб'єкт персональних даних, володілець, розпорядник, третя особа, у тому числі суб'єкт надання міжнародної технічної допомоги та Уповноважений Верховної Ради України з прав людини [118]. Посібник М. Бем, І. Городиського та ін., підготовлений у межах спільної програми Ради Європи та ЄС, наводить докладну характеристику кожної з цих груп і підкреслює, що ефективність захисту персональних даних залежить від діяльності уповноважених органів, тобто суб'єктів, що наділені владними повноваженнями у відповідній сфері [11]. Ця законодавча класифікація, однак, не є придатною для цілей нашого дослідження з кількох причин.

По-перше, вона включає суб'єкта персональних даних фізичну особу, яка є пасивним носієм прав, а не активним суб'єктом забезпечення захисту. По-друге, вона змішує суб'єктів обробки (володілець, розпорядник) із суб'єктом контролю (Уповноважений), хоча між ними існує принципова функціональна відмінність. По-третє, ця класифікація взагалі не охоплює низки органів публічної влади, що реально беруть участь у забезпеченні захисту персональних даних у сфері цифрового публічного управління:

Мінцифри, галузевих органів як держателів реєстрів, органів місцевого самоврядування. Така неповнота є самостійною науковою проблемою і підтверджує необхідність доктринального визначення досліджуваної категорії.

На підставі аналізу суміжних категорій та з урахуванням специфіки цифрового публічного управління визначимо змістовні ознаки суб'єктів забезпечення захисту персональних даних у цій сфері. Першою ознакою є наявність владних повноважень (нормотворчих, контрольних або правозастосовних) саме у сфері захисту персональних даних. Другою ознакою є спрямованість діяльності на забезпечення захисту, а не лише на обробку персональних даних. Третьою ознакою є публічно-правовий характер статусу, закріплений законом або підзаконним актом. Четверта ознака це здійснення діяльності у сфері публічного управління або щодо суб'єктів публічного управління.

Технічні адміністратори реєстрів, що виконують сервісні функції з обслуговування інформаційних систем, не входять до цієї категорії, оскільки їх правовий статус визначається договором, а не публічно-правовим актом, і вони позбавлені владних повноважень у сфері захисту персональних даних.

На підставі зазначених ознак запропонуємо авторське визначення. Суб'єктами забезпечення захисту персональних даних у сфері цифрового публічного управління є органи та посадові особи публічної влади, які наділені владними повноваженнями нормотворчого, контрольного або правозастосовного характеру і здійснюють їх з метою реалізації та охорони права особи на захист персональних даних у відносинах з публічною адміністрацією.

За функціональним критерієм їх можна класифікувати на три групи: наглядовий суб'єкт (Уповноважений ВРУ з прав людини), регуляторно-координуючі суб'єкти (Мінцифри) та галузеві суб'єкти (держателі реєстрів та інші органи публічної влади).

Центральним суб'єктом забезпечення захисту персональних даних у системі публічного управління України є Уповноважений Верховної Ради України з прав людини (далі – Уповноважений). З 1 січня 2014 року, після прийняття Закону України «Про внесення змін до деяких законів України щодо діяльності Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних» від 13.05.2014 № 1262-VII [102], функції наглядового органу у цій сфері було покладено виключно на Уповноваженого. До цього моменту ці функції розподілялися між кількома органами, що породжувало дублювання повноважень і неефективність. Передача повноважень Уповноваженому мала на меті, зокрема, наближення моделі нагляду до вимог Конвенції 108, Додатковий протокол до якої 2001 року вимагав від держав-сторін запровадити наглядовий орган у сфері захисту персональних даних [166].

Правовий статус Уповноваженого у сфері захисту персональних даних визначається насамперед статтею 23 Закону № 2297-VI [118], яка встановлює широкий перелік його повноважень. До них належать: отримання звернень і скарг з питань захисту персональних даних та прийняття рішень за їх результатами; проведення планових і позапланових, виїзних і безвиїзних перевірок володільців і розпорядників персональних даних; отримання доступу до будь-якої інформації, необхідної для здійснення контролю; видання обов'язкових для виконання вимог (приписів) про усунення порушень; надання рекомендацій щодо практичного застосування законодавства; складання протоколів про адміністративні правопорушення і направлення їх до суду; затвердження підзаконних нормативно-правових актів у сфері захисту персональних даних [118]. Крім того, Уповноважений щорічно звітує про стан дотримання законодавства у цій сфері у складі своєї доповіді до Верховної Ради України.

Для реалізації цих повноважень у Секретаріаті Уповноваженого функціонує спеціалізований Департамент у сфері захисту персональних даних, основними завданнями якого є здійснення парламентського контролю,

нормотворча діяльність у сфері захисту даних, моніторинг стану дотримання прав людини та забезпечення виконання міжнародних зобов'язань України [27].

Аналіз звітів Уповноваженого свідчить про те, що найбільш поширеними порушеннями у сфері захисту персональних даних, виявленими під час перевірок, є незаконне поширення персональних даних. Зокрема, оприлюднення їх на офіційних веб-сайтах органів державної влади та місцевого самоврядування, а також несанкціоноване втручання у приватне і сімейне життя з використанням інформаційно-телекомунікаційних технологій [160]. Водночас практика контрольної діяльності Уповноваженого у сфері цифрового публічного управління залишається обмеженою: більшість перевірок стосуються обробки персональних даних у трудових відносинах, а не у системах цифрового публічного управління. Також зазначимо, що кількість перевірок органів публічної влади щодо дотримання вимог захисту персональних даних у цифрових системах є недостатньою з огляду на масштаб і ризики обробки даних у таких системах.

Попри формально широкий перелік повноважень, інституційна модель Уповноваженого як наглядового органу у сфері захисту персональних даних має суттєві структурні обмеження, які знижують ефективність його діяльності в цій сфері.

Уповноважений є конституційним органом парламентського контролю за дотриманням прав і свобод людини із надзвичайно широким мандатом, що охоплює всі без винятку права людини. Функція нагляду у сфері захисту персональних даних є лише однією з багатьох і фактично конкурує за інституційні ресурси з іншими напрямами діяльності. У науковій літературі зазначається, що поєднання функцій загального омбудсмана і спеціалізованого наглядового органу з захисту даних об'єктивно обмежує спроможність ефективно реагувати на системні порушення у цифровій публічній сфері [56].

Ще одним аспектом є те, що принципова вимога Конвенції 108+, Протокол CETS № 223 до якої прийнятий Радою Європи у травні 2018 року, а також статей 51-59 GDPR [180] стосується повної незалежності наглядового органу, що передбачає відсутність зовнішнього впливу на його діяльність, самостійне формування бюджету та кадрового складу. Україна ратифікувала базову Конвенцію 108 ще у 2010 році, однак Протокол CETS № 223, яким запроваджуються ці підвищені вимоги до наглядових органів, досі не ратифікований. Рада Європи у межах спільного з ЄС проєкту підтримки Офісу омбудсмана публічно наголошувала на тому, що ратифікація Конвенції 108+ є необхідною передумовою реформи системи захисту персональних даних в Україні [27]. Чинний правовий статус Уповноваженого як парламентського омбудсмана не забезпечує в повній мірі вимог щодо спеціалізованої інституційної незалежності, притаманної моделі Data Protection Authority.

Також варто зазначити, що ресурсна та технічна спроможність Департаменту у сфері захисту персональних даних є явно недостатньою для системного нагляду за обробкою персональних даних у масштабній цифровій публічній інфраструктурі України. Як справедливо зазначається у науковій літературі, нагальною потребою України є не лише приведення законодавства у відповідність до стандартів GDPR та Конвенції 108+, а й створення наглядового органу з належним рівнем інституційної спроможності [56].

Таким чином, попри те, що Уповноважений формально виконує функції наглядового органу у сфері захисту персональних даних, його інституційна модель не відповідає сучасним міжнародним стандартам у цій сфері. Ця проблема детально буде розглянута у підрозділі 3.3 дисертаційного дослідження.

Особливе місце серед суб’єктів забезпечення захисту персональних даних у сфері цифрового публічного управління посідає Міністерство цифрової трансформації України (далі – Мінцифри). Воно утворено постановою Кабінету Міністрів України від 02.09.2019 і є головним органом у системі центральних органів виконавчої влади, що забезпечує формування та

реалізацію державної політики у сфері цифровізації, цифрових інновацій, електронного урядування, розвитку національних електронних інформаційних ресурсів та надання електронних публічних послуг [93]. Як справедливо зазначають О. Шелемеха та О. Волох, створення Мінцифри «стало одним із важливих кроків держави у цифровізації українського суспільства, що є неможливою без відповідної державної політики, а сучасні виклики у сфері цифровізації є багатовекторними і пов'язані не лише з рівнем надання електронних послуг, а й з питаннями цифрових прав громадян та інформаційної безпеки суспільства» [159].

Адміністративно-правовий статус Мінцифри визначається Положенням про Міністерство цифрової трансформації України, затвердженим постановою Кабінету Міністрів України від 18.09.2019 № 856 [93], та Законом України «Про центральні органи виконавчої влади» від 17.03.2011 № 3166-VI [127]. За своєю природою Мінцифри є головним органом у системі центральних органів виконавчої влади, що відповідає за формування державної політики у відповідній сфері. Д. Луніна, досліджуючи адміністративно-правовий статус Мінцифри, підкреслює, що специфіка цього органу полягає у міжгалузевому характері його компетенції, яка охоплює одночасно технологічну, правову та соціальну складові цифровізації публічного управління [76].

Положення № 856 визначає розгалужену систему завдань і повноважень Міністерства. Аналізуючи їх через призму захисту персональних даних, можна виокремити кілька ключових функціональних напрямів:

– нормотворчий. Мінцифри розробляє пропозиції щодо прийняття або внесення змін до нормативно-правових актів з питань захисту персональних даних, а також встановлює стандарти, норми і правила у сферах, що належать до його компетенції;

– організаційно-технологічний. Міністерство забезпечує функціонування системи електронної взаємодії державних електронних інформаційних ресурсів, єдиного державного вебпорталу електронних послуг,

єдиного державного вебпорталу відкритих даних та національного реєстру електронних інформаційних ресурсів;

– координуючий. Мінцифри погоджує та координує галузеві й регіональні програми та проєкти інформатизації, здійснює моніторинг у сфері інформатизації;

– просвітницький та методичний. Міністерство сприяє розвитку цифрових навичок і цифрових прав громадян, зокрема розробляє разом із Національним агентством з питань державної служби навчальні курси з питань захисту персональних даних для державних службовців [93].

О. Шелемеха та О. Волох класифікують повноваження Мінцифри за критерієм типу на загальнодержавні, адміністративні, регіональні, соціальні та господарські, наголошуючи, що ключовий акцент у діяльності органу спрямований на реалізацію загальнодержавних та адміністративних повноважень, які є найбільш чітко визначеними нормативно [159]. У контексті захисту персональних даних особливого значення набувають загальнодержавні повноваження, зокрема право розробляти пропозиції щодо визначення порядку функціонування державних інформаційних ресурсів та електронних реєстрів, а також брати участь у формуванні державної політики у сфері захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

Окрім регуляторних і нормотворчих функцій, Мінцифри є безпосереднім адміністратором ключових цифрових платформ публічного управління, насамперед «Дії» та системи електронної взаємодії інформаційних ресурсів. У сфері управління Мінцифри перебуває державне підприємство «Дія», яке є технічним адміністратором центрального засвідчувального органу. Це означає, що Міністерство одночасно формує регуляторне середовище для захисту персональних даних і безпосередньо відповідає за функціонування систем, що акумулюють персональні дані мільйонів громадян. Захист персональних даних при цьому є одним із завдань Міністерства, яке несе відповідальність за забезпечення безпеки персональних

даних у контексті цифрових публічних послуг та розробку відповідної політики й механізмів захисту від несанкціонованого доступу [159]. На виконання цих зобов'язань Мінцифри затвердило власний Порядок обробки та захисту персональних даних, володільцем яких є Міністерство, узгоджений з Уповноваженим Верховної Ради України з прав людини [116].

Принципова особливість Мінцифри як суб'єкта у досліджуваній системі полягає в тому, що його повноваження у сфері захисту персональних даних мають переважно регуляторно-методичний і технологічний характер на відміну від контрольних повноважень Уповноваженого. Мінцифри не є органом, що здійснює перевірки суб'єктів обробки персональних даних, видає обов'язкові приписи або складає протоколи про адміністративні правопорушення у цій сфері. Натомість воно є органом, що формує архітектуру цифрового публічного управління, від якості якої безпосередньо залежить рівень захисту персональних даних у відповідних системах. Процес цифровізації, підкреслює Л. Руденко, сприяє підвищенню ефективності, доступності та прозорості надання адміністративних послуг, проте одночасно актуалізує потребу в чіткому правовому регулюванні захисту персональних даних у цифровому середовищі [140]. Саме в цьому регуляторно-технологічному вимірі Мінцифри виступає ключовим суб'єктом системи, органічно доповнюючи контрольну функцію Уповноваженого Верховної Ради України з прав людини.

Система суб'єктів забезпечення захисту персональних даних у сфері цифрового публічного управління не вичерпується Уповноваженим та Мінцифри. Важливу роль у цій системі відіграють галузеві суб'єкти – органи державної влади, що є держателями або адміністраторами реєстрів, а також органи місцевого самоврядування. Їх роль у досліджуваній системі визначається тим, що саме вони є безпосередніми операторами переважної більшості публічних цифрових систем, у яких акумулюються персональні дані громадян, і несуть пряму відповідальність за забезпечення захисту цих даних у межах відповідних систем.

Відповідно до Закону України «Про публічні електронні реєстри» № 1907-IX держатель публічного електронного реєстру це «орган державної влади, орган місцевого самоврядування, юридична особа публічного права, визначена законом, або саморегулівна організація, що забезпечує створення, функціонування та ведення публічного електронного реєстру» [125]. Саме держатель несе відповідальність за встановлення порядку функціонування реєстру, визначення складу реєстрових даних і вимог до їх захисту в межах відповідної галузевої системи. У цьому сенсі галузеві органи-держателі реєстрів є суб'єктами забезпечення захисту персональних даних у запропонованому нами розумінні, оскільки вони наділені владними повноваженнями нормотворчого характеру щодо захисту персональних даних у відповідних цифрових системах.

Серед галузевих органів-держателів реєстрів, що обробляють значні масиви персональних даних у цифровій публічній сфері, особливо виділяються такі:

– Міністерство охорони здоров'я є держателем Електронної системи охорони здоров'я (ЕСОЗ), що акумулює медичні персональні дані, що формують найбільш чутливу категорію за класифікацією Закону № 2297-VI [118] так GDPR [180];

– Міністерство юстиції є держателем Єдиного державного демографічного реєстру та Єдиного державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань – реєстрів, що містять базові ідентифікаційні дані практично кожного громадянина;

– Міністерство соціальної політики є держателем систем, що забезпечують обробку персональних даних отримувачів соціальних виплат та послуг в рамках Єдиної інформаційної системи соціальної сфери, запровадженої Законом № 4607-IX від 18.09.2025 (набере чинності 27.05.2026) [112];

– Пенсійний фонд України адмініструє персональні дані застрахованих осіб у системі обов'язкового державного соціального страхування.

Кожен із зазначених органів у межах своїх галузевих повноважень затверджує власні порядки обробки та захисту персональних даних, що стосуються відповідних реєстрових систем, погоджуючи їх з Уповноваженим Верховної Ради України з прав людини. Так, Міністерство освіти і науки України затвердило окремий Порядок обробки та захисту персональних даних, що визначає порядок обробки персональних даних, володільцем яких є Міністерство освіти і науки України [117]. Аналогічні акти прийнято й іншими галузевими органами. Така галузева нормотворчість є виявом регуляторних повноважень відповідних суб'єктів у сфері захисту персональних даних.

Особливе місце серед галузевих суб'єктів системи займає Національне агентство з питань запобігання корупції (НАЗК), яке є держателем та адміністратором Єдиного державного реєстру декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування, а також Єдиного державного реєстру осіб, які вчинили корупційні або пов'язані з корупцією правопорушення. Ці реєстри мають подвійну правову специфіку з точки зору захисту персональних даних. З одного боку, вони містять значний обсяг персональних даних публічних службовців, а з іншого значна частина цих даних законодавчо виведена з режиму конфіденційності [113]. Зокрема, відповідно до статті 5 Закону № 2297-VI персональні дані, зазначені у декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування, не належать до інформації з обмеженим доступом, крім відомостей, визначених Законом України «Про запобігання корупції» [118]. В умовах воєнного стану НАЗК запровадило часткове вилучення декларацій окремих категорій декларантів із публічного доступу, що само по собі є прикладом обмеження звичайного режиму доступу до персональних даних з міркувань безпеки. Ці обставини роблять НАЗК одним із найбільш наочних прикладів суб'єкта, що здійснює балансування між принципом публічності даних і правом на захист персональних даних у системі цифрового публічного управління.

Органи місцевого самоврядування є самостійним і чисельно найбільшим видом суб'єктів системи забезпечення захисту персональних даних у сфері публічного управління. Вони обробляють значні масиви персональних даних громадян – у процесі реєстрації місця проживання, надання соціальних послуг, земельних відносин, управління комунальним майном. Відповідно до статті 4 Закону України «Про захист персональних даних» органи місцевого самоврядування є повноправними суб'єктами відносин, пов'язаних із персональними даними у ролі їх володільців і розпорядників [118]. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини за 2023 рік підтверджує, що органи місцевого самоврядування є одними з найбільш частих адресатів рекомендацій у сфері захисту персональних даних, а порушення з боку цих органів, зокрема, незаконне оприлюднення персональних даних на офіційних вебсайтах, є поширеною практикою [160].

В умовах цифровізації роль органів місцевого самоврядування як суб'єктів забезпечення захисту персональних даних суттєво зростає. Вони є активними учасниками системи електронних публічних послуг, отримують доступ до персональних даних громадян через систему «Дія» та інші цифрові платформи, а також у межах впровадження концепції «смарт-сіті» запроваджують власні цифрові системи, що обробляють персональні дані. А. С. Михайлик аналізуючи нормативно-правове регулювання захисту персональних даних в Україні, підкреслює, що органи місцевого самоврядування відповідно до частини 2 статті 19 Конституції України зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами, що повною мірою поширюється на їх діяльність у сфері обробки персональних даних [82].

Надалі необхідно чітко окреслити межу, що відділяє галузевих суб'єктів системи від технічних адміністраторів реєстрів. Відповідно до Закону України «Про публічні електронні реєстри» технічним адміністратором реєстру є «юридична особа публічного права, яка в межах та в обсягах, визначених договором, забезпечує супровід, функціонування та адміністрування

публічного електронного реєстру» [125]. На відміну від держателя реєстру, правовий статус технічного адміністратора визначається договором, а не законом. Технічний адміністратор не наділений владними повноваженнями у сфері захисту персональних даних. Він виконує сервісні функції забезпечення технічного функціонування системи і не може ні встановлювати вимоги до захисту даних, ні здійснювати контроль за їх дотриманням, ні застосовувати заходи відповідальності. Саме ця відсутність владних повноважень є конститутивною ознакою, що виключає технічних адміністраторів реєстрів з числа суб'єктів забезпечення захисту персональних даних. Відповідальність за захист персональних даних у реєстрових системах несе держатель реєстру, а не його технічний адміністратор. Між ними існують договірні відносини, у межах яких держатель визначає вимоги до захисту даних, а технічний адміністратор зобов'язаний їх виконувати. Таким чином, технічний адміністратор є об'єктом впливу суб'єкта-держателя в частині вимог щодо захисту персональних даних, а не самостійним суб'єктом у досліджуваній системі.

Аналіз системи суб'єктів забезпечення захисту персональних даних у сфері цифрового публічного управління виявляє її вагому інституційну ваду, а саме відсутність спеціалізованого незалежного наглядового органу. Проведений вище аналіз засвідчив, що наявна система суб'єктів є функціонально фрагментованою: Уповноважений здійснює загальний парламентський контроль, Мінцифри формує технологічну архітектуру цифрового публічного управління, галузеві органи забезпечують захист даних у відповідних реєстрових системах. Проте жоден із цих суб'єктів не є спеціалізованим незалежним органом у сфері захисту персональних даних у тому розумінні, яке закладене у міжнародних стандартах.

Вимога щодо незалежного наглядового органу є ключовим елементом Конвенції 108+ [166] та GDPR [180]. Статті 51-59 GDPR встановлюють розгорнуту модель органу нагляду: він має бути повністю незалежним при виконанні своїх завдань, мати достатні людські, технічні та фінансові ресурси

для ефективного виконання своїх функцій, самостійно визначати структуру і штатний розпис, а його члени мають призначатися у порядку, що виключає будь-який зовнішній вплив на їх діяльність [180]. Функції такого органу повинні включати нагляд за застосуванням законодавства про захист даних, розгляд скарг суб'єктів персональних даних, проведення розслідувань, видачу обов'язкових вказівок і накладення санкцій. В країнах ЄС цю модель реалізують спеціалізовані Data Protection Authorities, які є незалежними регуляторними органами, що діють виключно у сфері захисту персональних даних і не суміщають цю функцію з жодними іншими повноваженнями.

Україна усвідомлює цю інституційну прогалину і вже зробила кроки у напрямі її усунення на законодавчому рівні. У Верховній Раді зареєстровано два взаємопов'язані законопроєкти: № 8153 «Про захист персональних даних» [128] і № 6177 «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації» [129]. Перший законопроєкт пропонує нову редакцію базового закону, приведену у відповідність до стандартів GDPR, тоді як другий деталізує порядок створення та функціонування нового незалежного колегіального органу, а саме Національної комісії. Показово, що законопроєкт № 8153 у листопаді 2023 року прийнятий Верховною Радою у першому читанні та рекомендований профільним комітетом до прийняття за основу, хоча й з низкою зауважень щодо необхідності доопрацювання окремих положень відповідно до вимог GDPR [128]. Уповноважений Верховної Ради України з прав людини у своїх рекомендаціях також закликав розглянути та надати висновок щодо законопроєкту № 6177.

З 2011 по 2014 рік органом контролю у сфері захисту персональних даних в Україні була Державна служба з питань захисту персональних даних як самостійний орган виконавчої влади. Її було ліквідовано у 2014 році саме з метою приведення інституційної моделі у відповідність до вимог Конвенції 108, яка передбачає незалежний наглядовий орган, але не орган, підпорядкований Кабінету Міністрів [45]. Таким чином, питання про

інституційну форму незалежного органу в Україні має вже більш ніж десятирічну історію і досі залишається невирішеним.

Відсутність спеціалізованого незалежного регулятора має конкретні практичні наслідки для захисту персональних даних у сфері цифрового публічного управління. Уповноважений, маючи широкі повноваження, об'єктивно не може зосередити достатні ресурси на системному нагляді за обробкою персональних даних у масштабній цифровій публічній інфраструктурі. Мінцифри, поєднуючи регуляторні та операторські функції, не є й не може бути незалежним наглядовим органом за визначенням. Галузеві органи здійснюють захист персональних даних виключно у межах своїх секторальних повноважень, не маючи прав та можливостей для системного міжгалузевого нагляду. Наслідком є те, що обробка персональних даних у публічній цифровій сфері здійснюється фактично без спеціалізованого незалежного контролю, що є системною вадою, яка безпосередньо впливає на рівень захисту прав суб'єктів персональних даних [42]. Детальний аналіз напрямів вирішення цієї проблеми, зокрема конкретні пропозиції щодо моделі нового органу, буде здійснено у наступному розділі.

Аналіз правового статусу і функціональних повноважень суб'єктів системи забезпечення захисту персональних даних у сфері цифрового публічного управління, дозволяє перейти до характеристики їх взаємодії. Така взаємодія є необхідною умовою ефективного функціонування системи в цілому, оскільки жодний із суб'єктів не здатний самостійно охопити всі аспекти захисту персональних даних у масштабній цифровій публічній інфраструктурі. Водночас аналіз чинної нормативної бази засвідчує, що взаємодія суб'єктів системи характеризується рядом суттєвих вад, що безпосередньо позначаються на її ефективності.

Базова проблема взаємодії суб'єктів системи полягає у відсутності в чинному законодавстві будь-якого координаційного механізму між ними. Закон України «Про захист персональних даних» [118] та підзаконна нормативна база регулюють повноваження Уповноваженого, галузевих

органів і органів місцевого самоврядування автономно, не визначаючи порядку їх взаємодії при здійсненні контрольних і наглядових функцій, механізмів обміну інформацією щодо виявлених порушень, процедури узгодження позицій при виникненні колізій між вимогами різних нормативних актів у сфері захисту персональних даних. Уповноважений, здійснюючи контроль за дотриманням законодавства, не має формалізованого механізму взаємодії з галузевими органами-держателями реєстрів щодо виявлених системних порушень у відповідних цифрових системах. Результатом є ситуація, за якої кожен суб'єкт системи діє у межах власної компетенції, практично не координуючи свої дії з іншими суб'єктами.

Тісно пов'язаною з відсутністю координаційного механізму є проблема нормативної фрагментованості у сфері захисту персональних даних. Кожен галузевий орган-держатель реєстру затверджує власний порядок обробки та захисту персональних даних у відповідній системі, причому ці акти часто відрізняються за рівнем деталізації та вимогами до захисту даних. Посібник Офісу Уповноваженого з питань захисту персональних даних фіксує, що така ситуація породжує питання щодо узгодженості різних нормативних актів між собою, зокрема між положеннями Закону № 2297-VI та галузевих законів, що регулюють діяльність відповідних реєстрів [11]. Відсутність єдиних стандартів у підзаконних актах галузевих органів означає, що рівень захисту персональних даних у різних публічних цифрових системах є неоднорідним і залежить від того, наскільки ретельно конкретний орган підійшов до розробки власного порядку обробки даних.

Окремої уваги заслуговує системна колізія між режимом захисту персональних даних, встановленим Законом України «Про захист персональних даних», та режимом відкритості публічної інформації, визначеним Законом України «Про доступ до публічної інформації». Значна частина персональних даних, якими оперують органи публічної влади, є одночасно публічною інформацією і, відповідно, підпадає під обидва правові режими. Між ними виникають практичні колізії: стаття 5 Закону № 2297-VI

встановлює, що персональні дані, які стосуються здійснення особою, уповноваженою на виконання функцій держави, посадових повноважень, не є конфіденційною інформацією [118], тоді як на практиці органи місцевого самоврядування нерідко посилаються на захист персональних даних для обмеження доступу до відомостей, які за законом мають бути відкритими. Показовим прикладом є судова практика, зафіксована Центром демократії та верховенства права: Степанівська селищна рада відмовила у наданні інформації про розмір заробітних плат посадових осіб, посилаючись на захист персональних даних в умовах воєнного стану, однак суд визнав такі дії протиправними, підтвердивши, що відповідна інформація належить до безумовно відкритої [138]. Ця колізія є наслідком відсутності чіткого механізму розмежування сфер застосування двох законодавчих режимів і породжує правову невизначеність як для суб'єктів обробки даних, так і для суб'єктів персональних даних.

Ще одним виміром проблем взаємодії є відсутність чіткого розмежування компетенції між Уповноваженим і Мінцифри у сфері нормативного регулювання захисту персональних даних у цифрових публічних системах. Уповноважений затверджує підзаконні нормативно-правові акти у сфері захисту персональних даних, зокрема Типовий порядок обробки персональних даних [114], тоді як Мінцифри розробляє пропозиції щодо змін до нормативно-правових актів з питань захисту персональних даних і формує стандарти функціонування цифрових публічних систем [93]. Точний розподіл нормотворчих компетенцій між цими двома органами у сфері захисту персональних даних в цифровому публічному управлінні законодавчо не врегульований. Цифровізація публічного адміністрування актуалізує потребу у чіткому правовому регулюванні всіх аспектів захисту персональних даних у цифровому середовищі, зокрема й у питанні розподілу нормотворчих повноважень між відповідними органами.

Таким чином, взаємодія суб'єктів системи забезпечення захисту персональних даних у сфері цифрового публічного управління

характеризується відсутністю координаційного механізму, нормативною фрагментованістю, колізією правових режимів і недостатньою визначеністю розподілу компетенції між ключовими суб'єктами. Ці вади є проявом загальної інституційної незавершеності системи, що склалася в умовах відсутності спеціалізованого незалежного регулятора.

Проведений аналіз засвідчує, що система суб'єктів забезпечення захисту персональних даних у сфері цифрового публічного управління в Україні є інституційно сформованою, однак функціонально незавершеною. Наявні суб'єкти (Уповноважений Верховної Ради України з прав людини, Міністерство цифрової трансформації, галузеві органи-держателі реєстрів та органи місцевого самоврядування) виконують різні за характером функції у сфері захисту персональних даних, проте без належного координаційного механізму та в умовах відсутності спеціалізованого незалежного регулятора. Дослідження адміністративних процедур обробки персональних даних у системах цифрового публічного управління, яке є предметом наступного підрозділу, дозволить повніше розкрити практичний вимір функціонування цієї системи.

2.3. Характеристика основних адміністративних процедур обробки персональних даних у системах цифрового публічного управління

Дослідження адміністративних процедур обробки персональних даних у сфері цифрового публічного управління потребує насамперед концептуального визначення самого поняття «адміністративна процедура обробки персональних даних» та його відмежування від суміжних категорій. «Адміністративна процедура в цифровому форматі характеризується тим, що її основні стадії (подання заяви, розгляд, ухвалення рішення, повідомлення заявника) відбуваються повністю або частково із використанням електронних засобів комунікації, що передбачає електронну ідентифікацію та

аутентифікацію учасників, електронний документообіг і автоматизовану обробку даних» [23]. У контексті цифрового публічного управління будь-яка адміністративна процедура, що здійснюється із залученням цифрових систем, невіддільно пов'язана з обробкою персональних даних: реєстрація, верифікація, зберігання та передача відомостей про фізичних осіб є необхідними елементами такої процедури.

Базовим нормативним підґрунтям для розуміння відповідних процедур є Закон України «Про захист персональних даних», який визначає обробку персональних даних «будь-яку дію або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем» [118]. Кожна з цих операцій набуває специфічних ознак у контексті цифрового публічного управління, де вона здійснюється автоматизовано, у масовому масштабі та у рамках встановлених владних повноважень органів публічної адміністрації. Відповідно, адміністративну процедуру обробки персональних даних у сфері цифрового публічного управління визначимо як урегульовану нормативно-правовими актами послідовність дій органів публічної адміністрації, їх посадових осіб та уповноважених підприємств щодо збирання, зберігання, використання, передачі та знищення персональних даних фізичних осіб із застосуванням цифрових інформаційно-комунікаційних технологій у межах реалізації владних повноважень.

Як зазначають Р. Мигаль, Є. Фітяк та Д. Кузик цифровізація адміністративних процедур є не лише технологічним вдосконаленням управлінських процесів, а якісним оновленням правових механізмів, що забезпечує ефективне функціонування публічної влади та захист прав громадян у цифровій сфері [81]. Це твердження повністю поширюється і на процедури обробки персональних даних, зважаючи на те, що правовий вимір таких процедур є не менш важливим, ніж технологічний.

За стадіями обробки зазначені процедури поділяються на чотири основні групи:

1. Процедури збирання персональних даних, тобто первинного введення відомостей про фізичну особу до цифрових систем публічного управління. Вони охоплюють реєстрацію місця проживання, оформлення документів, подання заяв на адміністративні послуги, верифікацію особи через електронну ідентифікацію. Правовою підставою збирання є або відповідна норма закону, що уповноважує орган на збір певних категорій даних, або, у передбачених випадках, згода суб'єкта персональних даних [118]. Принципово важливо, що в умовах цифрового публічного управління збирання даних нерідко відбувається автоматично шляхом запиту до державних реєстрів, без безпосередньої участі особи у кожній конкретній операції.

2. Процедури зберігання персональних даних, що охоплюють накопичення, структурування та захист інформації у базах даних відповідних цифрових систем. Вимоги до зберігання включають, зокрема, дотримання принципу цільового обмеження (дані зберігаються лише в обсязі, необхідному для визначеної мети), забезпечення цілісності та конфіденційності даних, а також визначення строків зберігання. Закон № 2297-VI встановлює загальні вимоги до режиму зберігання, однак конкретні строки та порядок, як правило, визначаються галузевими нормативними актами.

3. Процедури передачі персональних даних, які в умовах цифрового публічного управління набувають особливого значення у зв'язку з розвитком систем міжвідомчого електронного обміну. Передача може здійснюватися між органами публічної влади в межах однієї держави (внутрішня передача), між органами і суб'єктами господарювання, а також через державний кордон (транскордонна передача). Правовою підставою передачі є або норма закону, що встановлює відповідні повноваження, або угода з особою [118]. У сфері цифрового публічного управління автоматизований характер передачі через системи міжвідомчої взаємодії породжує окремі специфічні правові проблеми.

4. Процедури знищення персональних даних, зокрема їх видалення з баз даних після досягнення мети обробки або закінчення встановленого строку зберігання. У цифрових системах публічного управління процедура знищення є технічно складнішою, ніж у традиційному паперовому діловодстві, так як дані можуть існувати у кількох копіях, резервних сховищах і розподілених системах одночасно. Відповідна правова проблема, що полягає у забезпеченні реального, а не лише формального знищення даних, є актуальною у сфері цифрового урядування.

Принципова особливість адміністративних процедур обробки персональних даних у сфері цифрового публічного управління полягає в їх переважно автоматизованому характері. На відміну від традиційної обробки, де кожна дія потребує безпосередньої участі посадової особи, в умовах цифрових систем більшість операцій здійснюється без участі людини, на основі заздалегідь визначених алгоритмів. Це підвищує швидкість і масштаб обробки, проте одночасно ускладнює реалізацію окремих прав суб'єктів персональних даних, зокрема права на доступ до інформації про обробку та права на заперечення проти неї. Стрімкий розвиток цифровізації адміністративних процедур супроводжується правовими викликами, серед яких фрагментарність нормативного регулювання, відсутність єдиного процесуального стандарту для цифрової форми та ризики порушення прав людини у сфері захисту персональних даних [23; 81].

Закон України «Про адміністративну процедуру» від 17.02.2022 № 2073-IX [100] заклав загальну процесуальну основу для адміністративних процедур в Україні, передбачивши можливість їх здійснення в електронній формі, однак не містить спеціальної деталізації порядку обробки персональних даних у рамках таких процедур. Це є нормативною прогалиною, що актуалізує потребу в дослідженні конкретних процедур обробки даних у ключових цифрових системах публічного управління.

Центральною інфраструктурою міжвідомчого електронного обміну в Україні є Система електронної взаємодії державних електронних

інформаційних ресурсів «Трембіта», яка є організаційно-технічною платформою, що дозволяє органам державної влади, органам місцевого самоврядування та суб'єктам господарювання будувати безпечні міжвідомчі інформаційні взаємодії [140]. В основі «Трембіти» лежить удосконалена естонська платформа обміну даними X-ROAD, адаптована до умов та вимог українського законодавства. Функціонування цієї системи нерозривно пов'язане з масштабною автоматизованою обробкою персональних даних громадян. Кожен запит до реєстру в автоматичному режимі, кожна транзакція в системі передбачає передачу, верифікацію або використання відомостей про конкретних фізичних осіб, що підпадає під сферу дії Закону України «Про захист персональних даних».

Правова природа системи «Трембіта» передбачає поєднання елементів адміністративно-правового регулювання (суб'єктний склад, повноваження, процедури підключення та доступу), інформаційно-правового регулювання (режим даних, стандарти обміну, захист інформації) та технічного регулювання (вимоги до шлюзів безпечного обміну, форматів електронних повідомлень, криптографічного захисту). Правову основу функціонування системи становлять Постанова Кабінету Міністрів України від 08.09.2016 № 606 «Деякі питання електронної взаємодії електронних інформаційних ресурсів» [28], Закон України «Про публічні електронні реєстри» № 1907-IX [125] та ряд інших нормативно-правових актів.

Відповідно до пункту 7 Положення про систему «Трембіта», затвердженого Постановою № 606, суб'єктами системи є: держатель системи; адміністратор системи; учасник системи, у тому числі оператор; суб'єкт електронної взаємодії. Держателем системи є Міністерство цифрової трансформації України, повноваження якого у цій ролі визначені пунктом 8 Положення, адміністратором визначене державне підприємство «ДІЯ», функції якого закріплені пунктом 9 Положення [28]. Учасниками є органи державної влади, органи місцевого самоврядування та суб'єкти господарювання, що мають зареєстрований шлюз безпечного обміну, а

суб’єктами електронної взаємодії власники електронних інформаційних ресурсів, що безпосередньо здійснюють обмін даними. Кожен із зазначених суб’єктів несе певний обсяг правових обов’язків щодо захисту персональних даних, що є предметом обміну.

Постанова КМУ № 606 закріплює такі принципи електронної інформаційної взаємодії як «технологічної нейтральності; використання єдиних правил, відкритих форматів даних, протоколів та стандартів обміну; інформування фізичних осіб про запити щодо їх персональних даних; повторного використання даних та програмних засобів; уникнення надлишковості та дублювання даних» [28]. Порівняльний аналіз цих принципів із стандартами захисту персональних даних виявляє як точки збігу, так і окремі розбіжності. Принцип уникнення надлишковості та дублювання даних кореспондує принципу мінімізації даних GDPR [180], що вимагає обробки лише тих персональних даних, які є необхідними та достатніми для досягнення законної мети. Принцип інформування фізичних осіб про запити щодо їх персональних даних відповідає праву суб’єкта даних на прозорість, закріпленому у Законі № 2297-VI [118]. Водночас принцип повторного використання даних потенційно суперечить принципу цільової обмеженості: дані, зібрані для однієї реєстрової мети, не можуть автоматично використовуватися в інших цілях, навіть якщо технічна можливість такого використання в системі є. Ця колізія є однією з ключових правових проблем функціонування системи міжвідомчого обміну з точки зору захисту персональних даних.

Участь у системі «Трембіта» передбачає проходження адміністративної процедури підключення. Загальні засади цієї процедури визначені Постановою № 606, відповідно до якої підключення здійснюється на договірній основі, а держатель системи затверджує угоду про приєднання та регламент роботи системи [28]. Деталізація конкретних процедурних кроків «реєстрації учасника, встановлення та реєстрації шлюзу безпечного обміну, публікації сервісів у каталозі системи) здійснюється Регламентом роботи

системи «Трембіта», затвердженим адміністратором системи. Реєстрація електронних інформаційних ресурсів у Національному реєстрі здійснюється відповідно до Закону України «Про публічні електронні реєстри» [125]. Кожен з цих кроків має самостійне правове значення з точки зору захисту персональних даних. Реєстрація конкретної електронної взаємодії означає формальне визначення обсягу та структури даних, якими обмінюватимуться суб'єкти. Цим встановлюється межа правомірного обміну, вихід за яку є порушенням принципу мінімізації. Угода про підключення є правовим інструментом розподілу відповідальності за захист даних між суб'єктами взаємодії. Разом з тим чинне законодавство не встановлює чітких вимог щодо обов'язкового включення до таких угод положень про захист персональних даних за аналогією до угод про обробку даних, передбачених статтею 28 GDPR (ч. 1, ч. 3) [180]. Ця прогалина є суттєвою, оскільки договірний механізм є в системах міжвідомчого обміну основним інструментом розподілу відповідальності за порушення у сфері захисту персональних даних.

Система «Трембіта» є децентралізованою, тобто вона не передбачає централізації даних і зміни їх власника, натомість надає доступ до даних державних реєстрів різним установам відповідно до заздалегідь визначених повноважень. Кожна конкретна взаємодія є строго регламентованою і споживач отримує лише ті дані, які необхідні для реалізації його конкретних повноважень і лише в обсязі, зафіксованому у зареєстрованому інтерфейсі взаємодії. Ця модель є важливою гарантією дотримання принципу мінімізації даних, однак її ефективність залежить від правильності первісного визначення обсягу даних, необхідних для кожної взаємодії, яке на практиці здійснюється технічними фахівцями відомств без обов'язкової оцінки впливу на захист персональних даних (DPIA – Data Protection Impact Assessment). Відповідно до статті 35 GDPR, такий тип обробки є саме тим, для якого проведення DPIA є обов'язковим [180]. Впровадження обов'язкової оцінки впливу як передумови реєстрації нової електронної взаємодії у системі є необхідним кроком для

приведення адміністративних процедур у відповідність до міжнародних стандартів.

Захист персональних даних у системі забезпечується також технічними засобами. Всі повідомлення, що передаються через «Трембіту», підписуються електронною печаткою та шифруються відповідно до національних криптографічних стандартів [164]. Як зазначають О. Задерейко та співавтори, системний аналіз захищеності державних електронних реєстрів та баз персональних даних є необхідною умовою забезпечення їх сталого функціонування [38]. Разом з тим, технічна захищеність каналу передачі не замінює правових гарантій, оскільки шифрування передачі не вирішує питань правомірності підстави конкретного запиту, відповідності обсягу запитаних даних принципу мінімізації та дотримання цільової обмеженості подальшого використання отриманих даних.

Аналіз адміністративних процедур обробки персональних даних у системі «Трембіта» дозволяє виявити три ключові правові прогалини. Першою є відсутність механізму повідомлення суб’єктів персональних даних про конкретні автоматизовані запити, оскільки принцип інформування, закріплений у Постанові № 606, не забезпечений конкретним процедурним механізмом реалізації на рівні кожної транзакції. Другою є нечіткий розподіл відповідальності між суб’єктами системи за порушення у сфері захисту персональних даних. У конкретній транзакції задіяні щонайменше постачальник і споживач даних та адміністратор системи, однак чинне законодавство не містить чіткого розподілу відповідальності між ними у разі витоку чи неправомірного обміну. Третьою є відсутність обов’язкової оцінки впливу на захист персональних даних як умови реєстрації нових електронних взаємодій, що є суттєвим ризиком з точки зору відповідності міжнародним стандартам. Подальша експлуатація, модернізація та інтеграція систем електронного урядування має сприяти налагодженню ефективної взаємодії між владою, бізнесом та громадськістю, однак ефективна взаємодія можлива лише за умови чіткої правової основи, яка гарантує захист прав усіх учасників,

включаючи суб’єктів персональних даних. Більш детально про це нами описано у [64].

Платформа «Дія» є центральним елементом цифрової інфраструктури публічних послуг в Україні та найбільшою за масштабом системою взаємодії між громадянами та органами публічної влади в цифровому середовищі. Правовою основою функціонування Порталу Дія є постанова Кабінету Міністрів України від 04.12.2019 № 1137 «Питання Єдиного державного вебпорталу електронних послуг» [92], а також Закон України «Про особливості надання публічних (електронних публічних) послуг» від 15.07.2021 № 1689-IX [122]. Технічним адміністратором порталу є державне підприємство «ДІЯ», що перебуває у сфері управління Мінцифри, тоді як Міністерство цифрової трансформації є його держателем і одночасно належить до кола суб’єктів, що здійснюють обробку персональних даних користувачів [94]. «Дослідження цифрових платформ для надання державних послуг підтверджує, що досвід України у розробленні та впровадженні платформи «Дія» показує, що цифровізація може значно спростити адміністративні процеси, скоротити бюрократичні бар’єри та підвищити доступність державних послуг, проте водночас актуалізує виклики захисту персональних даних і кібербезпеки» [133].

Особливістю платформи «Дія» з точки зору захисту персональних даних є застосування підходу data-in-transit (дані з реєстрів не зберігаються на серверах платформи, а передаються безпосередньо на пристрій користувача) [94]. Це принципово відрізняє архітектуру «Дії» від класичних централізованих баз даних і є важливою технічною гарантією мінімізації ризиків несанкціонованого доступу до персональних даних. Водночас для повноцінного функціонування платформа все ж обробляє певний обсяг персональних даних користувачів зокрема, дані електронного кабінету зберігаються протягом строку його функціонування, але не довше п’яти років [94]. Відповідно до Повідомлення про обробку персональних даних, Мінцифри є одночасно і володільцем, і розпорядником персональних даних,

що обробляються за допомогою програмних засобів Порталу Дія. Третіми особами, яким передаються персональні дані, є органи державної влади, органи місцевого самоврядування, підприємства та організації, що належать до сфери їх управління, яким дані передаються відповідно до визначеного законодавством порядку взаємодії між Порталом Дія та іншими електронними інформаційними ресурсами [94].

З процедурної точки зору отримання електронної публічної послуги через «Дію» охоплює кілька послідовних операцій із персональними даними.

1. Ідентифікація та аутентифікація особи через механізм Дія.Підпис або MobileID.

2. Автоматизований запит з реєстрів даних, необхідних для надання конкретної послуги. Зокрема, при оформленні комплексних послуг («єМалятко», «єОселя», «єПідтримка») система автоматично запитує дані з кількох реєстрів одночасно без необхідності для особи подавати ці відомості вручну.

3. Обробка поданої заяви, у тому числі можлива передача даних до відповідного органу публічної влади для прийняття рішення.

4. Видача результату послуги в електронній формі та збереження відповідних записів.

Цифровізація адміністративних послуг як така спрямована на формування сервісної держави, основною функцією якої є захист інтересів та задоволення потреб громадян шляхом їх обслуговування [71], і саме тому правові основи процедур обробки персональних даних у відповідних системах є невіддільною від якості самих послуг.

Правовою підставою обробки персональних даних при наданні електронних публічних послуг є, як правило, норма закону, що встановлює повноваження відповідного органу та визначає перелік необхідних даних. Це відповідає підпункту 2 частини першої статті 11 Закону України «Про захист персональних даних», який передбачає як підставу обробки «дозвіл на обробку персональних даних, наданий володільцю бази персональних даних

відповідно до закону виключно для здійснення його повноважень» [118]. Разом з тим Закон України «Про особливості надання публічних (електронних публічних) послуг» не містить спеціального регулювання питань обробки персональних даних у процесі надання електронних публічних послуг [122], що є нормативною прогалиною, яка потребує усунення.

Принциповою особливістю платформи «Дія» є функція сповіщення громадянина про факт запиту його персональних даних державними органами. Кожного разу, коли орган публічної влади здійснює запит щодо персональних даних особи через підключені до платформи системи, користувач отримує відповідне повідомлення у мобільному додатку «Дія». Таким чином реалізується право суб'єкта персональних даних знати про джерела збирання своїх даних та мету їх обробки, закріплене у пунктах 1-2 частини другої статті 8 Закону України «Про захист персональних даних» [118]. Цей механізм є практичною реалізацією принципу прозорості і усуває прогалину, яку було виявлено при аналізі системи «Трембіта» раніше. На відміну від «Трембіти», «Дія» забезпечує конкретний технічний механізм інформування особи про автоматизовані запити щодо її даних. Аналогічний механізм закріплено і на законодавчому рівні для Єдиної інформаційної системи соціальної сфери. Закон № 4607-IX (набере чинності 27.05.2026) прямо передбачає право особи на отримання інформації про запити будь-яких осіб щодо інформації про неї із «застосуванням електронного сповіщення засобами мобільного зв'язку чи шляхом розміщення повідомлення в електронному кабінеті» [112]. Такий підхід є позитивним прикладом нормативного закріплення механізму нотифікації суб'єктів персональних даних, що заслуговує на поширення на інші цифрові системи публічного управління.

Повідомлення про обробку персональних даних Порталу «Дія» прямо відтворює перелік прав суб'єктів персональних даних: право знати про джерела збирання та мету обробки; право на доступ до своїх персональних даних; право на виправлення та знищення даних; право заперечувати проти обробки [118; 94]. Реалізація цих прав у цифровому середовищі має свою

специфіку. Зокрема, видалення електронного кабінету на Порталі Дія автоматично тягне видалення персональних даних (п. 7 Повідомлення), що є важливим механізмом практичного забезпечення права на знищення даних.

Реєстрові системи публічного управління є основними носіями персональних даних громадян у цифровому середовищі держави. На відміну від транзитних систем («Трембіти» і «Дії») реєстри здійснюють довгострокове зберігання персональних даних і є первинним джерелом відомостей, що використовуються для надання адміністративних послуг, соціальних виплат, ідентифікації особи та виконання інших публічних функцій. У цьому контексті адміністративні процедури обробки персональних даних у реєстрових системах мають ключове значення для розуміння адміністративно-правового механізму захисту персональних даних у сфері цифрового публічного управління загалом. Розглянемо особливості цих процедур на прикладі двох великих реєстрових систем: Єдиного державного демографічного реєстру (ЄДДР) та Електронної системи охорони здоров'я (ЕСОЗ).

ЄДДР є електронною інформаційно-комунікаційною системою, призначеною для зберігання, захисту, обробки, використання і поширення визначеної законом інформації про особу та про документи, що оформлюються із застосуванням засобів реєстру, із забезпеченням дотримання гарантованих Конституцією України свободи пересування та заборони втручання в особисте і сімейне життя. Правовою основою функціонування ЄДДР є Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» від 20.11.2012 № 5492-VI [111].

З точки зору захисту персональних даних принципово важливими є статті 8, 9 та 11 цього Закону. Стаття 8 встановлює гарантії захисту і безпеки інформації реєстру, зокрема пряму заборону особам, які працюють з базами даних реєстру, вимагати, обробляти та використовувати будь-яку інформацію, не передбачену законом. Ця заборона є практичною реалізацією принципу мінімізації даних та цільового обмеження у вітчизняному реєстровому

законодавстві. Стаття 9 закріплює права осіб, персональні дані яких внесені до реєстру, серед яких особливої уваги заслуговує право «отримання від уповноважених суб'єктів на безоплатній основі повідомлення про кожен випадок звернення щодо передачі інформації про неї з Реєстру» [111]. Це право є найбільш розвиненим механізмом нотифікації суб'єктів персональних даних серед усіх розглянутих у цьому підрозділі систем. На відміну від принципу інформування у «Трембіті», де відсутній конкретний процедурний механізм, та механізму сповіщень у «Дії», що охоплює лише запити через відповідну платформу, стаття 9 Закону № 5492-VI прямо зобов'язує уповноважених суб'єктів повідомляти особу про кожен окремий випадок звернення щодо передачі її даних.

Стаття 11 Закону детально регулює порядок отримання інформації з ЄДДР, встановлюючи вичерпний перелік суб'єктів, що мають право на доступ, та обсяг відомостей, що їм надаються [111]. Надання даних про особу здійснюється виключно у випадках, передбачених законами України, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини або за згодою самої особи. Це формулювання є більш обмежувальним, ніж загальна норма Закону, і відображає підвищений рівень захисту, що застосовується до даних цієї реєстрової системи. Водночас ряд змін до статті 11, внесені протягом 2022-2023 років у зв'язку з воєнним станом, суттєво розширили коло суб'єктів, що мають право на отримання даних з реєстру, зокрема щодо передачі даних до реєстрів призовників та військовозобов'язаних [111]. Це є проявом загальної тенденції розширення підстав обробки персональних даних в умовах воєнного стану, про що нами було описано раніше.

ЕСОЗ є інформаційно-комунікаційною системою, що забезпечує автоматизацію ведення обліку медичних послуг та управління медичною інформацією шляхом створення, розміщення, оприлюднення та обміну інформацією, даними і документами в електронному вигляді. Правову основу функціонування ЕСОЗ становить постанова КМУ від 25.04.2018 № 411 «Деякі

питання електронної системи охорони здоров'я» [29]. ЕСОЗ має дворівневу архітектуру, до якої входить центральна база даних (ЦБД), держателем якої є Національна служба здоров'я України (НСЗУ), та медичні інформаційні системи (МІС), що забезпечують програмне забезпечення медичних закладів, через яке здійснюється введення даних та їх передача до ЦБД.

Принципово важливою особливістю ЕСОЗ з точки зору захисту персональних даних є архітектурне розмежування між персональними та медичними даними пацієнта. Такі дані зберігаються відокремлено у різних кластерах ЦБД у зашифрованому вигляді та пов'язуються між собою лише через унікальний ідентифікатор пацієнта [29]. Таке технічне рішення унеможливлює безпосереднє зіставлення ідентифікованої особи з її медичними даними у разі несанкціонованого доступу, що відповідає принципу «захисту за архітектурним задумом» (privacy by design).

Медична інформація про пацієнта є особливою категорією персональних даних. Дані про стан здоров'я відповідно до статті 7 Закону України «Про захист персональних даних» відносяться до чутливих категорій і потребують підвищеного рівня захисту [118]. Обробка таких даних допускається лише у суворо визначених законом випадках. У контексті ЕСОЗ доступ медичного працівника до медичних даних пацієнта в ЦБД здійснюється або за наданою пацієнтом згодою, або без такої згоди у передбачених законом випадках, зокрема, у невідкладних медичних ситуаціях [29]. Це є одним із небагатьох прикладів у системі цифрового публічного управління України, де законодавство чітко закріплює механізм згоди суб'єкта персональних даних як умову доступу до його даних, а не лише посилається на законодавчо визначені повноваження відповідного органу.

Зіставлення адміністративних процедур обробки персональних даних в ЄДДР і ЕСОЗ дозволяє виявити як спільні риси, так і суттєві відмінності у рівні правових гарантій. Обидві системи функціонують на підставі спеціальних нормативних актів, що встановлюють вичерпний перелік підстав доступу, коло уповноважених суб'єктів та гарантії захисту. Водночас ЄДДР

вирізняється найбільш розвиненим механізмом нотифікації суб'єктів (правом на повідомлення про кожен випадок звернення щодо передачі даних), тоді як ЕСОЗ найбільш чіткою технічною гарантією захисту через архітектурне розмежування персональних і медичних даних. Спільною правовою прогалиною для обох систем є відсутність обов'язкової оцінки впливу на захист персональних даних при запровадженні нових функціоналів та розширенні кола суб'єктів доступу – вимоги, що відповідає статті 35 GDPR [180] і залишається нереалізованою в українському реєстровому законодавстві.

Аналіз адміністративних процедур обробки персональних даних у конкретних цифрових системах публічного управління, здійснений вище, дозволяє виявити ряд наскрізних правових проблем, що стосуються реалізації прав суб'єктів персональних даних. Окремі з них потребують окремого розгляду, оскільки виходять за межі будь-якої конкретної платформи і мають системний характер.

Частина перша статті 11 Закону України «Про захист персональних даних» встановлює шість підстав для обробки персональних даних. Для сфери цифрового публічного управління ключовою є друга підстава: «дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень» [118]. Саме ця підстава є типовою для функціонування державних реєстрів, систем міжвідомчого обміну та платформ електронних послуг. Таким чином, згода суб'єкта персональних даних у сфері цифрового публічного управління не є типовою підставою обробки, оскільки органи публічної влади обробляють персональні дані на підставі закону, а не індивідуального дозволу особи. Це принципово відрізняє правовий режим обробки персональних даних у публічному управлінні від режиму, встановленого для приватних суб'єктів. Виняток становлять чутливі категорії персональних даних. Зокрема, доступ лікаря до медичних даних пацієнта в ЕСОЗ за загальним правилом потребує явної згоди пацієнта [29]. Разом з тим обробка персональних даних на підставі

закону не звільняє органи публічної влади від обов'язку забезпечити особі реалізацію її прав, передусім права на доступ до своїх даних, права на їх виправлення та права бути повідомленою про факт обробки.

Порівняльний аналіз каталогу прав суб'єктів персональних даних за Законом України «Про захист персональних даних» і GDPR виявляє суттєву відмінність у частині права на знищення даних. GDPR закріплює самостійне право на стирання, або «право бути забутим» (ст. 17 GDPR), що дозволяє особі вимагати видалення своїх даних за певних умов без обов'язкового звернення до суду [180]. Чинне українське законодавство передбачає видалення або знищення персональних даних на чотирьох підставах: закінчення строку зберігання, припинення правовідносин, припис Уповноваженого та рішення суду [118]. Принципова відмінність від GDPR полягає в тому, що ст. 17 GDPR надає суб'єкту даних пряме право вимагати від контролера видалення своїх даних на широких підставах, зокрема, у разі відкликання згоди або якщо дані більше не є необхідними для мети обробки [180]. Вмотивована вимога суб'єкта за п. 6 ч. 2 ст. 8 Закону № 2297-VI обмежена лише двома підставами: незаконна обробка або недостовірність даних [118]. Таким чином, право особи ініціювати знищення своїх персональних даних у чинному українському законодавстві є суттєво вужчим, ніж «право на забуття» за GDPR. Ця прогалина є особливо відчутною у контексті цифрових систем публічного управління, де обробка персональних даних здійснюється масово й автоматизовано та може бути усунена шляхом прийняття нового закону про захист персональних даних з урахуванням стандартів GDPR.

Навіть за наявності правових підстав для знищення персональних даних їх практична реалізація у розподілених цифрових системах є значно складнішою, ніж у традиційних паперових архівах. Дані, отримані одним органом від іншого через систему «Трембіта», можуть бути збережені у власних інформаційних системах органу-отримувача, а знищення «вихідних» даних у реєстрі-постачальнику не тягне автоматичного знищення їхніх копій у системах органів-отримувачів. Ця проблема є проявом загальної прогалини

відсутності у чинному законодавстві чіткого регулювання долі персональних даних після завершення мети, для якої вони передавались між суб'єктами електронної взаємодії. Закон України «Про публічні електронні реєстри» містить лише загальні засади щодо строків зберігання реєстрової інформації [125], тоді як питання синхронізованого знищення даних у розподілених системах залишається поза межами нормативного регулювання.

Окремим аспектом адміністративних процедур обробки персональних даних у сфері цифрового публічного управління є транскордонна передача персональних даних. Стаття 29 Закону № 2297-VI встановлює загальне правило: «передача персональних даних іноземним суб'єктам відносин, пов'язаних із персональними даними, здійснюється лише за умови забезпечення відповідною державою належного захисту персональних даних у випадках, встановлених законом або міжнародним договором України» [118]. В умовах воєнного стану зазначена проблематика набула особливої гостроти у зв'язку з використанням хмарних технологій для зберігання державних інформаційних ресурсів, у тому числі тих, що містять персональні дані громадян. Постанова КМУ від 21.03.2022 № 263 дозволила зберігати державні інформаційні ресурси у хмарних сервісах закордонних провайдерів, однак без спеціального механізму захисту персональних даних при такій передачі [30].

Проведений аналіз адміністративних процедур обробки персональних даних у ключових системах цифрового публічного управління України свідчить про те, що ці процедури є різноманітними за своєю правовою природою та структурою і утворюють якісно відмінні моделі залежно від типу системи, що потребує диференційованих правових підходів до їх регулювання. Водночас усі розглянуті системи об'єднує спільна системна проблема: попри наявність розгорнутого каталогу прав суб'єктів персональних даних, рівень їх практичної реалізації залишається нерівномірним, а окремі механізми, зокрема право на знищення даних у розподілених системах та обов'язкова оцінка впливу на захист персональних

даних, взагалі відсутні на нормативному рівні. Зазначені недоліки зумовлюють необхідність удосконалення адміністративно-правового механізму захисту персональних даних у сфері цифрового публічного управління.

Висновки до розділу 2

Проведене дослідження адміністративно-правового механізму захисту персональних даних у сфері цифрового публічного управління в його статичному вимірі дозволило сформувати ряд висновків. Нормативно-правове регулювання у цій сфері є багаторівневим, однак характеризується системною фрагментарністю: норми Закону України «Про захист персональних даних», галузевого законодавства та підзаконних актів функціонують паралельно без належної внутрішньої узгодженості, що породжує правову невизначеність у правозастосовній практиці. Система суб’єктів забезпечення захисту персональних даних є інституційно сформованою, проте функціонально незавершеною: відсутність спеціалізованого незалежного регулятора, нечіткий розподіл компетенції між Уповноваженим і Мінцифри та слабкість координаційних механізмів знижують загальну ефективність наглядової функції держави у цій сфері. Аналіз адміністративних процедур обробки персональних даних у конкретних цифрових системах («Трембіті», «Дії», ЄДДР та ЕСОЗ) засвідчив, що при загальній технологічній розвиненості цих систем правове забезпечення захисту персональних даних у них залишається недостатнім, оскільки механізми нотифікації суб’єктів є нерівномірними, право на знищення даних позбавлене ефективного позасудового механізму, а обов’язкова оцінка впливу на захист персональних даних як системний інструмент превентивного контролю відсутня. Зазначені недоліки визначають напрями вдосконалення адміністративно-правового механізму захисту персональних даних.

РОЗДІЛ 3
УДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ ЦИФРОВІЗАЦІЇ ПУБЛІЧНОГО УПРАВЛІННЯ

3.1. Адміністративна відповідальність за порушення законодавства про захист персональних даних

Адміністративна відповідальність є одним із ключових елементів механізму правового регулювання, що надає охоронній функції права реального забезпечувального значення. Без ефективного механізму відповідальності нормативні вимоги щодо захисту персональних даних перетворюються на декларативні приписи, позбавлені примусового потенціалу. Саме тому стан адміністративної відповідальності у сфері захисту персональних даних є вагомим індикатором практичної ефективності всього адміністративно-правового механізму захисту. Аналіз чинного законодавства свідчить, що цей індикатор фіксує системну дисфункцію. Єдина спеціальна норма адміністративної відповідальності у відповідній сфері, а саме стаття 188-39 Кодексу України про адміністративні правопорушення [55], є очевидно недостатньою як за обсягом охоплюваних діянь, так і за розміром передбачених санкцій. Чинна редакція цієї статті, сформована після реформи 2013 року, передбачає три самостійні склади адміністративного правопорушення: «неповідомлення або несвоєчасне повідомлення Уповноваженого ВРУ з прав людини про обробку персональних даних або про зміну відомостей, що підлягають повідомленню, а також повідомлення неповних чи недостовірних відомостей; невиконання законних вимог (приписів) Уповноваженого або визначених ним посадових осіб секретаріату щодо запобігання або усунення порушень законодавства про захист персональних даних; недодержання встановленого законодавством порядку

захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних» [55].

Санкція статті диференційована залежно від складу та суб'єкта правопорушення. За першим складом передбачено штраф на громадян від 100 до 200 неоподатковуваних мінімумів доходів громадян (далі – н.м.д.г.) та на посадових осіб і суб'єктів підприємницької діяльності від 200 до 400 н.м.д.г. За другим – відповідно від 200 до 300 та від 300 до 1000 н.м.д.г. За третім – від 100 до 500 та від 300 до 1000 н.м.д.г. У разі повторного вчинення правопорушення протягом року розмір штрафів збільшується до 1000-2000 н.м.д.г. [55]. З огляду на те, що один н.м.д.г. становить 17 гривень, максимальний розмір штрафу за повторне правопорушення не перевищує 34 000 грн. Зазначимо, що це сума, яка не може відігравати помітної превентивної ролі щодо суб'єктів, що обробляють персональні дані в значних обсягах.

Аналіз диспозиції ст. 188-39 КУпАП крізь призму сучасних стандартів захисту персональних даних дозволяє виявити кілька принципових прогалин. Найсуттєвішою є відсутність відповідальності за порушення принципів обробки персональних даних, закріплених у ст. 6 Закону № 2297-VI [118]. Порушення принципу мінімізації, цільового обмеження, точності даних чи обмеження строків зберігання не утворює складу жодного адміністративного правопорушення навіть у разі, якщо воно є очевидним і систематичним. Третій склад ст. 188-39 КУпАП охоплює лише порушення порядку захисту, що призвели до конкретного наслідку, а саме незаконного доступу або порушення прав суб'єкта. Таким чином, за межами адміністративної відповідальності залишаються численні систематичні порушення, що не потягли формально кваліфікованих наслідків, але суперечать основоположним принципам обробки персональних даних.

Відсутня також відповідальність за відмову у реалізації таких прав суб'єктів персональних даних як незабезпечення доступу особи до її даних, ухилення від виконання вимоги про виправлення чи знищення даних або від повідомлення про обробку. Закон № 2297-VI закріплює ці права як суб'єктивні

права особи [118], однак КУпАП не передбачає жодної санкції за їх порушення з боку суб'єктів обробки, що фактично позбавляє відповідні права механізму реалізації їх захисту.

Суб'єктами правопорушень за ст. 188-39 КУпАП є громадяни, посадові особи та громадяни суб'єкти підприємницької діяльності [55]. Юридичні особи як самостійні суб'єкти адміністративної відповідальності у цій сфері відсутні. Між тим саме юридичні особи (підприємства, установи та організації) є типовими операторами масової обробки персональних даних. Персональна відповідальність посадової особи з максимальним штрафом у 34000 гривень не є відчутним стимулом для системних організаційних змін у великій компанії чи державній установі. Для порівняння: стаття 83 GDPR передбачає штрафи на юридичних осіб у розмірі до 20 млн євро або 4% річного глобального обороту залежно від того, яка сума є більшою [180]. Поряд з адміністративною відповідальністю за ст. 188-39 КУпАП чинне законодавство передбачає і кримінальну відповідальність у суміжній сфері. Стаття 182 Кримінального кодексу України встановлює відповідальність за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконну зміну такої інформації, передбачаючи санкції у вигляді штрафу від 500 до 1000 н.м.д.г., виправних робіт або обмеження волі до трьох років [73]. Однак відсутність чіткої нормативної межі між адміністративним правопорушенням за ст. 188-39 КУпАП і кримінальним правопорушенням за ст. 182 ККУ породжує правову невизначеність у кваліфікації конкретних діянь, а вкрай мала кількість обвинувальних вироків за цією статтею свідчить про те, що й кримінально-правовий механізм захисту персональних даних залишається переважно декларативним. Ця диспропорція відображає принципово різні підходи до розуміння функції санкції у сфері захисту персональних даних.

Нормативна недостатність статті 188-39 КУпАП знаходить своє підтвердження і в площині правозастосовної практики. Якщо нормативні прогалини є свідченням недоліку законодавства, то стан правозастосування є

свідченням системних недоліків функціонування механізму адміністративної відповідальності у сфері захисту персональних даних загалом. У теорії права усталеною є теза про те, що без втілення правових приписів у реальну поведінку суб'єктів норми права втрачають своє соціальне призначення і перетворюються на суто декларативні конструкції [37]. У правовій доктрині та науковому дискурсі такі норми прийнято характеризувати як «мертві», тобто формально чинні, але фактично позбавлені правозастосовного змісту внаслідок системних дисфункцій механізму їх реалізації. Стаття 188-39 КУпАП є саме таким прикладом, оскільки попри формальну чинність і наявність санкцій, ця норма фактично не застосовується в масштабах, навіть наближених до реального рівня порушень у сфері захисту персональних даних.

Показовими є дані щорічних доповідей Уповноваженого Верховної Ради України з прав людини. Так, за результатами 2024 року до Уповноваженого надійшло 7312 загальних звернень, з яких значна частина стосувалась порушень у сфері захисту персональних даних. За цей же рік Секретаріатом Уповноваженого складено загалом лише 40 протоколів про адміністративні правопорушення за статтями 188-39, 188-40 та 212-3 КУпАП разом, з яких безпосередньо за ст. 188-39 КУпАП – лише 2 протоколи [161]. Для порівняння: за даними того ж Уповноваженого, лише у 2023 році надійшло 652 повідомлення про незаконну обробку персональних даних [162]. Таким чином, між кількістю зафіксованих порушень і кількістю складених протоколів існує разюча невідповідність – менш ніж 0,5% порушень трансформуються у протоколи про адміністративне правопорушення. Ще менша частина справ доходить до стадії реального накладення стягнень.

Аналогічну картину фіксує аналіз матеріалів Єдиного державного реєстру судових рішень. Станом на 2018 рік у реєстрі налічувалось лише 27 документів, пов'язаних із порушенням законодавства у сфері захисту персональних даних [178]. Динаміка наступних років суттєво не змінила цієї картини: кількість справ за ст. 188-39 КУпАП у судовій практиці залишається

мізерною на тлі масштабів реальних порушень. Схожу тенденцію спостерігаємо і щодо ст. 182 ККУ, за якою у 2007-2021 роках було постановлено лише 22 обвинувальні вироки [74], що також свідчить про неефективність кримінально-правового механізму захисту персональних даних.

Серед справ, що доходять до судового розгляду, типовою є справа № 361/1579/20, розглянута Броварським міськрайонним судом Київської області. За обставинами цієї справи голова правління садового товариства поширила у загальному чаті месенджера звернення особи, що містило її прізвище, ім'я, по батькові, адресу, номер телефону та електронну адресу. Суд визнав голову правління винною у вчиненні правопорушення, передбаченого ч. 4 ст. 188-39 КУпАП, і наклав стягнення у розмірі 5100 гривень. Це рішення залишив без змін Київський апеляційний суд та Касаційний адміністративний суд Верховного Суду [96]. Наведена справа є показовою у кількох відношеннях. По-перше, вона ілюструє той тип порушення, який дійсно охоплюється ст. 188-39 КУпАП, а саме конкретне поширення персональних даних без згоди особи. По-друге, вона демонструє типовий суб'єкт відповідальності, яким у даному випадку виступає посадова особа невеликої організації, а не великий оператор масової обробки даних. По-третє, розмір фактично накладеного стягнення у 5100 грн. жодним чином не відповідає навіть мінімальному стримувальному ефекту.

Аналіз структурних причин феномену «мертвої норми» у цій сфері виявляє кілька взаємопов'язаних чинників. Уповноважений ВРУ з прав людини наділений повноваженнями складати протоколи про адміністративні правопорушення, однак не має права самостійно накладати стягнення. Справи передаються до суду, що суттєво подовжує та ускладнює процедуру притягнення до відповідальності. Додатковою перешкодою є проблема доказування, так як порушення у сфері захисту персональних даних нерідко відбуваються у цифровому середовищі, де збирання та процесуальне закріплення належних доказів є самостійним і складним завданням. Не менш

суттєвою є низька правова обізнаність суб’єктів персональних даних щодо їхніх прав і механізмів захисту, внаслідок чого переважна більшість порушень взагалі не стає предметом скарг. Нарешті, відсутність достатнього ресурсного забезпечення унеможливлює проведення Уповноваженим систематичних перевірок у цій сфері. Показово, що сам наглядовий орган у щорічній доповіді констатує потребу у розширенні власних повноважень щодо безпосереднього накладення штрафів та стягнень без обов’язкового судового провадження [161], що є вагомим аргументом на користь реформування інституційного механізму відповідальності.

Наведені вище дані про стан правозастосування набувають особливої гостроти в контексті реального масштабу порушень у сфері захисту персональних даних в Україні. Питання полягає не лише в тому, що ст. 188-39 КУпАП фактично не застосовується, а й у тому, наскільки ця ситуація відповідає реальному стану дотримання законодавства. Як видно з викладеного вище, між масштабом порушень і реакцією держави існує значний розрив, що підкреслює суттєві прогалини в рамках концепції ефективного механізму адміністративної відповідальності.

За даними щорічної доповіді Уповноваженого ВРУ з прав людини, лише у 2023 році до Секретаріату надійшло 1205 звернень (1336 повідомлень) щодо ймовірного порушення права на захист персональних даних [162]. У 2024 році загальна кількість звернень до Уповноваженого сягнула 1550, що на 28,6% більше порівняно з 2023 роком, причому кожне четверте звернення у категорії громадянських прав стосувалося питань доступу до інформації та захисту персональних даних [161]. Водночас у 2023 році кількість зареєстрованих в Україні кіберінцидентів зросла на 62,5% порівняно з попереднім роком, і метою значної частини кібератак було саме заволодіння персональними даними [162]. При цьому наведені цифри фіксують лише видиму частину значно більшого явища, оскільки переважна більшість порушень у сфері захисту персональних даних взагалі не стає предметом звернень через низьку

правову обізнаність суб’єктів персональних даних та відсутність у них практичного розуміння механізмів захисту своїх прав.

На тлі наведених даних можна прослідкувати недостатність реакції держави. За умов, коли щороку фіксуються сотні повідомлень про порушення у сфері захисту персональних даних, кількість складених протоколів про адміністративні правопорушення залишається одиничною, а реальне накладення стягнень є поодиноким. Таке співвідношення унеможливлює виконання санкцією її превентивної та каральної функцій і фактично сигналізує суб’єктам обробки персональних даних про відсутність реального ризику відповідальності за порушення законодавства.

Наведені дані свідчать про те, що дисбаланс між масштабом порушень і реакцією держави не є випадковим збігом обставин або тимчасовою дисфункцією, він є структурною характеристикою чинного механізму адміністративної відповідальності у цій сфері. В його основі лежить сукупність взаємопов’язаних чинників: недостатня охопність ст. 188-39 КУпАП, що виключає переважну більшість реально поширених порушень зі сфери адміністративної відповідальності; процедурна обтяженість механізму притягнення до відповідальності; відсутність у наглядового органу повноважень щодо самостійного накладення стягнень та символічний розмір санкцій, що не створює жодного стримувального ефекту. Результатом є ситуація, за якої суб’єкти обробки персональних даних фактично позбавлені будь-якого реального ризику адміністративної відповідальності, що є неприйнятним з точки зору сучасних стандартів захисту персональних даних. Саме ці стандарти, закріплені у праві ЄС, визначають той орієнтир, відносно якого слід оцінювати наявний стан речей.

Аналіз санкційного механізму адміністративної відповідальності за порушення у сфері захисту персональних даних у праві ЄС дає змогу визначити нормативний стандарт, відносно якого слід оцінювати чинну українську модель. Основним інструментом такого порівняння є стаття 83 Регламенту (ЄС) 2016/679 (GDPR) [180], яка закріплює дворівневу систему

адміністративних штрафів, побудовану на принципах ефективності, пропорційності та стримувального ефекту.

Перший рівень охоплює порушення організаційно-технічних вимог та обов'язків контролера і оператора. Зокрема, недотримання принципів захисту даних за замовчуванням, порушення вимог щодо ведення реєстрів обробки, призначення відповідальних осіб тощо. За такі порушення ст. 83(4) GDPR передбачає штраф до 10 млн. євро або до 2% загального глобального річного обігу підприємства, залежно від того, яка сума є вищою [180]. Другий рівень охоплює більш серйозні порушення, а саме недотримання основних принципів обробки, умов надання згоди, прав суб'єктів даних, незаконної передачі даних до третіх країн. За ці порушення ст. 83(5) GDPR передбачає штраф до 20 млн. євро або до 4% глобального річного обігу [180]. Принципово важливим є те, що GDPR не встановлює нижньої межі штрафу, а його конкретний розмір визначається наглядовим органом з урахуванням тяжкості, тривалості та характеру порушення, кількості постраждалих суб'єктів, наявності умислу та інших обставин.

Наглядові органи держав-членів ЄС активно застосовують зазначені санкції. Люксембурзький регулятор із захисту даних наклав штраф на Amazon 746 млн. євро, ірландський регулятор на Meta 1,2 млрд. євро за передачу даних до США [46]. Показово, що навіть відносно менш значущі порушення, пов'язані, наприклад, із неналежним позначенням про ведення відеозйомки, призводять до накладення штрафів у тисячах євро. Дослідницька служба Верховної Ради України у своїй аналітичній довідці констатує, що практика застосування фінансових санкцій наглядовими органами держав-членів є значно більш поширеною, ніж судові позови про відшкодування збитків [46].

Зіставлення санкційних механізмів ст. 188-39 КУпАП і ст. 83 GDPR виявляє принципову відмінність не лише кількісного, а й якісного характеру. По-перше, максимальний розмір штрафу за ст. 188-39 КУпАП становить 34 тис. грн., тоді як верхня межа за GDPR 20 млн. євро, тобто різниця у понад 17000 разів. По-друге, суб'єктом відповідальності за ст. 188-39 КУпАП є лише

фізична особа або ФОП, тоді як GDPR передбачає відповідальність підприємства як такого, розраховуючи штраф від його глобального обороту. По-третє, GDPR застосовується безпосередньо наглядовим органом без обов'язкового судового провадження, що суттєво підвищує оперативність реагування. По-четверте, на відміну від трьох вузьких складів ст. 188-39 КУпАП, GDPR охоплює широкий спектр порушень від недотримання принципів обробки до порушень прав суб'єктів та незаконної транскордонної передачі даних.

Наведені відмінності відображають різні концептуальні підходи до функції адміністративної відповідальності у сфері захисту персональних даних. Якщо ст. 188-39 КУпАП виконує переважно символічну функцію, то ст. 83 GDPR є інструментом реального управління поведінкою суб'єктів обробки через економічний ризик. З урахуванням курсу України на гармонізацію з правом ЄС у рамках виконання Угоди про асоціацію, саме модель GDPR має визначати вектор реформування вітчизняного механізму адміністративної відповідальності у цій сфері.

Стан правозастосовної практики за ст. 188-39 КУпАП є не лише наслідком інституційних та процедурних недоліків, а й прямим відображенням системних прогалин у самому законодавстві. Ці прогалини стосуються як складів адміністративних правопорушень, так і суб'єктного складу відповідальності, санкцій і меж розмежування між адміністративною та кримінальною відповідальністю.

Закон України «Про захист персональних даних» закріплює у ст. 6 низку основоположних принципів обробки персональних даних, таких як законність, цільове обмеження, мінімізація, точність, обмеження строків зберігання [118]. Порушення цих принципів є найбільш поширеним типом порушень у практиці наглядових органів держав членів ЄС. Однак жоден із трьох складів ст. 188-39 КУпАП не охоплює такі порушення безпосередньо [55]. Третій склад, що передбачає відповідальність за недодержання порядку захисту персональних даних, охоплює лише ті випадки, коли порушення призвело до конкретного

наслідку, яким може бути незаконний доступ або порушення прав суб'єкта. Систематична обробка надмірних даних, зберігання їх поза межами встановлених строків або обробка з метою, відмінною від задекларованої, не передбачають жодної адміністративної відповідальності, якщо не спричинили формально кваліфікованих наслідків.

Закон № 2297-VI закріплює широкий перелік прав суб'єктів персональних даних: право на доступ до своїх даних, їх виправлення, знищення, заперечення проти обробки тощо [118]. Разом з тим, відмова у реалізації цих прав з боку суб'єктів обробки не утворює жодного складу адміністративного правопорушення за чинним КУпАП. Таким чином, права, гарантовані матеріальним законодавством, позбавлені механізму адміністративно-правового примусу до їх виконання. Аналогічна ситуація склалася щодо порушень, пов'язаних із відсутністю правової підстави для обробки персональних даних або обробкою без згоди суб'єкта у випадках, коли така згода є обов'язковою.

Як зазначено вище суб'єктами відповідальності за ст. 188-39 КУпАП є виключно громадяни та посадові особи, а юридичні особи як самостійні суб'єкти адміністративної відповідальності у цій сфері відсутні [55]. Між тим переважна більшість суб'єктів масової обробки персональних даних як банки, телекомунікаційні оператори, медичні установи, органи публічної влади є саме юридичними особами. Покладення відповідальності виключно на конкретну посадову особу не забезпечує системних змін у практиці обробки даних організацією і не створює організаційних стимулів до дотримання законодавства. К. Головко у своєму дослідженні адміністративно-правових аспектів захисту персональних даних також констатує невідповідність суб'єктного складу відповідальності реальній структурі суб'єктів обробки в умовах цифровізації [23].

Цифровізація публічного управління супроводжується стрімким розширенням практики автоматизованої обробки персональних даних та профілювання фізичних осіб. Ці процеси несуть підвищені ризики для прав

суб’єктів персональних даних, зокрема в контексті прийняття автоматизованих рішень, що мають юридичні наслідки. Чинне законодавство України не передбачає жодного спеціального складу адміністративного правопорушення у цій сфері, що є суттєвим відставанням від стандартів GDPR, який присвячує цій проблематиці окремі статті та закріплює право суб’єкта на оскарження автоматизованих рішень [180].

Чинна система санкцій за ст. 188-39 КУпАП не передбачає жодної диференціації залежно від масштабу порушення, кількості постраждалих суб’єктів, категорії оброблюваних даних або наявності умислу. Порушення, що стосується обробки даних однієї особи, і порушення, що зачіпає масив даних мільйонів громадян, формально тягнуть однакові санкції. Це суперечить принципу пропорційності, закріпленому в ст. 83(1) GDPR як обов’язкова вимога до системи санкцій [180], та унеможливлює адекватну правову реакцію на порушення різного ступеня суспільної небезпечності.

Сукупність наведених прогалин свідчить про те, що система адміністративної відповідальності у сфері захисту персональних даних в Україні потребує не часткового вдосконалення, а системного реформування, яке має охоплювати як розширення переліку складів правопорушень, так і перегляд суб’єктного складу відповідальності, диференціацію санкцій і чітке розмежування адміністративної та кримінальної відповідальності.

Системні прогалини, встановлені нами раніше, зумовлюють необхідність не точкових змін до чинної ст. 188-39 КУпАП, а формування принципово нової системи складів адміністративних правопорушень і санкцій у сфері захисту персональних даних. О. Гіляка у дослідженні захисту персональних даних в умовах цифровізації обґрунтовує, що ефективний механізм правового захисту у цій сфері має поєднувати розширення охоронюваних правових відносин із відповідним санкційним інструментарієм, здатним забезпечити реальне дотримання вимог законодавства [19]. Розроблення такої системи має ґрунтуватися на трьох вихідних засадах:

– відповідності стандартам GDPR як обов'язкової умови виконання вимог євроінтеграційного процесу;

– дотримання принципів пропорційності та правової визначеності;

– реалістичності з точки зору адміністративного права України.

Чинна ст. 188-39 КУпАП охоплює лише три вузькі склади, жоден з яких не стосується порушень принципів обробки персональних даних або прав суб'єктів. М. Колотило у своєму дослідженні звертає увагу на те, що ефективна система відповідальності у цій сфері має охоплювати весь цикл обробки персональних даних від збирання до знищення з відповідним диференційованим реагуванням на порушення на кожному етапі [59]. З урахуванням цього підходу та стандартів GDPR [180] пропонується доповнити систему складів адміністративних правопорушень такими групами діянь:

– порушення принципів обробки персональних даних, включаючи обробку без законної підстави, з метою, відмінною від задекларованої, надмірне збирання даних та зберігання поза межами встановлених строків;

– порушення прав суб'єктів персональних даних, включаючи відмову у доступі до даних, ухилення від виправлення або знищення на вимогу суб'єкта;

– порушення у сфері безпеки обробки персональних даних, зокрема незабезпечення технічних і організаційних заходів захисту та неповідомлення про інцидент безпеки;

– порушення при автоматизованій обробці та профілюванні.

Щодо четвертої групи варто зауважити, що її запровадження є особливо актуальним з огляду на стрімке поширення систем автоматизованого прийняття рішень у публічному управлінні. Як зазначає Н. Головацький, запровадження алгоритмічної підзвітності та права на пояснення автоматизованих рішень є невід'ємним елементом гармонізації національного законодавства з GDPR та Законом України «Про адміністративну процедуру» [21]. К. Головко також наголошує на необхідності запровадження спеціальних складів правопорушень, пов'язаних з автоматизованою обробкою, з огляду на розширення відповідних практик у цифровому публічному управлінні [23].

Рух у напрямі розширення охоронюваних відносин вже розпочато на законодавчому рівні. 20 листопада 2024 року Верховна Рада України прийняла за основу в першому читанні законопроєкт № 8153 «Про захист персональних даних» [128], який суттєво розширює перелік правових відносин у цій сфері. Водночас Н. Семчук у своєму дослідженні гармонізації кримінального законодавства України зі стандартами ЄС справедливо зауважує, що законодавчі ініціативи у рамках законопроєкту № 8153 роблять великий акцент на збільшенні штрафів, однак не приділяють достатньої уваги системному вдосконаленню складів правопорушень, що обмежує їх ефективність [147]. Ця оцінка повною мірою стосується і адміністративно-правового виміру, оскільки без чіткого розширення переліку забороненої поведінки підвищення розміру санкцій не вирішує проблеми охоплення типових порушень.

Нова система санкцій має запровадити диференціацію за кількома критеріями. Принцип пропорційності є одним із базових принципів адміністративної відповідальності, який вимагає відповідності між тяжкістю правопорушення та суворістю санкції та проявляється як у площині балансування публічних і приватних інтересів, так і у площині обмеження певних прав для досягнення легітимної мети. І. Середа у дослідженні конституційно-правових обмежень та гарантій у сфері захисту персональних даних підкреслює, що принцип пропорційності є однією з ключових гарантій захисту персональних даних, який вимагає від держави забезпечення відповідності між обсягом втручання у право на захист даних та легітимною метою такого втручання, і це повною мірою стосується не лише обмежувальних заходів, а й системи санкцій [148]. Застосування цього принципу до системи санкцій за порушення законодавства про захист персональних даних означає необхідність диференціації залежно від: тяжкості порушення, менш суворі санкції за організаційно-технічні порушення та значно суворіші за прямі порушення прав суб’єктів або обробку чутливих категорій даних; масштабу порушення (кількість постраждалих суб’єктів і

обсяг порушених прав мають впливати на розмір санкції); суб'єктного складу (для юридичних осіб санкції мають розраховуватися у прив'язці до річного обороту за аналогією з GDPR); повторності (повторне вчинення аналогічного правопорушення протягом визначеного строку має передбачати суттєво вищі санкції).

Законопроєкт № 8153 у цьому відношенні є кроком вперед. Він передбачає встановлення штрафів для фізичних осіб в розмірі 30000-100000 грн. за випадок (до 20 млн. грн. загалом), для юридичних осіб 0,5-1% річного обороту (не менше 100000 грн, до 90 млн. грн. або 5% обороту) [128]. Такий підхід диференціації за суб'єктом та прив'язка до обороту для юридичних осіб є методологічно правильним, хоча й залишається значно меншим за аналогічні показники GDPR.

Р. Мигаль та ін. у дослідженні адміністративно-правового регулювання цифровізації адміністративних процедур зазначають, що саме юридичні особи є основними суб'єктами масової обробки персональних даних в умовах цифровізації, і будь-яка модель відповідальності, що виключає їх зі сфери санкцій, є апріорі неефективною [81]. Покладення відповідальності виключно на конкретну посадову особу не забезпечує системних змін у практиці обробки даних організацією і не створює організаційних стимулів до дотримання законодавства. Запровадження відповідальності юридичних осіб вимагає відповідного доповнення КУпАП щодо підстав і порядку накладення санкцій на організації, з визначенням критеріїв розміру штрафу залежно від їх фінансових показників.

Л. Гудзь у дослідженні права на приватність у контексті застосування штучного інтелекту обґрунтовує, що реформування системи відповідальності у сфері захисту персональних даних є неповним без запровадження механізмів судового контролю над автоматизованими рішеннями, права суб'єктів на доступ до пояснень таких рішень, а також системи санкцій за відповідні порушення [24]. Ці елементи мають стати невід'ємною частиною оновленої

системи адміністративної відповідальності поряд із процесуальними гарантіями для осіб, щодо яких застосовуються стягнення.

Реформування системи складів і санкцій не матиме практичного ефекту без одночасного вдосконалення процедурного механізму притягнення до відповідальності та інституційного забезпечення наглядової функції держави у цій сфері. Саме процедурний і інституційний виміри є тим вузьким місцем, яке перетворює навіть формально ефективні санкції на «мертві норми». Як свідчить аналіз щорічних доповідей Уповноваженого ВРУ з прав людини, чинна інституційна модель у вигляді покладення наглядових функцій у сфері захисту персональних даних на омбудсмана є структурно недостатньою для забезпечення ефективного правозастосування [161].

Відповідно до вимог Додаткового протоколу до Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних, ратифікованого Україною, кожна сторона зобов'язана створити незалежний контролюючий орган у сфері захисту персональних даних. Аналогічну вимогу містить і ст. 51 GDPR [180]. Чинна модель, за якої відповідні функції виконує Уповноважений ВРУ з прав людини паралельно з широким колом інших омбудсманських повноважень, не відповідає цій вимозі ні за обсягом ресурсного забезпечення, ні за структурою повноважень. О. Гіляка та А. Мерник у дослідженні правового регулювання та практики ЄСПЛ у сфері цифрових прав обґрунтовують, що ефективний захист персональних даних вимагає наявності спеціалізованого наглядового органу з реальними повноваженнями не лише щодо нагляду, а й щодо примусового виконання вимог законодавства, включаючи самостійне накладення фінансових санкцій [20].

Реакцією законодавця на вимоги норм міжнародних нормативно правових актів стало розробка законопроекту про створення колегіального незалежного органу зі спеціальним статусом, структурою та повноваженнями. Відповідно до законопроєкту № 6177 від 18.10.2021 таким органом повинна стати Національна комісія з питань захисту персональних даних та доступу до

публічної інформації [129]. Законопроєкт передбачає, що Комісія матиме право приймати обов'язкові для виконання рішення про запобігання та усунення порушень, а також накладати штрафи на суб'єктів контролю. При цьому рішення Комісії є виконавчими документами, що підлягають примусовому виконанню [129]. Водночас питання матеріальної відповідальності юридичних осіб як самостійних суб'єктів у цій сфері врегульовується не законопроєктом № 6177, а законопроєктом № 8153, який запроваджує фінансові санкції для контролерів та операторів персональних даних залежно від їх річного обороту [128]. Отже, два законопроєкти вирішують різні, але взаємодоповнюючі завдання: № 6177 інституційне (хто і в якому порядку накладає санкції), № 8153 матеріальне (за що і в якому розмірі). Така модель відповідає досвіду держав-членів ЄС, де наглядові органи у сфері захисту персональних даних є самостійними регуляторами з власними повноваженнями щодо накладення штрафів на юридичних осіб.

Чинний механізм, за якого Уповноважений складає протокол і передає справу до суду, є процедурно перевантаженим і унеможливлює оперативне реагування на порушення. М. Колотило звертає увагу на те, що ефективність наглядового органу у сфері захисту персональних даних прямо залежить від наявності у нього повноважень щодо самостійного накладення фінансових санкцій без обов'язкового залучення суду [59]. Це підтверджується і позицією самого Уповноваженого ВРУ з прав людини, який у щорічній доповіді за 2024 рік констатує необхідність надання йому аналогічних повноважень [161]. Більш детально про особливості наглядового органу у сфері захисту персональних даних описано нами у праці [66].

Пропонована модель має передбачати дворівневу систему оскарження. На першому рівні визначається право суб'єкта звернутися до Комісії з вимогою про перегляд прийнятого рішення у встановлені строки, на другому у випадку непогодження з результатом першого оскарження рішення Комісії в адміністративному судочинстві з відповідним розподілом тягаря доказування між сторонами. При цьому О. Гіляка та А. Мерник наголошують,

що право на ефективний судовий засіб правового захисту проти наглядового органу є невід'ємною гарантією, закріпленою у практиці як ЄСПЛ, так і Суду ЄС, і його забезпечення є обов'язковою умовою легітимності системи адміністративних санкцій у сфері захисту персональних даних [20].

Чинна процедура притягнення до адміністративної відповідальності, що регулюється КУпАП, розроблялась без урахування специфіки правопорушень у цифровому середовищі, що суттєво ускладнює її практичне застосування у сфері захисту персональних даних. З огляду на це пропонуємо доповнити процедурний механізм кількома взаємопов'язаними елементами. Насамперед необхідно закріпити особливий порядок збирання та фіксації цифрових доказів, зокрема щодо отримання та збереження даних про обробку, електронних журналів і метаданих з метою забезпечення їх допустимості у провадженні про адміністративне правопорушення. Для типових і очевидних порушень, де факт правопорушення не вимагає складного доказування, доцільно запровадити скорочені строки розгляду справ, а для менш серйозних порушень спрощене провадження, за яким добровільне визнання порушення та його усунення є підставою для застосування мінімальної санкції без повноцінного розгляду. Окремого врегулювання потребує питання строків давності, так як чинні строки не враховують того, що порушення у сфері захисту персональних даних можуть бути тривалими або прихованими і виявлятися значно пізніше від моменту їх вчинення.

Ще одним важливим аспектом є те, що реформування механізму адміністративної відповідальності не має обмежуватися лише каральним виміром. Н. Семчук обґрунтовує, що ефективна система захисту персональних даних потребує поєднання реальних санкцій із превентивними механізмами, тобто обов'язковими оцінками впливу на захист даних для масштабних проєктів обробки, консультативними функціями наглядового органу та системою добровільного дотримання вимог [147]. Уповноважений ВРУ з прав людини у 2024 році провів 41 просвітницький захід та видав 490 публікацій і роз'яснень [161], що свідчить про розуміння важливості превентивного

виміру, але водночас унаочнює диспропорцію між просвітницькою діяльністю та реальним правозастосуванням. Новий спеціалізований орган має поєднувати обидва виміри, і каральний, і превентивний у збалансованому форматі.

Ефективність механізму адміністративної відповідальності у сфері захисту персональних даних залежить також від налагодженої взаємодії між наглядовим органом, правоохоронними органами та судами. Р. Мигаль та ін. звертають увагу на те, що цифровізація адміністративних процедур вимагає системного підходу до координації між різними суб'єктами публічного управління у питаннях, що стосуються обробки персональних даних [81]. Це передбачає, зокрема, чіткий розподіл повноважень між Комісією та правоохоронними органами у разі виявлення ознак кримінального правопорушення, механізм передачі матеріалів між органами, а також інформаційний обмін щодо виявлених порушень.

Сукупність наведених пропозицій утворює цілісну концепцію реформування механізму адміністративної відповідальності у сфері захисту персональних даних, що охоплює три взаємопов'язані виміри. Нормативний полягає у розширенні складів і диференціації санкцій, інституційний передбачає створення спеціалізованого незалежного наглядового органу з реальними повноваженнями. Суть процедурного у адаптації провадження до специфіки цифрового середовища з одночасним забезпеченням процесуальних гарантій.

3.2. Оптимізація публічного управління у сфері забезпечення захисту персональних даних під час надання електронних публічних послуг

Практика надання електронних публічних послуг через платформу «Дія» сформувала правову ситуацію, яка не має однозначного вирішення в рамках чинного законодавства про захист персональних даних. У процесі

отримання конкретної послуги громадянин взаємодіє одночасно з двома суб'єктами (платформою як технічним посередником і відповідним органом публічної влади як надавачем послуги), однак законодавство не визначає чітко, хто з них є контролером персональних даних, хто оператором, і яким чином між ними розподіляється відповідальність у разі порушення прав суб'єкта. Нерозв'язаність цього питання є системною прогалиною, що безпосередньо впливає на здатність суб'єктів персональних даних реалізувати свої права у найбільш поширеному сценарії взаємодії з публічною адміністрацією.

Згідно з офіційним повідомленням Міністерства цифрової трансформації України про обробку персональних даних, Міністерство визначене як «володілець» даних, що обробляються через Портал Дія, тоді як органи влади, послуги яких надаються через платформу, є третіми особами, яким дані передаються у процесі надання відповідних послуг [94]. Таке формулювання створює правову невизначеність, яка полягає в тому, що Міністерство фактично виконує роль контролера на технічному рівні обробки, тоді як орган-надавач послуги самостійно визначає мету і підстави обробки конкретних персональних даних у межах своїх повноважень. Обидва суб'єкти водночас впливають на мету та засоби обробки, що за критеріями ст. 26 GDPR кваліфікується як спільне контролерство, яке передбачає обов'язкове укладення відповідної угоди між спільними контролерами з чітким розподілом обов'язків і забезпеченням її доступності для суб'єктів даних [180]. Закон № 2297-VI такої конструкції не передбачає, а оперує лише поняттями «володілець» і «розпорядник» [118], що робить неможливим правове врегулювання відносин між платформою і органами-надавачами в умовах агрегованої моделі надання послуг. О. Яворська у дослідженні захисту персональних даних у цифровому середовищі за досвідом ЄС зазначає, що розмитість відповідальності між кількома суб'єктами обробки є однією з ключових системних проблем, з якою зіткнулася практика застосування GDPR в державному секторі, і що її усунення можливе лише шляхом законодавчого

закріплення конструкції спільного контролерства з конкретним розподілом обов'язків між учасниками [163].

Більш детально особливості правового статусу платформи «Дія» охарактеризовано автором цього дослідження в окремій науковій праці [69].

Описана невизначеність має безпосередні практичні наслідки для можливості захисту прав. Якщо персональні дані громадянина, отримані через «Дію» при зверненні за певною послугою, були використані з метою, відмінною від задекларованої, або стали доступними третім особам, незрозуміло, до кого суб'єкт персональних даних має звертатись із вимогою. Відповідальність Міністерства як «володільця» платформи стосується технічного рівня обробки, а відповідальність органу-надавача змісту і правомірності обробки в межах його повноважень. Відсутність нормативно закріпленого розподілу між ними перетворює суб'єкта даних на особу, яка формально має право вимоги, але практично позбавлена чіткого адресата цієї вимоги. Це суперечить принципу підзвітності, закріпленому у ст. 5(2) GDPR, відповідно до якого контролер несе відповідальність і повинен бути здатним продемонструвати дотримання принципів обробки персональних даних [180]. За відсутності чіткого визначення того, хто є контролером у конкретній ситуації, реалізація принципу підзвітності стає неможливою.

Окремим виміром є питання повноти інформування суб'єктів персональних даних. Повідомлення Міністерства цифрової трансформації не містить вичерпного переліку органів третіх осіб, яким передаються дані при наданні конкретних послуг [94]. Суб'єкт може ознайомитись із загальним описом мети обробки, але не з конкретним переліком отримувачів у кожному окремому випадку. Це не відповідає стандартам ст. 13 GDPR, яка вимагає надання суб'єкту даних конкретної інформації про отримувачів або категорії отримувачів персональних даних на момент їх збирання [180]. М. Пальчик, К. Шкрібляк та Ю. Березецький у дослідженні захисту персональних даних як напряму забезпечення національної безпеки наголошують, що витік відомостей із державних баз даних підриває довіру громадян до управлінських

інституцій, а одним із чинників такої недовіри є саме непрозорість щодо того, які суб’єкти і в якому обсязі мають доступ до персональних даних, переданих через державні платформи [89]. Ця ситуація унаочнюється реальними інцидентами. Публічні суперечки між Нотаріальною палатою України, Міністерством цифрової трансформації та Міністерством юстиції щодо витоку реальних даних із державних реєстрів під час тестування системи е-нотаріату, а також неодноразові повідомлення про можливий несанкціонований доступ до даних через «Дію» так і не отримали однозначного правового вирішення питання відповідальності, так як кожен із задіяних органів влади заперечував свою причетність, тоді як норма закону, яка б визначала відповідального суб’єкта, відсутня [44].

Отож, чинний правовий режим обробки персональних даних через платформу «Дія» характеризується відсутністю законодавчого регулювання конструкції спільного контролерства, невизначеністю розподілу відповідальності між платформою і органами-надавачами та недостатньою прозорістю інформування суб’єктів даних. Усунення цих проблем є необхідною передумовою для ефективного захисту прав суб’єктів персональних даних у системах електронних публічних послуг та для відповідності українського законодавства стандартам GDPR в частині підзвітності та прозорості обробки.

Система «Трембіта» функціонує на основі Постанови Кабінету Міністрів України від 8 вересня 2016 року № 606 «Деякі питання електронної взаємодії державних електронних інформаційних ресурсів» та є децентралізованою платформою, де кожен учасник встановлює власні компоненти і обмінюється даними напряму з іншими учасниками без проходження через проміжні вузли [28]. Станом 2024 рік до «Трембіти» підключено 229 органів державної влади, місцевого самоврядування та суб’єктів господарювання і 125 реєстрів, а щоденна кількість транзакцій сягає 15 мільйонів [139]. Ця архітектура визначає і ключову правову проблему, яка полягає у тому, що при децентралізованому обміні між 229 учасниками і 125

реєстрами питання про те, хто несе відповідальність за конкретний неправомірний обмін даними і на підставі яких правових критеріїв такий обмін відбувається, не має нормативної відповіді.

Тримачем системи «Трембіта» є Міністерство цифрової трансформації України, адміністратором державне підприємство «Дія», тоді як учасниками є власне органи-держателі реєстрів [149]. У такій конфігурації відповідальність розподілена між трьома рівнями суб'єктів, і жоден із них не несе чіткої відповідальності за конкретний акт неправомірного міжвідомчого обміну. Тримач відповідає за функціонування системи в цілому, адміністратор за технічне адміністрування, а орган-учасник за власний шлюз безпечного обміну та зміст своїх запитів. Чинне законодавство не містить норм, які б визначали, до кого суб'єкт персональних даних має звертатись із вимогою у разі, якщо неправомірний обмін здійснено одним органом через систему, адміністровану іншим суб'єктом за загальним наглядом третього. Ця прогалина є структурним аналогом проблеми, описаної вище щодо платформи «Дія», але у значно більших масштабах, оскільки «Трембіта» об'єднує не одну платформу і кілька органів, а сотні учасників.

Нормативна база «Трембіти» деталізує технічні вимоги до підключення, шифрування, ідентифікації учасників та протоколювання подій [28], але не встановлює правових критеріїв, яким має відповідати конкретний запит до реєстру з точки зору законності обробки персональних даних. Рішення про те, чи є конкретний запит правомірним, фактично приймається самим органом, що його здійснює. При цьому відсутній будь-який механізм попереднього контролю правомірності запиту з боку тримача або адміністратора системи. Підсистема моніторингу, запроваджена у 2023 році [130], фіксує факт доступу після його здійснення і дозволяє суб'єкту даних отримати сповіщення через «Дію», але не є механізмом попереднього контролю, оскільки вона виявляє можливе порушення, а не запобігає йому.

Для порівняння, естонська платформа X-Road, на основі якої створено «Трембіту», функціонує в правовому середовищі, де кожен запит до реєстру

здійснюється на підставі чіткого законодавчого повноваження відповідного органу, а наглядовий орган із захисту персональних даних має реальні механізми перевірки правомірності кожного типу обміну ще на стадії підключення нового сервісу до системи. В Україні аналогічний механізм попереднього правового контролю відсутній.

Окремою напрямком є розширення кола учасників системи на суб'єктів господарювання приватних компаній, що закріплено у новій редакції Положення про систему «Трембіта», затвердженій постановою Кабінету Міністрів України від 17.01.2023 № 38 [106]. Якщо доступ органів публічної влади до персональних даних через «Трембіту» принаймні формально обґрунтований виконанням ними законних повноважень, то для приватних суб'єктів правова підстава є значно менш визначеною. Закон України «Про захист персональних даних» вимагає наявності законної підстави для будь-якої обробки персональних даних [118], однак нормативна база «Трембіти» не встановлює спеціальних критеріїв для оцінки правомірності участі приватних суб'єктів у конкретних обмінах реєстровими даними, що є прогалиною, яка потребує усунення.

«Трембіта» функціонує за принципом передачі даних у момент запиту, тобто дані не зберігаються в самій системі, а лише транзитно передаються між реєстрами. Ця архітектура, яка позиціонується як перевага з точки зору безпеки, водночас породжує правову проблему. Оскільки транзакція є миттєвою і не залишає слідів у централізованому сховищі, суб'єкт персональних даних, який бажає отримати інформацію про те, які органи мали доступ до його даних і з якою метою, технічно може отримати таку інформацію лише через підсистему моніторингу [130] якщо вона підключена до конкретного реєстру. Право суб'єкта персональних даних знати про осіб, яким передаються його дані, закріплене у ст. 8 Закону № 2297-VI [118], але механізм його реалізації у контексті системи «Трембіта» залишається функціонально неповним.

Введення воєнного стану в Україні 24 лютого 2022 року суттєво змінило правовий режим обробки персональних даних. Цей вимір проблеми є специфічним в контексті інституційної неефективності, оскільки йдеться не про прогалини у законодавстві в умовах мирного часу, а про свідоме обмеження гарантій захисту персональних даних, здійснене в умовах збройного конфлікту, і про те, чи відповідають ці обмеження вимогам пропорційності та необхідності, що висуваються міжнародними стандартами.

Конституція України у ст. 32 гарантує право на захист персональних даних, однак ст. 64 допускає тимчасове обмеження конституційних прав в умовах воєнного або надзвичайного стану. Закон України «Про правовий режим воєнного стану» наділяє відповідних суб'єктів (органи військового командування, військові адміністрації) широкими повноваженнями, необхідними для протидії збройної агресії, без вичерпного переліку допустимих форм обмеження прав суб'єктів персональних даних. З іншої сторони, Закон України «Про захист персональних даних» не містить окремих норм про правовий режим обробки персональних даних в умовах воєнного стану, а спеціального режиму захисту персональних даних під час надзвичайних обставин, на відміну від ряду держав ЄС, в Україні офіційно не запроваджено [89]. Я. Худолєй та Н. Загребельна зазначають, що така нормативна невизначеність породжує ситуацію, коли органи влади діють у «сірій зоні», спираючись на загальні повноваження воєнного стану без чіткої правової підстави для конкретних обмежень прав суб'єктів персональних даних [157].

Найбільш показовим прикладом розширення обробки персональних даних в умовах воєнного стану є запровадження реєстру військовозобов'язаних «Оберіг» та послідовне розширення переліку даних, що до нього включаються. Реєстр був введений в експлуатацію у 2022 році і поступово наповнювався персональними даними громадян включно з медичними даними, даними про місце проживання, трудовий статус та освіту. Законом України «Про внесення змін до деяких законів України щодо

удосконалення порядку обробки та використання даних у державних реєстрах для військового обліку» [103] у 2024 році коло даних та суб'єктів доступу до реєстру було суттєво розширено. При цьому, як зазначають дослідники Центру демократії та верховенства права, ці зміни лише частково враховують принципи пропорційності та мінімізації даних, а механізми захисту прав осіб, внесених до реєстру, залишаються недостатньо деталізованими [17].

Міжнародні стандарти захисту персональних даних, зокрема Конвенція Ради Європи № 108+ та GDPR, допускають обмеження права на захист персональних даних в інтересах національної безпеки, але лише за умови дотримання критеріїв законності, необхідності та пропорційності. Стаття 11 Конвенції № 108+ прямо передбачає, що обмеження права на захист персональних даних повинні бути передбачені законом, необхідними у демократичному суспільстві та пропорційними до законної мети. І. Середа констатує, що право на захист персональних даних, закріплене у ст. 32 Конституції України, є невід'ємною складовою права на приватність, а тому будь-які обмеження цього права в умовах воєнного стану мають ґрунтуватися на чітких правових підставах, відповідати принципам законності, пропорційності та необхідності, підлягати судовому контролю і бути прозорими для суб'єктів даних [148]. В. Світличний окремо наголошує, що в умовах воєнного стану в Україні обмеження у сфері захисту персональних даних нерідко запроваджуються підзаконними актами без достатнього законодавчого підґрунтя, що суперечить принципу законності [146].

Окремою правовою проблемою є відсутність нормативно закріпленого механізму відновлення гарантій захисту персональних даних після припинення воєнного стану. Персональні дані, зібрані в умовах воєнного стану на ширших правових підставах, не підлягають автоматичному знищенню або обмеженню в обробці після закінчення дії особливого правового режиму, оскільки відповідні норми у чинному законодавстві відсутні. В. Кірієнко зазначає, що захист персональних даних в умовах збройного конфлікту має розглядатися не лише як елемент правового захисту особи, а й як компонент

національної безпеки, адже масиви персональних даних, зібрані в умовах збройного конфлікту, становлять потенційну мішень для ворожих кібератак і можуть бути використані проти самих суб'єктів цих даних [49]. Ця обставина свідчить про те, що послаблення гарантій захисту персональних даних в умовах воєнного стану може суперечити не лише правам особи, а й самим безпековим інтересам держави, заради яких ці гарантії послаблювались.

Раніше нами було виявлено конкретні правові проблеми окремих платформ і систем. Спільним більшості з них є те, що ці проблеми виникли не внаслідок умисних порушень, а внаслідок відсутності правових механізмів, які б змусили розробників публічних цифрових сервісів завчасно враховувати вимоги захисту персональних даних на етапі проектування та до моменту запуску. Саме цю функцію у праві ЄС виконують два взаємопов'язані інструменти – принцип privacy by design і обов'язкова оцінка впливу на захист даних (DPIA). Разом з тим, жоден з яких не знайшов належного відображення в українському законодавстві.

Принцип privacy by design, закріплений у ст. 25 GDPR, зобов'язує контролера впроваджувати технічні та організаційні заходи захисту персональних даних ще на етапі розроблення продукту або системи, а не після її запуску [180]. Такий підхід передбачає, що захист приватності є вихідною умовою проектування, а не наступним додатковим кроком. В. Рядінська та Т. Плугатар у дослідженні правового регулювання цифровізації публічного управління в ЄС констатують, що саме вимога privacy by design є одним із ключових стандартів, яким зобов'язані відповідати органи публічної адміністрації при розробці та впровадженні цифрових сервісів, і що її відсутність у національному законодавстві є суттєвою перешкодою для визнання відповідного рівня захисту даних [143].

Чинний Закон № 2297-VI не містить жодної норми, яка б відтворювала цей принцип [118]. Законопроєкт № 8153, прийнятий у першому читанні, передбачає запровадження вимоги «захисту даних за проектуванням та за замовчуванням» [128]. На практиці це означає, що жоден із ключових

публічних цифрових сервісів («Дія», «Трембіта» чи «Оберіг») не зобов'язаний був проходити верифіковану оцінку відповідності принципам privacy by design перед введенням в експлуатацію. Правові проблеми, виявлені нами раніше (невизначеність розподілу відповідальності між «Дією» та органами-надавачами, відсутність правових критеріїв допустимості запиту у «Трембіті»), значною мірою є наслідком саме відсутності цього превентивного правового інструменту.

Відповідно до ст. 35 GDPR, контролер зобов'язаний провести оцінку впливу на захист персональних даних (DPIA) до початку обробки, якщо вона може призвести до високого ризику порушення прав і свобод фізичних осіб [180]. Обов'язок проведення DPIA виникає, зокрема, у разі масштабної систематичної обробки персональних даних, масштабного використання спеціальних категорій даних, систематичного моніторингу фізичних осіб, а також у разі впровадження нових технологій, тобто саме в тих випадках, що є типовими для публічних цифрових платформ в Україні. Усі три аналізовані в цьому підрозділі системи («Дія», «Трембіта» і «Оберіг») підпадають під ці критерії.

Закон № 2297-VI не містить вимоги проведення DPIA ні для публічного, ні для приватного сектору [118]. Фактично рішення про запуск державного цифрового сервісу в Україні приймається без будь-якої формалізованої оцінки ризиків для прав суб'єктів персональних даних, що принципово відрізняє українську практику від стандартів ЄС. О. Яворська зазначає, що в державах-членах ЄС DPIA є не формальним актом бюрократичної відповідності, а реальним правовим механізмом, що дозволяє виявити ризики і усунути їх до моменту, коли вони стануть фактичними порушеннями прав мільйонів суб'єктів [163]. Відсутність аналогічного обов'язку в Україні означає, що держава фактично запускає масштабні цифрові системи обробки персональних даних «наосліп» з точки зору захисту прав суб'єктів.

Поєднання відсутності privacy by design і DPIA породжує ситуацію, за якої правові проблеми публічних цифрових сервісів виявляються лише після

їх запуску, а саме на етапі, коли системи вже функціонують, громадяни вже передали свої дані, а виправлення архітектурних і правових недоліків потребує значно більших зусиль і ресурсів. Саме це й демонструє досвід платформи «Дія» та системи «Трембіта». Проблеми розподілу відповідальності, відсутність правових критеріїв допустимості запиту, неповнота механізмів реалізації прав суб'єктів є наслідком рішень, прийнятих на етапі проектування без правових вимог щодо захисту персональних даних.

Правові проблеми сформульовані у цьому підрозділі утворюють взаємопов'язану систему прогалин, що потребує комплексного законодавчого вирішення. Йдеться не про ізольовані технічні недоліки окремих платформ, а про системну невідповідність правового регулювання цифрових публічних послуг стандартам захисту персональних даних, що витікають із Угоди про асоціацію з ЄС і є умовою набуття Україною статусу держави з достатнім рівнем захисту даних. Сформулюємо окремі напрямки покращень, структуровані відповідно до виявлених проблем і спрямовані на їх усунення у рамках завершення роботи над законопроєктом № 8153.

Законопроєкт № 8153 у ст. 30 містить норму про спільне контролерство, яка визначає обов'язок укладення договору про розподіл обов'язків та гарантує суб'єкту право реалізовувати свої права щодо кожного з контролерів [128]. Водночас, на відміну від ст. 26 GDPR [180], ця стаття не передбачає солідарної відповідальності спільних контролерів перед суб'єктом персональних даних. Пропонуємо доповнити ст. 30 законопроєкту окремою частиною про солідарну відповідальність спільних контролерів за шкоду, заподіяну суб'єкту внаслідок порушення вимог обробки, із правом зворотної вимоги між ними відповідно до договору про розподіл обов'язків. Без цього нормативного елемента правовий режим платформи «Дія» залишатиметься юридично невизначеним незалежно від того, які інші вдосконалення будуть внесені до законодавства.

Чинна нормативна база «Трембіти» регулює технічні аспекти підключення та обміну, але не встановлює правових критеріїв для оцінки

правомірності конкретного запиту з точки зору захисту персональних даних. Пропонуємо доповнити постанову Кабінету Міністрів України від 08.09.2016 № 606 окремим розділом про правові засади обробки персональних даних у системі «Трембіта», що має визначати: обов'язковість наявності законної правової підстави для кожного типу обміну персональними даними; вимогу документування мети кожного типу запиту і відповідності цієї мети первісній меті збирання даних у відповідному реєстрі; критерії правомірності участі суб'єктів господарювання як учасників системи стосовно доступу до персональних даних; обов'язкове підключення підсистеми моніторингу для всіх учасників системи без винятку. Без таких критеріїв формальна наявність у законодавстві принципів мінімізації та цільового обмеження залишається декларативною і не забезпечує реального захисту прав суб'єктів у системах масштабного міжвідомчого обміну.

Досвід воєнного стану продемонстрував, що розширення обробки персональних даних в умовах збройного конфлікту відбувається за відсутності чіткої правової рамки, яка б встановлювала допустимі межі та гарантії. Пропонуємо внести до законопроєкту № 8153 окрему статтю «Обробка персональних даних в умовах воєнного або надзвичайного стану» у такій редакції:

1. В умовах воєнного або надзвичайного стану, введеного відповідно до Конституції України та законів України, органи державної влади та органи місцевого самоврядування можуть здійснювати обробку персональних даних на підставах і в обсязі, необхідних для відсічі збройної агресії, забезпечення оборони держави, громадської безпеки та захисту критичної інфраструктури, з дотриманням вимог цього Закону, якщо інше не встановлено законом.

2. Обмеження прав суб'єктів персональних даних, передбачених цим Законом, в умовах надзвичайних обставин допускається лише якщо воно: передбачене законом; є необхідним у демократичному суспільстві; є пропорційним законній меті, яку переслідує; обмежене у часі строком дії відповідного правового режиму.

3. Органи, що здійснюють обробку персональних даних на підставі частини першої цієї статті, зобов’язані документувати правову підставу, мету та обсяг кожного виду такої обробки. Зазначена документація підлягає перевірці уповноваженим органом з питань захисту персональних даних.

4. Після припинення дії воєнного або надзвичайного стану органи, що здійснювали обробку персональних даних, зобов’язані у строк, що не перевищує шести місяців здійснити перегляд необхідності подальшої обробки кожної категорії персональних даних, зібраних на розширених правових підставах та знищити або деідентифікувати персональні дані, правова підстава для обробки яких відпала.

5. Повний обсяг прав суб’єктів персональних даних, передбачених цим Законом, відновлюється з моменту припинення дії воєнного або надзвичайного стану, якщо інше не встановлено законом.

Законопроєкт № 8153 у нинішній редакції передбачає вимогу захисту даних за проектуванням та за замовчуванням, однак не деталізує спеціальних вимог для публічного сектору і не встановлює обов’язковості DPIA для державних платформ. Пропонуємо при доопрацюванні законопроєкту до другого читання доповнити його нормами, що визначають:

– обов’язковість проведення DPIA перед запуском будь-якого публічного цифрового сервісу, що здійснює масштабну систематичну обробку персональних даних за аналогією зі ст. 35 GDPR;

– обов’язковість публічного оприлюднення результатів DPIA для загальнодержавних платформ;

– участь незалежного наглядового органу у верифікації DPIA для платформ, що обробляють дані понад одного мільйона суб’єктів;

– вимогу підтвердження відповідності принципам privacy by design як умову введення в експлуатацію нових державних інформаційних систем, що обробляють персональні дані. Ці механізми є ключовими елементами, завдяки яким держави-члени ЄС забезпечують відповідність своїх цифрових

публічних сервісів стандартам GDPR, і без їх запровадження формальна гармонізація законодавства не матиме практичного ефекту.

Наведені пропозиції є взаємодоповнюючими і спрямовані на формування цілісної системи правового регулювання, за якої захист персональних даних у системах електронних публічних послуг забезпечується не лише через ретроспективні механізми відповідальності, а передусім через превентивні правові інструменти, вбудовані в процес розроблення, запуску та функціонування публічних цифрових сервісів.

3.3. Гармонізація адміністративно-правового забезпечення захисту персональних даних в Україні з правом Європейського Союзу: пріоритети та механізми реалізації

Аналіз, здійснений у попередніх питаннях цього розділу, мав переважно критичний характер. Були виявлені конкретні правові прогалини в системі адміністративної відповідальності за порушення у сфері захисту персональних даних, у правовому режимі електронних публічних сервісів та у механізмах превентивного захисту і сформульовані конкретні пропозиції щодо їх усунення шляхом доопрацювання законопроєкту № 8153 та суміжних актів. Разом з тим, дані пропозиції є частиною більш широкого і системного завдання, яке стоїть перед Україною, яке полягає у тому, щоб не просто усунути окремі недоліки чинного законодавства, а здійснити повноцінну гармонізацію національного законодавства у сфері захисту персональних даних із правом ЄС у рамках процесу вступу до Союзу. Вирішення ситуації про те, що саме і в якій послідовності має бути зроблено, ґрунтується не на академічних рекомендаціях, а на конкретних правових зобов'язаннях України.

Зобов'язання України щодо гармонізації законодавства у сфері захисту персональних даних мають кількарівневу правову природу. Базовим є зобов'язання, закріплене у ст. 15 Угоди про асоціацію між Україною та ЄС,

ратифікованої Законом України від 16.09.2014 № 1678-VII. Відповідно до Угоди сторони «домовились співробітничати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема відповідних документів Ради Європи. Співробітництво у сфері захисту персональних даних може включати, inter alia, обмін інформацією та експертами» [154]. Формулювання «найвищі європейські та міжнародні стандарти» охоплює насамперед два документи Конвенцію Ради Європи № 108+ та GDPR, що прямо підтверджується висновком Ради Європи щодо законопроєкту № 8153 [98].

Зазначені документи не є обов'язковими для України, однак отримання Україною статусу кандидата на членство в ЄС у червні 2022 року і офіційне відкриття переговорів про вступ у червні 2024 року суттєво трансформували правову природу впливу цих документів. Відповідно до переговорної рамки, прийнятої у червні 2024 року, захист персональних даних охоплює кілька переговорних розділів. Право на захист персональних даних як основоположне право розглядається в рамках глави 23 «Судова влада та основоположні права» (Кластер 1 «Основи процесу вступу до ЄС»), тоді як повноцінна гармонізація матеріального права у сфері захисту даних відповідно до GDPR є предметом глави 10 «Цифрова трансформація та медіа» (Кластер 3 «Конкурентоспроможність та інклюзивний розвиток»), а захист персональних даних у правоохоронній сфері розглядається у главі 24 «Юстиція, свобода та безпека». Ця розподіленість між кластерами є важливою з практичної точки зору: прогрес у Кластері 1 умовлює відкриття наступних кластерів, і недостатній рівень захисту персональних даних як основоположного права може стати перешкодою для просування переговорів в цілому. [90]. Завершення процесу скринінгу у вересні 2025 року означає перехід від діагностичної до переговорної фази, в рамках якої Україна має демонструвати не лише намір адаптувати законодавство, а вже вжиті конкретні заходи [90].

Важливим також є поняття «адекватний рівень захисту», або adequacy за критеріями ст. 45 GDPR. Отримання рішення Єврокомісії про адекватність є умовою вільного транскордонного потоку персональних даних між Україною та державами-членами ЄС і розглядається як один із практичних показників реальної, а не лише формальної гармонізації. Для отримання такого статусу недостатньо формальної наявності законодавства, необхідним є функціонування незалежного наглядового органу, здатного реально забезпечувати виконання закону, а також наявність механізмів захисту прав суб'єктів даних, ефективних на практиці, а не лише задекларованих. Саме цей критерій визначає реальну ефективність, а не формальну відповідність тексту і відрізняє гармонізацію як юридичний процес від гармонізації як законотворчої техніки.

О. Яворська у дослідженні захисту персональних даних у цифровому середовищі підкреслює, що досвід держав, які проходили процес отримання рішення про адекватність, а саме Японії, Південної Кореї, Великої Британії після Brexit, зазначає, що Єврокомісія оцінює не лише текст законів, а й практику правозастосування, незалежність наглядового органу, наявність судового контролю і реальні механізми відшкодування шкоди суб'єктам даних [163]. Жоден з цих елементів не може бути забезпечений одним лише прийняттям нового закону, оскільки кожен вимагає системних інституційних і процедурних змін, частина яких виходить за межі законопроєкту № 8153.

Для повноцінного розгляду механізму гармонізації, необхідно зрозуміти принципову методологічну особливість, яка визначає специфіку адаптації законодавства у сфері захисту персональних даних порівняно з іншими сферами acquis. Ця особливість пов'язана з юридичною природою GDPR як регламенту ЄС на відміну від директиви.

У праві ЄС регламент має пряму дію і не потребує транспозиції в національне законодавство держав-членів, оскільки він застосовується безпосередньо. Директива натомість є обов'язковою щодо результату, але залишає державам-членам свободу вибору форми і методів досягнення цього

результату. Для країни-кандидата, яка ще не є державою-членом, різниця набуває принципового значення. GDPR як регламент не діє в Україні безпосередньо, тому Україна зобов'язана не стільки застосовувати його, як відтворити його зміст у власному законодавстві. Як зазначає Н. Расторгуєва у дослідженні інституційних засад адаптації acquis в Україні, саме у сфері регламентів виникає найбільш делікатна правова ситуація, яка полягає в тому, що держава-кандидат ухвалює закон, який відтворює зміст регламенту. Але цей закон є тимчасовим, оскільки після вступу до ЄС він має втратити чинність, так як регламент починає діяти безпосередньо [131]. Це означає, що зусилля з гармонізації законодавства у цій частині мають двоїстий характер: вони є необхідними для переговорного процесу, але водночас є тимчасовим рішенням, яке після вступу має бути замінено прямою дією GDPR.

Ця методологічна особливість породжує практичний ризик, який у науковій літературі отримав назву формальної гармонізації. Зміст ризику полягає у тому, що ухвалення закону, текст якого відтворює acquis, не гарантує одночасного забезпечення інституційних і процедурних умов, необхідних для його реального застосування. Стосовно законопроєкту № 8153 цей ризик є цілком конкретним. Аналіз законопроєкту, проведений у 2024 році, фіксує ситуацію, яку можна охарактеризувати як «копіювання GDPR», тобто відтворення термінології, визначень, прав і обов'язків регламенту без достатнього врахування інституційних реалій України і без одночасного створення механізму, що забезпечить реальне виконання цих норм [7]. Іншими словами, текст закону може повністю відповідати acquis, але право залишатиметься декларативним, якщо відсутні: незалежний наглядовий орган із реальними повноваженнями і ресурсами; процедури отримання, розгляду і виконання рішень за скаргами суб'єктів даних; правозастосовна практика, що підтверджує дієвість санкцій. Хоча термін «копіювання» є спрощенням, він точно відображає суть проблеми, яка полягає у тому, що між формальним відтворенням тексту acquis і його реальною імплементацією існує принциповий розрив.

Такий розрив не є суто українською проблемою, він виникав у процесі вступу ряду держав, що приєднувалась до ЄС. Досвід країн Центральної і Східної Європи, які вступали у 2004 і 2007 роках, свідчить, що саме у сфері захисту персональних даних формальна відповідність законодавства і реальна ефективність його застосування розходились найбільше і найдовше. Польща, Угорщина, Румунія і Болгарія ухвалили відповідне законодавство ще до вступу, проте наглядові органи з питань захисту даних у цих країнах набули реальної операційної спроможності лише через кілька років після вступу. Як констатує у своєму дослідженні К. Гуртова, існування політичної волі і нормативної бази є необхідною, але не достатньою умовою ефективної адаптації, необхідна глибша імплементація, інституційна стійкість та контроль за виконанням адаптованих положень [25].

Для України цей виклик є особливо гострим з двох причин. По-перше, GDPR є значно складнішим і деталізованішим актом, ніж Директива 95/46/ЄС, яку імплементували держави першої хвилі розширення. По-друге, Україна адаптує законодавство в умовах воєнного стану, що суттєво обмежує інституційну спроможність і уповільнює формування правозастосовної практики. Ці чинники разом означають, що Україна має реалістично оцінювати не лише те, чи відповідає текст законопроєкту № 8153 тексту GDPR, а й те, чи буде цей закон реально застосовуватись після його прийняття, і яких інституційних передумов для цього бракує.

Зосередженість наукового і публічного дискурсу щодо реформи законодавства України у сфері захисту персональних даних майже виключно на GDPR і законопроєкті № 8153 створює хибне враження, що гармонізація у цій сфері зводиться до єдиного законодавчого завдання. Насправді acquis ЄС у сфері захисту персональних даних охоплює кілька самостійних інструментів, і один з них це Директива Європейського Парламенту і Ради (ЄС) 2016/680 від 27 квітня 2016 року про захист фізичних осіб у зв’язку з опрацюванням персональних даних компетентними органами для цілей запобігання, розслідування, виявлення або переслідування за вчинення кримінальних

правопорушень або виконання кримінальних покарань [31] залишається поза межами поточних законодавчих ініціатив України і потребує окремої уваги.

Директива 2016/680 є самостійним правовим інструментом, прийнятим одночасно з GDPR, але з принципово іншим предметом регулювання. GDPR не поширюється на обробку персональних даних, що здійснюється компетентними органами для цілей запобігання злочинам, їх розслідування, виявлення та переслідування, а також виконання кримінальних покарань [180]. Саме ці відносини регулює Директива 2016/680, яка встановлює комплексну рамку захисту персональних даних з урахуванням специфічної природи правоохоронної і кримінально-юстиційної діяльності з одного боку, і забезпечує права осіб, чиї дані обробляються поліцейськими та судовими органами (підозрюваних, свідків, потерпілих), з іншого [31]. Держави-члени ЄС були зобов'язані інтегрувати Директиву в національне законодавство до 6 травня 2018 року. Перший звіт Єврокомісії про її застосування, оприлюднений у 2022 році, констатував, що навіть після кількох років дії Директиви в окремих державах-членах залишаються невирішені питання стосовно обсягу прав суб'єктів даних і незалежності наглядових органів у правоохоронній сфері [168].

Хоча GDPR і Директива 2016/680 утворюють єдиний пакет реформи права ЄС у сфері захисту персональних даних, між ними є принципові відмінності, що унеможливлюють застосування одного законодавчого акта для виконання зобов'язань за обома інструментами. По-перше, Директива 2016/680 дозволяє значно ширші обмеження прав суб'єктів даних, ніж GDPR, зокрема стосовно права на доступ, права на виправлення та права на видалення, якщо такі обмеження є необхідними і пропорційними для цілей правоохоронної діяльності. По-друге, вона встановлює спеціальні вимоги щодо ведення журналів обробки даних, які не передбачені GDPR у такому вигляді. По-третє, Директива вимагає, щоб розмежування між різними категоріями суб'єктів даних (підозрюваними, засудженими, потерпілими, свідками) знаходило відображення в диференційованому правовому режимі

обробки їхніх персональних даних, чого не вимагає GDPR. Нарешті, Директива встановлює особливі вимоги до DPIA у правоохоронному контексті і до передачі даних міжнародним партнерам, наприклад поліцейським і судовим органам третіх країн [31].

Чинне українське законодавство не містить окремого спеціального закону про захист персональних даних у правоохоронній діяльності. Обробка персональних даних поліцією, прокуратурою, судами та іншими правоохоронними органами регулюється загальними нормами Закону № 2297-VI, профільними законами про окремі органи та розпорошеними спеціальними нормами. Законопроєкт № 8153 частково торкається правоохоронної сфери, зокрема, він містить окремі положення про особливості обробки персональних даних правоохоронними органами, однак висновок Ради Європи від 24 квітня 2023 року прямо зазначає, що ці положення потребують суттєвого доопрацювання для забезпечення відповідності Директиві 2016/680 [31]. Зокрема, умови допустимого втручання у права суб'єктів даних у правоохоронному контексті визначені недостатньо конкретно і потребують окремого законодавчого врегулювання.

Саме у правоохоронній сфері розрив між українським законодавством і acquis ЄС є найбільш значним, а складність адаптації пов'язана з тим, що Директива 2016/680 передбачає одночасне вирішення двох суперечливих завдань: забезпечення ефективності правоохоронної діяльності і гарантування прав осіб, чиї дані обробляються. Для України, яка одночасно здійснює реформу правоохоронної системи і адаптує законодавство до acquis ЄС в умовах воєнного стану, це завдання є особливо складним. Воно потребує не лише прийняття спеціального законодавчого акта, а й формування нової правозастосовної культури в правоохоронних органах, які традиційно не звикли розглядати захист персональних даних підозрюваних і свідків як правозастосовний пріоритет.

Директива 2016/680, аналіз якої здійснено вище, залишається поза увагою поточних законодавчих ініціатив України. Не менш актуальним, але

ще менш відображеним у вітчизняному правовому дискурсі є EU AI Act, як регуляторний інструмент, що набув чинності 1 серпня 2024 року і безпосередньо впливає на сферу захисту персональних даних. Регламент Європейського Парламенту і Ради (ЄС) 2024/1689 від 13 червня 2024 року про гармонізацію норм щодо штучного інтелекту набув чинності 1 серпня 2024 року і застосовується поетапно до 2026 року [132]. Для України цей документ має принципове значення не лише як зразок для майбутнього регулювання ШІ, а й тому, що він безпосередньо впливає на сферу захисту персональних даних в такий спосіб, який чинне українське законодавство та законопроєкт № 8153 не відображають.

EU AI Act і GDPR є взаємодоповнюючими правовими інструментами, і ст. 2 EU AI Act прямо підтверджує, що Акт не впливає на дію норм GDPR [132]. Водночас їхнє спільне застосування породжує принципово нові вимоги до контролерів і операторів персональних даних, зокрема у публічному секторі. EU AI Act класифікує системи ШІ за рівнем ризику і для систем «високого ризику», до яких віднесено, зокрема, системи ШІ, що використовуються органами влади для оцінювання фізичних осіб, управління міграцією, доступу до публічних послуг і правоохоронної діяльності, встановлює вимоги, які безпосередньо стосуються захисту персональних даних. До таких віднесено: обов’язкова оцінка відповідності до запуску системи, документування процесів обробки даних, забезпечення прозорості алгоритмічних рішень і права на оскарження автоматизованих рішень [132]. Кожна з цих вимог є самостійним правовим зобов’язанням, яке доповнює вимоги GDPR, але не дублює їх. Це означає, що відповідність законопроєкту № 8153 вимогам GDPR не означає автоматичної відповідності acquis ЄС у частині систем ШІ з публічного сектору.

О. Кожухар у дослідженні правового регулювання систем ШІ та захисту персональних даних доводить, що архітектура сучасних систем ШІ на всіх етапах їхнього життєвого циклу пов’язана з обробкою значних масивів персональних даних, а принципи захисту персональних даних (мінімізації,

прозорості та цільового обмеження) мають бути невід'ємною складовою механізму правового регулювання ШІ в Україні [57]. Ця теза є ключовою для розуміння того, що гармонізація у сфері захисту персональних даних не може бути здійснена лише через прийняття закону, аналогічного GDPR, без одночасного вирішення питань, пов'язаних з регулюванням ШІ.

Системи ШІ, що вже функціонують або впроваджуються у публічному секторі України, зокрема алгоритми виявлення ризиків у публічних закупівлях, системи аналізу судового реєстру, а також анонсоване Міністерством цифрової трансформації інтегрування ШІ у платформу «Дія», підпадають під категорію «систем ШІ високого ризику» за EU AI Act, оскільки вони застосовуються органами влади і безпосередньо стосуються прав та інтересів фізичних осіб [168]. Для таких систем Акт вимагає, серед іншого, проведення оцінки впливу на основоположні права до їх запуску, механізму людського нагляду за автоматизованими рішеннями, а також забезпечення права фізичних осіб на пояснення і оскарження рішень, прийнятих за допомогою ШІ. Жодна з цих вимог не знайшла відображення в чинному Законі № 2297-VI, і лише частково у законопроєкті № 8153 у положеннях про автоматизовану обробку персональних даних і профілювання.

Україна сьогодні дотримується стратегії поступового регулювання штучного інтелекту, що передбачає пріоритет галузевого саморегулювання над прийняттям окремого комплексного законодавчого акта, а EU AI Act використовується як орієнтир для формування національної регуляторної рамки, а не зразок для прямого відтворення у законодавстві. Водночас, як зазначають дослідники, ця стратегія є виправданою лише як короткострокова оскільки як кандидат на членство в ЄС Україна зрештою буде зобов'язана забезпечити відповідність законодавства EU AI Act як частини acquis [141]. Це означає, що вже зараз у процесі підготовки законопроєкту № 8153 до другого читання необхідно враховувати вимоги EU AI Act у частині, що стосується захисту персональних даних при використанні систем ШІ, зокрема, вимоги до

оцінки впливу на основоположні права, до прозорості і пояснюваності алгоритмічних рішень, а також до права осіб на оскарження таких рішень.

Таким чином нами послідовно продемонстровано, що гармонізація законодавства у сфері захисту персональних даних не може зводитись до текстового відтворення acquis. Центральним елементом, без якого будь-яка законодавча реформа залишатиметься декларативною, є здатність відповідного державного органу реально забезпечувати виконання закону. Саме цей вимір гармонізації є найменш видимим у публічному дискурсі і водночас найбільш критичним для отримання Україною статусу держави з високим рівнем захисту даних.

Сьогодні функції наглядового органу у сфері захисту персональних даних виконує Уповноважений Верховної Ради України з прав людини, для якого ця функція є лише однією з багатьох і не є профільною [118]. Ця модель не відповідає вимогам ст. 51 GDPR, яка передбачає наявність спеціалізованого незалежного наглядового органу, що здійснює виключно функції у сфері захисту персональних даних [180]. Некоректність такої моделі підтверджується і висновком Ради Європи від 24 квітня 2023 року, де прямо зазначено, що поєднання повноважень омбудсмана та наглядового органу з питань захисту персональних даних не забезпечує достатньої спеціалізації і незалежності для ефективного виконання наглядових функцій [98]. Формально законопроєкт № 6177 передбачає створення спеціалізованої Комісії [129], однак ресурсне забезпечення цього органу і реальні механізми його незалежності потребують окремого аналізу.

GDPR у ст. 52 визначає незалежність наглядового органу через чотири взаємопов’язані виміри: функціональну незалежність (орган діє без зовнішніх інструкцій), фінансову незалежність (власний бюджет, що не залежить від поточних рішень уряду), кадрову незалежність (особливий порядок призначення і звільнення членів) та операційну незалежність (власний персонал, матеріально-технічне забезпечення) [180]. Практика держав-членів ЄС, що проходили оцінку на предмет отримання рішення про адекватність,

свідчить, що Єврокомісія перевіряє всі чотири виміри, і формальне закріплення незалежності в законі без реального ресурсного забезпечення не є достатнім. К. Гуртова у дослідженні теорії і практики адаптації законодавства України до acquis ЄС наголошує, що інституційна стійкість регуляторного органу є необхідною умовою реальної адаптації і що відсутність достатніх ресурсів зводить нанівець навіть найдосконаліше законодавство [25].

Аналітик Axon Partners О. Задніпровська у 2023 році зафіксувала принципову проблему, яка полягала у тому, що бюджет на відповідний рік не передбачав коштів для створення нового регуляторного органу у сфері захисту персональних даних, що ставило під сумнів реалістичність законодавчих змін у визначені строки [39]. Ця проблема не є суто фінансовою, вона відображає ширше питання про пріоритетність реформи захисту персональних даних в умовах воєнного стану і обмежених бюджетних ресурсів. Водночас саме в умовах кандидатства в ЄС відкладення інституційної реформи набуває нового правового виміру: переговорний прогрес у Кластері 1 залежить у тому числі від демонстрації реальних кроків у сфері захисту основоположних прав, а не лише від прийняття відповідного законодавства.

Окремим і принципово важливим виміром інституційної спроможності є здатність майбутнього наглядового органу України до співпраці з Європейською радою із захисту даних, як колегіальним органом, що координує діяльність наглядових органів держав-членів ЄС та забезпечує узгодженість застосування GDPR [180]. Держави, що претендують на отримання рішення про адекватність, мають демонструвати не лише відповідність законодавства, а й здатність наглядового органу до реального інформаційного обміну та координації з EDPB. Для України це означає, що майбутня Комісія має бути спроможна не лише виконувати внутрішні наглядові функції, а й брати участь у механізмах взаємної допомоги та спільного розслідування, передбачених ст. 60-67 GDPR [180]. Будівництво цієї спроможності вимагає підготовки кваліфікованого персоналу, налагодження

комунікаційних каналів та формування правозастосовної практики, яка була б зрозумілою і передбачуваною для Європейської ради.

Отже, інституційна спроможність є не технічним аспектом реформи, а її системоутворюючим елементом. Прийняття законопроєктів № 8153 і № 6177, усунення прогалин у регулюванні систем ШІ і правоохоронної сфери матимуть практичний ефект лише тоді, коли існуватиме орган, здатний реально забезпечувати їхнє виконання. Саме тому питання ресурсного забезпечення, кадрового потенціалу і операційної незалежності майбутнього наглядового органу є не менш важливим законодавчим завданням, ніж змістовна реформа матеріального права.

Проведений аналіз дозволяє сформулювати не лише перелік необхідних законодавчих змін, а й їхню раціональну послідовність з урахуванням переговорної динаміки, реального стану законодавства і інституційних можливостей України. Тобто сформувати своєрідну дорожну карту. Ця послідовність є принципово важливою, оскільки не всі елементи гармонізації мають однакову вагу і однакову реалістичність у конкретних умовах воєнного стану і обмежених ресурсів.

Першим кроком є прийняття законопроєкту № 8153 з урахуванням висновку Ради Європи та нашими рекомендаціями. Це є необхідною, хоча й недостатньою умовою гармонізації. Прийняття законопроєкту матеріально наблизить українське право до GDPR і Конвенції 108+, що є мінімальним стандартом, без досягнення якого будь-який подальший переговорний прогрес у сфері захисту персональних даних є неможливим. О. Шпакович, О. Шевчук та П. Мелотікова у порівняльному дослідженні захисту персональних даних в Україні і Чеській Республіці підкреслюють, що без прийняття нового матеріального закону і утворення незалежного наглядового органу жодна подальша гармонізація не може вважатись реальною, і що обидва ці кроки є нерозривно пов’язаними передумовами [183]. При доопрацюванні законопроєкту до другого читання пріоритетними є усунення прогалин, виявлених у висновку Ради Європи [98], насамперед у частині правоохоронної

обробки, солідарної відповідальності спільних контролерів і механізму відновлення гарантій після надзвичайних обставин.

Наступним кроком повинно стати прийняття законопроєкту № 6177 та утворення Національної комісії з належним ресурсним забезпеченням. Прийняття закону без функціонуючого наглядового органу є нереалізованою гармонізацією. Як показує досвід держав, що проходили оцінку на предмет отримання рішення про адекватність, Єврокомісія починає здійснювати оцінку лише після того, як наглядовий орган не лише формально утворений, а й розпочав реальну операційну діяльність, тобто розглядає скарги, проводить перевірки і видає рішення. Цей крок є другим за черговістю, але потребує паралельної підготовки через відбір персоналу, визначення бюджету, налагодження зав'язків з Європейською радою ще до формального прийняття законопроєкту № 6177.

Третім пріоритетом є розроблення і прийняття спеціального закону про захист персональних даних у правоохоронній сфері. Як зазначено нами раніше, Директива 2016/680 залишається поза межами законопроєкту № 8153 і потребує окремого законодавчого акта. Цей крок є менш термінованим з точки зору прийняття рішення про адекватність, але є обов'язковим для переговорного прогресу у главі 24 (Кластер 1), тобто для відкриття наступних переговорних кластерів. Його підготовка потребує залучення фахівців з кримінального процесу і правоохоронної діяльності поряд із фахівцями у сфері захисту персональних даних.

Наступним є пріоритет формування правозастосовної практики як умови отримання рішення про адекватність. Отримання рішення Єврокомісії про адекватний рівень захисту персональних даних є стратегічною метою, що виходить за рамки переговорного процесу і має самостійне практичне значення, оскільки воно відкриває вільний транскордонний потік персональних даних між Україною і державами ЄС, що є критичним для IT-індустрії і бізнес-середовища. Проте це рішення Єврокомісія ухвалює лише після накопичення реальної правозастосовної практики, і зазвичай не менш

ніж через два-три роки після початку функціонування наглядового органу. У дослідженні О. Яворської зазначено, що у випадках Японії і Великої Британії підготовка рішення про адекватність зайняла кілька років з моменту початку переговорів, і що ключовим критерієм оцінки була саме сукупність правозастосовної практики, а не формальна відповідність законодавства [163].

Для моніторингу прогресу гармонізації пропонуємо використовувати три взаємопов'язані критерії:

– нормативний визначає відповідність тексту законодавства вимогам GDPR, Директиви 2016/680 і Конвенції 108+ за оцінкою Ради Європи і EDPB, з особливою увагою до норм, що регулюють обробку персональних даних у системах цифрового публічного управління – платформах електронних послуг, реєстрах і системах міжвідомчого обміну;

– інституційний забезпечує реальну операційну спроможність наглядового органу, що вимірюється кількістю розглянутих скарг, виданих рішень і проведених перевірок щодо суб'єктів публічного сектору, а також рівнем незалежності органу за чотирма вимірами, визначеними ст. 52 GDPR, і його здатністю здійснювати нагляд за цифровими публічними сервісами, що обробляють персональні дані в масових масштабах;

– практичний характеризується рівнем обізнаності суб'єктів обробки, насамперед органів публічної влади як основних контролерів персональних даних в умовах цифровізації, і суб'єктів даних щодо їхніх прав і обов'язків, а також реальною доступністю механізмів захисту прав з урахуванням часу розгляду скарг, рівня виконання рішень і ефективності судового контролю.

Сукупне виконання всіх трьох критеріїв може свідчити про реальну, а не лише формальну гармонізацію законодавства України у сфері захисту персональних даних із правом ЄС і про готовність системи адміністративно-правового забезпечення захисту персональних даних в умовах цифровізації публічного управління до стандартів, що висуваються в рамках євроінтеграційного процесу.

Висновки до розділу 3

Проведене дослідження дозволило визначити, що система адміністративної відповідальності за порушення законодавства про захист персональних даних є структурно неефективною. Чинна редакція ст. 188-39 КУпАП характеризується вузьким суб'єктним складом, відсутністю відповідальності юридичних осіб та незначними санкціями, а практика її застосування додатково ускладнюється процедурними бар'єрами, зокрема відсутністю спеціального порядку збирання цифрових доказів і невизначеністю строків давності для тривалих або прихованих порушень. Чинна редакція ст. 188-39 КУпАП характеризується вузьким суб'єктним складом, відсутністю відповідальності юридичних осіб та незначними санкціями, що в сукупності з процедурною обтяженістю провадження перетворює цю норму на фактично недієвий інструмент правозастосування.

Правовий режим обробки персональних даних у системах електронних публічних послуг містить системні прогалини, що безпосередньо обмежують здатність суб'єктів даних реалізувати свої права. Відсутність законодавчого регулювання спільного контролерства, невизначеність правових критеріїв допустимості запитів у системі «Трембіта», обмеження гарантій захисту в умовах воєнного стану, а також відсутність вимог privacy by design і DPIA як передумов запуску публічних цифрових сервісів є взаємопов'язаними проблемами, що потребують системного законодавчого вирішення.

Гармонізація адміністративного законодавства України у сфері захисту персональних даних із правом ЄС є багатовимірним процесом, що виходить за межі прийняття одного законодавчого акта. Повноцінна гармонізація передбачає послідовне виконання чотирьох пріоритетів: прийняття законопроєкту № 8153 з урахуванням висновку Ради Європи; утворення Національної комісії з питань захисту персональних даних з належним ресурсним забезпеченням; розроблення спеціального законодавства у сфері захисту персональних даних у правоохоронній діяльності відповідно до

Директиви 2016/680; формування реальної правозастосовної практики як умови отримання рішення Єврокомісії про адекватний рівень захисту. Критеріями оцінки досягнутого рівня відповідності є нормативна, інституційна та практична складові, сукупне виконання яких свідчить про реальну, а не лише формальну гармонізацію в умовах цифровізації публічного управління.

ВИСНОВКИ

У роботі здійснено комплексне дослідження адміністративно-правового забезпечення захисту персональних даних в умовах цифровізації публічного управління, виявлено системні прогалини чинного законодавства та обґрунтовано перспективні шляхи його вдосконалення з урахуванням міжнародних стандартів і досвіду держав-членів Європейського Союзу.

1. Аналіз доктринальних підходів і нормативних визначень засвідчує, що персональні дані є специфічним об’єктом адміністративно-правової охорони, що відрізняється від об’єктів конституційно-правового і цивільно-правового регулювання. Адміністративне право здатне забезпечити нормативний, інституційний та юрисдикційний виміри такої охорони, що обумовлює його центральну роль у регулюванні відносин між суб’єктами публічного адміністрування і громадянином у цій сфері. Множинність наукових підходів до визначення персональних даних свідчить про складність самого об’єкта і неможливість його вичерпного нормативного визначення поза контекстом конкретних правовідносин. З урахуванням цього запропоновано авторське визначення персональних даних у контексті цифрового публічного управління як будь-яких відомостей чи сукупності відомостей про фізичну особу, яка ідентифікована або може бути ідентифікована, що збираються, зберігаються та обробляються суб’єктами публічного адміністрування в рамках адміністративних процедур, у тому числі із застосуванням цифрових технологій та інтегрованих інформаційних систем, на підставі та у спосіб, визначені законом, з метою реалізації публічно-владних повноважень та забезпечення прав і законних інтересів особи. Право на захист персональних даних охарактеризовано як самостійне публічне суб’єктивне право з тривимірною структурою правомочностей: права вимагати законності обробки від суб’єктів публічного адміністрування, права на реалізацію суб’єктивних прав щодо власних даних та права на захист у разі порушення,

що дозволяє чітко визначити його зміст, суб'єктний склад і механізм реалізації в адміністративно-правових відносинах.

2. Цифровізація публічного управління є чинником якісної трансформації правовідносин у сфері захисту персональних даних, що виявляється у розширенні їхнього суб'єктного складу, об'єкта, змісту прав і обов'язків та характеру правового зв'язку між державою і громадянином. Персональні дані перетворюються із статичного масиву відомостей на динамічний ресурс, що безперервно агрегується і змінює свій правовий режим залежно від контексту обробки, а сам правовий зв'язок між державою і громадянином із епізодичного і процедурно зумовленого стає постійним і багатовимірним. Виявлено два нові типи правовідносин, що не характерні для традиційного адміністративного права: відносини між суб'єктом даних і алгоритмом як суб'єктом автоматизованого управлінського рішення та відносини в умовах структурної інформаційної асиметрії, за якої держава формує комплексний цифровий профіль громадянина незалежно від його активних звернень. Аналіз функціонування платформи «Дія», системи «Трембіта» та реєстру «Оберіг» підтвердив, що зазначені правові ризики є реальними і потребують адекватного адміністративно-правового регулювання.

3. Міжнародно-правові стандарти захисту персональних даних утворюють багаторівневу архітектуру, що охоплює Конвенцію 108+, GDPR, Директиву 2016/680, Data Governance Act та EU AI Act як взаємопов'язані інструменти. Їхній вплив на національне адміністративне законодавство здійснюється через чотири механізми, що відрізняються за юридичною природою і порядком реалізації: нормативний через пряму дію ратифікованих міжнародних договорів; адаптаційний через зобов'язання привести законодавство у відповідність до acquis ЄС; юрисдикційний через обов'язкову практику ЄСПЛ щодо тлумачення ст. 8 Конвенції про захист прав людини; та орієнтувальний через добровільне запозичення стандартів, дотримання яких є індикатором реальної відповідності вимогам ЄС. Аналіз стану імплементації

засвідчив системний характер невідповідності українського законодавства міжнародним стандартам, що виявляється у термінологічному, інституційному та процедурному вимірах. Це обумовлює необхідність комплексного реформування адміністративного законодавства у цій сфері, яке має охоплювати одночасно матеріальне право, інституційну архітектуру та механізми правозастосування.

4. Нормативно-правове регулювання захисту персональних даних у сфері цифрового публічного управління характеризується структурним дисбалансом між стрімким розвитком законодавства про цифрові публічні послуги і реєстри та відставанням спеціального законодавства про захист персональних даних. Закони про електронні публічні послуги, публічні електронні реєстри, електронну ідентифікацію та електронні комунікації формують розгалужену нормативну рамку цифрового публічного управління, проте жоден із них не містить комплексного регулювання захисту персональних даних, обмежуючись бланкетними нормами до Закону № 2297-VI, який своєю чергою розроблявся без урахування реалій платформної моделі надання публічних послуг. Виявлені прогалини мають системний характер і охоплюють відсутність правового визначення статусу оператора цифрових платформ як контролера персональних даних, відсутність вимог до оцінки впливу на захист даних при впровадженні нових цифрових сервісів та відсутність механізму прозорості алгоритмічних рішень. Їх усунення потребує узгодженого реформування всього масиву законодавства про цифрове публічне управління з урахуванням стандартів GDPR.

5. Система суб’єктів забезпечення захисту персональних даних у сфері публічного управління є багаторівневою і охоплює суб’єктів нормотворчих, виконавчих, контрольно-наглядових та правоохоронних повноважень. Її функціональна класифікація з урахуванням специфіки цифрового публічного управління виявила системну прогалину у розподілі відповідальності між суб’єктами в умовах платформної моделі надання публічних послуг: чинне законодавство не визначає, хто і в якому обсязі несе відповідальність за захист

персональних даних у ситуаціях, коли кілька суб'єктів одночасно беруть участь в обробці даних через інтегровані платформи і реєстри. Ключовою інституційною прогалиною є відсутність спеціалізованого незалежного наглядового органу у сфері захисту персональних даних. Чинна модель, за якої відповідні функції покладено на Уповноваженого Верховної Ради України з прав людини, не забезпечує необхідного рівня спеціалізації, незалежності та операційної спроможності для ефективного нагляду за обробкою персональних даних у масштабах цифрового публічного управління. Запровадження Національної комісії з питань захисту персональних даних відповідно до законопроєкту № 6177 є необхідною інституційною передумовою реального захисту прав суб'єктів персональних даних та отримання Україною рішення Єврокомісії про адекватний рівень захисту.

6. Адміністративні процедури обробки персональних даних у системах цифрового публічного управління мають якісно відмінну природу порівняно з традиційними адміністративними процедурами, що зумовлює необхідність їх окремого правового регулювання. Ключовими ознаками цих процедур є автоматизований характер обробки без безпосередньої участі посадової особи, множинність суб'єктів у рамках однієї процедури та динамічне розширення обсягу даних внаслідок міжреєстрової взаємодії. Зазначена специфіка породжує правові проблеми, нехарактерні для традиційного адміністративного права: неможливість персоніфікованої відповідальності за автоматизоване рішення, складність забезпечення права на оскарження та відсутність механізмів, що гарантують пропорційність обсягу оброблюваних даних меті конкретної процедури. Встановлено, що правове регулювання таких процедур має ґрунтуватись на вимогах прозорості алгоритмічних рішень, підзвітності всіх суб'єктів обробки та реальної доступності механізмів захисту прав суб'єктів персональних даних, що відповідає стандартам GDPR і практиці ЄСПЛ та потребує законодавчого закріплення у спеціальних нормах про адміністративні процедури в умовах цифрового публічного управління.

7. Аналіз правозастосовної практики у сфері адміністративної відповідальності за порушення законодавства про захист персональних даних засвідчив феномен «мертвої норми», який полягає у тому, що за наявності тисяч звернень суб'єктів персональних даних кількість складених протоколів за ст. 188-39 КУпАП є мінімальною, а реальне притягнення до відповідальності поодиноким. Системними причинами цього є вузький суб'єктний склад відповідальності, що виключає юридичних осіб як самостійних суб'єктів, невідповідність розміру санкцій масштабу та суспільній небезпеці порушень, а також процедурна обтяженість провадження і відсутність спеціального порядку збирання цифрових доказів. Реформування системи адміністративної відповідальності у цій сфері запропоновано здійснити за моделлю дворівневої структури GDPR з диференціацією санкцій залежно від тяжкості порушення, його масштабу та суб'єкта, з одночасним запровадженням відповідальності юридичних осіб і спрощеного провадження для менш серйозних порушень за умови їх добровільного усунення. Реалізація цих пропозицій у рамках доопрацювання законопроєкту № 8153 до другого читання дозволить перетворити механізм адміністративної відповідальності на реально діючий інструмент захисту персональних даних.

8. Дослідження правового режиму захисту персональних даних у системах електронних публічних послуг виявило, що проблеми платформи «Дія», системи «Трембіта» та реєстру «Оберіг» мають спільну системну причину, а саме відсутність превентивних правових інструментів на етапі проектування та запуску публічних цифрових сервісів. Невизначеність розподілу відповідальності між платформою і органами-надавачами послуг, відсутність правових критеріїв допустимості запитів у системі міжвідомчого обміну, обмеження гарантій захисту в умовах воєнного стану – усі ці проблеми є наслідком рішень, прийнятих на етапі проектування без урахування вимог захисту персональних даних. Обґрунтовано пропозиції щодо законодавчого закріплення обов'язкових вимог privacy by design і проведення оцінки впливу на захист персональних даних як передумов введення в експлуатацію нових

державних інформаційних систем, що обробляють персональні дані громадян, а також щодо доповнення законопроєкту № 8153 нормою про спільне контролерство із солідарною відповідальністю суб'єктів перед суб'єктами персональних даних. Реалізація цих пропозицій дозволить перейти від реактивної до превентивної моделі захисту персональних даних у цифровому публічному управлінні.

9. Гармонізація адміністративного законодавства України у сфері захисту персональних даних із правом ЄС є багатовимірним процесом, що виходить за межі імплементації GDPR і охоплює Директиву 2016/680 про захист персональних даних у правоохоронній діяльності та EU AI Act у частині систем штучного інтелекту у публічному секторі. Зосередженість поточних законодавчих ініціатив виключно на законопроєкті № 8153 не забезпечує повноти гармонізації, оскільки правоохоронна сфера і регулювання ШІ залишаються поза його межами. Обґрунтовано пріоритетну послідовність законодавчих та інституційних змін, що охоплює прийняття законопроєкту № 8153 з урахуванням висновку Ради Європи, утворення Національної комісії з питань захисту персональних даних з належним ресурсним забезпеченням, розроблення спеціального законодавства у правоохоронній сфері відповідно до Директиви 2016/680 та формування реальної правозастосовної практики як умови отримання рішення Єврокомісії про адекватний рівень захисту. Сформульовано три взаємопов'язані критерії оцінки досягнутого рівня відповідності (нормативний, інституційний та практичний), сукупне виконання яких забезпечить реальну гармонізацію адміністративного законодавства України у сфері захисту персональних даних в умовах цифровізації публічного управління.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Авер'янов В. Б. Органи виконавчої влади в Україні. Київ: Ін Юре, 1997. 48 с.

2. Адміністративне право України. Академічний курс: підруч.: У двох томах: Том 1. Загальна частина / Ред. колегія: В. Б. Авер'янов (голова). К.: 2004. 584 с.

3. Адміністративне право України. Повний курс: підручник / В. Галунько, П. Діхтієвський, О. Кузьменко та ін. Херсон, 2021. 656 с.

4. Арістова І.В. Національний механізм реалізації цілей сталого розвитку в умовах інформаційного суспільства в Україні: роль юридичного механізму та його складових. Монографія: Сучасна парадигма публічного та приватного права в умовах сталого розвитку. Scientific monograph. Vol. 1. Riga, Latvia: Baltija Publishing, 2023. P. 1-31. DOI: https://doi.org/10.30525/978-9934-26-331-6-1

5. Атаманова Н. В., Луняченко І. В. До питання цифровізації публічного управління в Україні. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція*. 2024. № 68. С. 4-8. DOI: https://doi.org/10.32782/2307-1745.2024.68.1

6. Базалицький В.І. Дотримання прозорості в обробці персональних даних за допомогою штучного інтелекту. *Академічні візії*. 2024. Випуск 32. DOI: https://doi.org/10.5281/zenodo.11544316

7. Балануца О.О. Адаптація законодавства України до права ЄС як складова сучасного правотворення в Україні: сучасний стан та виклики. *Юридичний науковий електронний журнал.* 2024. № 12. С. 656-659. DOI: https://doi.org/10.32782/2524-0374/2024-12/153

8. Балацька В. С. Методи та засоби підвищення захищеності персональних даних у державних електронних реєстрах : дис. ... д-ра філософії : 125 Кібербезпека. Львів : Національний університет «Львівська політехніка», 2025. 231 с. URL:

https://lpnu.ua/sites/default/files/2025/radaphd/32586/disertaciyabalatskavaleriiasergiivna.pdf (дата звернення 26.04.2026)

9. Баранов О. А. Правове забезпечення інформаційної сфери: теорія, методологія і практика: монографія. 2014. Київ: Едельвейс, 2014. 497 с.

10. Бем М. В., Городиський І. М. Відповідальність за порушення законодавства про захист персональних даних: проблеми та шляхи вирішення. *Право України*. 2019. № 2. С. 237-255. DOI: https://doi.org/10.33498/louu-2019-02-237

11. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: правове регулювання та практичні аспекти : науково-практичний посібник. Київ: К.І.С., 2015. 220 с. URL: https://rm.coe.int/168059920c (дата звернення 26.04.2026)

12. Бершадська К. Захист персональних даних у цивільних правовідносинах: досвід ЄС та України. *Права людини в умовах воєнного стану: прикладний аспект*: зб. матеріалів І Всеукр. наук.-практ. онлайн конф. (м. Київ, 12 груд. 2025 р.) Київ : МДУ, 2025. С. 12-15.

13. Білецький М. О. Міжнародний досвід використання цифрових технологій в публічному управлінні. *Наукові перспективи*. 2024. № 11 (53). С. 53-67. DOI: https://doi.org/10.52058/2708-7530-2024-11(53)-53-67

14. Бліхар М. М. Правові основи захисту персональних даних в Інтернеті. *Науковий вісник Мукачівського державного університету*. 2023. № 62(1). С. 20-23. DOI: https://doi.org/10.32841/2307-1745.2023.62.4

15. Брижко В. М. Організаційно-правові питання захисту персональних даних : дис. … канд. юрид. наук : 12.00.07. Київ, 2004. 251 с.

16. Бугай О. В. Можливості та обмеження алгоритмічного прийняття рішень у публічному управлінні. Інвестиції: практика та досвід. 2022. № 17. С. 144-150. DOI: https://doi.org/10.32702/2306-6814.2022.17.144

17. Воюта Д. Захист персональних даних у сфері безпеки та оборони: реєстри «воєнного стану» («Оберіг») / Центр демократії та верховенства права.

2024. URL: https://cedem.org.ua/analytics/zahyst-personalnyh-danyh-oberig/ (дата звернення 26.04.2026)

18. Гачкевич А. О. Ключові аспекти проблеми захисту персональних даних у контексті розвитку штучного інтелекту. *Вісник Національної академії правових наук України*. 2025. № 32(4). С. 30-44. DOI: https://doi.org/10.31359/1993-0909-2025-32-4-30

19. Гиляка О. С. Право на приватність та захист персональних даних в умовах цифровізації. *Вісник Національної академії правових наук України*. 2023. Том 30, № 1. С. 15-30. DOI: https://doi.org/10.31359/1993-0909-2023-30-1-15

20. Гіляка О. С., Мерник А. М. Правове регулювання та практика Європейського суду з прав людини і Європейського суду справедливості щодо прав людини у сфері використання цифрових технологій. *Вісник Національної академії правових наук України.* 2024. Т. 31. № 1. С. 40-55. DOI: https://doi.org/10.31359/1993-0909-2023-31-1-40

21. Головацький Н. Т. Адміністративно-правові механізми захисту персональних даних у системах автоматизованого прийняття рішень як превенція корупційних ризиків. *Аналітично-порівняльне правознавство.* 2025. № 6. С. 548-552. DOI: https://doi.org/10.24144/2788-6018.2025.06.3.85

22. Головацький Н. Т. Інструменти діяльності публічної адміністрації у сфері обігу персональних даних. *Аналітично-порівняльне правознавство*. 2024. № 4. С. 331-335. DOI: https://doi.org/10.24144/2788-6018.2024.04.52

23. Головко К. М. Цифровізація адміністративних процедур в Україні: правові виклики та перспективи. *Правові новели.* 2025. № 26. С. 66-76. DOI: https://doi.org/10.32782/ln.2025.26.7

24. Гудзь Л. В. Забезпечення права на приватність у контексті використання штучного інтелекту: потенційні загрози та шляхи їх подолання. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2024. Т. 1. № 86. С. 175-180. DOI: https://doi.org/10.24144/2307-3322.2024.86.1.25

25. Гуртова К.М. Теорія і практика адаптації законодавства України до законодавства ЄС. *Київський часопис права.* 2023. № 4. С. 162-168. https://doi.org/10.32782/klj/2023.4.23

26. Гусаров С. М., Мельник К. Ю. Захист персональних даних працівника. *Право і безпека*. 2023. № 2(89). С. 133-145. DOI: https://doi.org/10.32631/pb.2023.2.12

27. Департамент у сфері захисту персональних даних Секретаріату Уповноваженого Верховної Ради України з прав людини: інформація про підрозділ. URL: https://ombudsman.gov.ua/uk/informaciya-pro-pidrozdil-zpd (дата звернення 26.04.2026)

28. Деякі питання електронної взаємодії електронних інформаційних ресурсів : постанова Кабінету Міністрів України від 08.09.2016 № 606. URL: https://zakon.rada.gov.ua/laws/show/606-2016-%D0%BF (дата звернення 26.04.2026)

29. Деякі питання електронної системи охорони здоров'я : Постанова Кабінету Міністрів України від 25.04.2018 № 411. URL: https://zakon.rada.gov.ua/laws/show/411-2018-п (дата звернення 26.04.2026)

30. Деякі питання забезпечення функціонування інформаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану: Постанова Кабінету Міністрів України від 21.03.2022 № 263. URL: https://zakon.rada.gov.ua/laws/show/263-2022-%25D0%25BF#Text (дата звернення 26.04.2026)

31. Директива Європейського Парламенту і Ради (ЄС) 2016/680 від 27.04.2016 про захист фізичних осіб у зв'язку з опрацюванням персональних даних компетентними органами для цілей запобігання, розслідування, виявлення або переслідування за вчинення кримінальних правопорушень або виконання кримінальних покарань. URL: https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng (дата звернення 26.04.2026)

32. Діордіца І., Коваленко І., Коваль О. Правова охорона персональних даних у сфері охорони здоров'я. *Науковий вісник*

Ужгородського національного університету. *Серія: Право*. 2024. № 82(2). С. 141-146. DOI: https://doi.org/10.24144/2307-3322.2024.82.2.22

33. Дубняк М. В. Е-урядування, Smart-управління та GovTech: проблеми правового забезпечення цифровізації публічного адміністрування. *Інформація і право*. 2025. № 3 (54). С. 86-96. DOI: https://doi.org/10.37750/2616-6798.2025.3(54).340494

34. Дуравкін П.М., Гафич І.І. Сучасні виклики та майбутнє правового захисту персональних даних: під впливом розвитку цифровізації. *Право та інновації*. 2023. № 3 (43). С. 89-100. DOI: http://doi.org/10.37772/2518-1718-2023-3(43)-12

35. Дяковський О. С. Характерні риси прояву захисту персональних даних. *Юридичний науковий електронний журнал*. 2025. № 2. С. 230-232. DOI: https://doi.org/10.32782/2524-0374/2025-2/53

36. Дяковський О.С. Порівняльна характеристика захисту персональних даних за національним та європейським законодавством. *Юридичний науковий електронний журнал.* 2023. № 8. С. 278-280. DOI: https://doi.org/10.32782/2524-0374/2023-8/64

37. Загальна теорія права : підручник / за ред. О. В. Петришина ; [наук. ред.: Д. В. Лук'янов, С. І. Максимов, В. С. Смородинський] ; Нац. акад. прав. наук України ; Нац. юрид. ун-т ім. Ярослава Мудрого. Вид. 2-ге, виправ. й перероб. Харків : Право, 2025. 576 с.

38. Задерейко О. В., Трофименко О. Г., Єленич С. І., Логінова Н. І., Гура В. І. Системний аналіз захищеності державних електронних реєстрів та баз персональних даних. *Кібербезпека: освіта, наука, техніка.* 2025. № 4 (28). С. 57-70. DOI: https://doi.org/10.28925/2663-4023.2025.28.735

39. Задніпровська О. Законопроєкт про персональні дані: чого чекати українському бізнесу. *Axon Partners.* 2023. URL: https://axon.partners/zakonoproiekt-pro-personalni-dani-choho-chekaty-ukrainskomu-biznesu/ (дата звернення 26.04.2026)

40. Захарчук І.В. Цифрові права громадян України: конституційно-правове закріплення та механізми реалізації. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Том 1, №90. С. 268-273. DOI: https://doi.org/10.24144/2307-3322.2025.90.1.34

41. Захист персональних даних пацієнта при роботі з інформаційно-комунікаційними системами електронної охорони здоров'я / Міністерство охорони здоров'я України. URL: https://moz.gov.ua/uk/zahist-personalnih-danih-paciyenta-pri-roboti-z-informacijno-komunikacijnimi-sistemami-elektronnoyi-ohoroni-zdorov-ya (дата звернення 26.04.2026)

42. Захист персональних даних та перспективи створення незалежного державного наглядового органу – експертне обговорення. Офіс Ради Європи в Україні. URL: https://www.coe.int/uk/web/kyiv/hr-ccj-all-news/-/asset_publisher/b9IKR8z6LsM0/content/protection-of-personal-data-and-prospects-for-the-establishment-of-an-independent-state-supervisory-body-expert-discussion (дата звернення 26.04.2026)

43. Заярний О. А. Правове забезпечення розвитку інформаційної сфери України: адміністративно-деліктний аспект : монографія. Київ: Видавничий дім «Гельветика», 2017. 700 с. URL: https://ippi.org.ua/sites/default/files/zayarnii_monografiya_tv_pereplet_0.pdf (дата звернення 26.04.2026)

44. Злив даних 20 млн. українців: у Мінцифри пояснили що сталося. *РБК-Україна.* 2025. URL: https://www.rbc.ua/rus/news/zliv-danih-20-mln-ukrayintsiv-diyi-sprostuvali-1758441481.html (дата звернення 26.04.2026)

45. Іванов О. Обов'язкове інформування, контроль та великі штрафи: як новий законопроєкт змінює правила захисту персональних даних. *Економічна правда.* 09.02.2024. URL: https://epravda.com.ua/columns/2024/02/9/709745/ (дата звернення 26.04.2026)

46. Інформаційна довідка щодо штрафних санкцій за порушення вимог GDPR / Дослідницька служба Верховної Ради України. URL:

https://research.rada.gov.ua/uploads/documents/33028.pdf (дата звернення 26.04.2026)

47. Касперський І. П. Проблеми забезпечення принципів захисту персональних даних у процесах цифрової трансформації. *Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання* : матеріали ІІ Всеукраїнської науково-практичної конференції, Київ, 25 грудня 2022 р. С. 33-37.

48. Кебус А. В. Законодавства України та держав ЄС щодо кримінально-правового захисту персональних даних. *Часопис Київського університету права*. 2023. № 1. С. 202-205. DOI: https://doi.org/10.36695/2219-5521.1.2023.43

49. Кірієнко В.М. Захист персональних даних як аспект національної безпеки в умовах збройного конфлікту. *Юридичний науковий електронний журнал.* 2024. № 1. С. 398-400. DOI: https://doi.org/10.32782/2524-0374/2024-1/90

50. Кірін Р. С. Періодизація розвитку законодавства про е-урядування. Juris Europensis Scientia. 2025. № 3. С. 18-24. DOI: https://doi.org/10.32782/chern.v3.2025.4

51. Кірін Р. С. Правові засади євроінтеграційного розвитку законодавства про е-урядування міст України у воєнний та повоєнний час. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2026. Вип. 93, ч. 1. С. 247-261. DOI: https://doi.org/10.24144/2307-3322.2026.93.1.36

52. Клочан В. В., Петрів І. М. Цифровізація публічного управління в територіальних громадах: інструменти, виклики та перспективи трансформації. *Актуальні проблеми економіки*. 2024. № 11 (2). С. 160-169. DOI: https://doi.org/10.32752/1993-6788-2024-2-281-160-169

53. Коваленко Ю. О. Особливості захисту персональних даних у ЄС та їх вплив на євроінтеграцію України. *Право та державне управління*. 2023. № 3. С. 138-145. DOI: https://doi.org/10.32782/pdu.2023.3.21

54. Коваленко Ю.О. Захист персональних даних в умовах євроінтеграції України. *Інтеграція України до Європейського Союзу: виклики в умовах воєнного стану* : зб. матер. і тез доповідей міжнар. наук.-практ. конф. (м. Київ, 4–6 листопада 2024 р.). Київ : Вид-во «Людмила», 2025. С. 144-146.

55. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-X. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text (дата звернення 26.04.2026)

56. Кожухар О. Правове регулювання систем штучного інтелекту та захист персональних даних: лінії взаємозв'язків. *Наукові записки НаУКМА. Юридичні науки*. 2025. Т. 16. С. 80-87. DOI: https://doi.org/10.18523/2617-2607.2025.16.80-87

57. Кожухар О. Принцип прозорості в контексті правового регулювання систем штучного інтелекту. *Наукові записки НаУКМА. Юридичні науки.* 2025. Т. 15. С. 78-85. DOI: https://doi.org/10.18523/2617-2607.2025.15.78-85

58. Коломоєць Ю.О. Проблеми забезпечення прав і свобод людини в умовах цифровізації системи публічного управління. *Державне управління: удосконалення та розвиток*. 2023. № 1. DOI: http://doi.org/10.32702/2307-2156.2023.1.6

59. Колотило М. Ю. Генезис правового регулювання персональних даних в Україні: адміністративно-правові аспекти. *Право і суспільство.* 2025. № 2. С. 238-249. DOI: https://doi.org/10.32842/2078-3736/2025.2.32

60. Колпаков В. К., Кузьменко О. В. Адміністративне право України: підручник. Київ : Юрінком Інтер, 2003. 544 с.

61. Конвенція про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини) від 04.11.1950. Ратифікована Законом України від 17.07.1997 № 475/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/995_004 (дата звернення 26.04.2026)

62. Конвенція про захист прав людини і основоположних свобод від 04.11.1950. Ратифікована Законом України від 17.07.1997 № 475/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/995_004 (дата звернення 26.04.2026)

63. Конституція України: Закон від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення 26.04.2026)

64. Костюк Д.І. Адміністративні процедури обробки персональних даних у системах міжвідомчого електронного обміну *Приватне право і підприємництво*. 2026. Вип. 26. С. 178–185. DOI: https://doi.org/10.32849/2409-9201.2026.26.19

65. Костюк Д.І. Імплементація стандартів конвенції 108+ та GDPR в адміністративне законодавство України. *Україна в умовах реформування правової системи: сучасні реалії та міжнародний досвід*: матеріали IX Міжнародної науково-практичної конференції (м. Тернопіль, 2–3 травня 2025 р.). Тернопіль: ЗУНУ, 2025. С. 346–348. URL: https://confuf.wunu.edu.ua/index.php/confuf/article/view/1732/1711

66. Костюк Д.І. Наглядовий орган у сфері захисту персональних даних: стандарти незалежності та перспективи інституційної реформи в Україні *Людина, суспільство, держава: актуальні питання правового регулювання взаємодії*: тези доп. учасників. II наук.-практ. конф. (Київ, 21 лист. 2025 р.). Київ: 2025. С. 65–67. DOI: https://doi.org/10.71404/PPSS.2025.3.18. URL: https://library.pp-ss.pro/index.php/ndippsn_20251121/article/view/kostiuk/pdf

67. Костюк Д.І. Нормативно-правове регулювання обробки персональних даних у публічних електронних реєстрах України. *Актуальні проблеми правознавства*. 2026. № 1 (45). С. 98–105. DOI: https://doi.org/10.35774/app2026.01.098

68. Костюк Д.І. Персональні дані як об’єкт адміністративно-правової охорони. *Актуальні проблеми приватного та публічного права* : матеріали VIII Міжнародної науково-практичної конференції присвяченої 97-річчю від

дня народження члена-кореспондента НАПрН України, академіка Міжнародної кадрової академії, заслуженого діяча науки України, доктора юридичних наук, професора О. І. Процевського, Харків, 27 березня 2026 року. Харківський національний педагогічний університет імені Г. С. Сковороди, Україна. Видавництво: ХНПУ імені Г. С. Сковороди, 2026. С. 505–507.

69. Костюк Д.І. Правовий статус платформи «Дія» як суб'єкта обробки персональних даних. *Журнал східноєвропейського права*. 2026. № 145. С. 321–328. DOI: https://doi.org/10.71404/2409-6415.145.36

70. Кравчук В. Захист персональних даних в умовах воєнного стану. *Юридичний науковий електронний журнал.* 2022. № 9. С. 319-321. URL: http://lsej.org.ua/9_2022/77.pdf (дата звернення 26.04.2026)

71. Краковська А., Бабик М. Цифровізація адміністративних послуг в Україні: проблеми та перспективи розвитку. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2022. Вип. 70. С. 329-334. URL: https://doi.org/10.24144/2307-3322.2022.70.52

72. Крамський С. О., Дарушин О. В., Захарченко О. В. Еволюція електронного урядування сталого розвитку в Україні. *Київський економічний науковий журнал.* 2025. № 9. С. 143-148. DOI: https://doi.org/10.32782/2786-765X/2025-9-19

73. Кримінальний кодекс України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення 26.04.2026)

74. Кримінально-правова характеристика діяння порушення недоторканності приватного життя (ст. 182 КК України) : монографія / за заг. ред. В.К. Матвійчука. Київ: Видавництво Ліра-К, 2022. 232 с.

75. Лист Державної служби з питань захисту персональних даних від 31.12.2013 № 10/3173-13. URL: https://hrliga.com/index.php?module=norm_base&op=view&id=1220 (дата звернення 26.04.2026)

76. Луніна Д. С. Адміністративно-правовий статус Міністерства цифрової трансформації України. *Юридична наука.* 2020. № 2 (104). С. 225-236. DOI: https://doi.org/10.32844/2222-5374-2020-104-2.26

77. Мазепа С. Імплементація європейських стандартів інформаційної безпеки в національне законодавство: проблеми та перспективи. *Держава та регіони. Серія: Право.* 2025. № 3. С. 44-49. DOI: https://doi.org/10.32782/1813-338X-2025.3.6

78. Малюга Л. Ю., Шкрібляк К. П. Особливості захисту персональних даних у процесі цифровізації трудових відносин. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Вип. 91, ч. 2. С. 114-120. DOI: https://doi.org/10.24144/2307-3322.2025.91.2.14

79. Маслак Н. В. Відкритість та доступність публічних електронних реєстрів України: переваги та виклики на шляху апроксимації *acquis cottmunautaire* Європейського Союзу. *Європеїзація кримінального права України*: матеріали міжнародної наукової конференції, 19 грудня 2024 р. С. 253-257.

80. Медяник В. А. Цифровізація публічного управління в соціальній сфері: адміністративно-правовий вектор трансформації в Україні. *Аналітично-порівняльне правознавство*. 2025. № 4 (1). С. 226-231. DOI: https://doi.org/10.24144/2788-6018.2025.04.1.37

81. Мигаль Р. В., Фітяк Є. М., Кузик Д. О. Адміністративно-правове регулювання цифровізації адміністративних процедур в Україні. *Академічні візії.* 2024. Вип. 33. DOI: https://doi.org/10.5281/zenodo.14771983

82. Михайлик А. С. До питання нормативно-правового регулювання захисту персональних даних працівників в Україні. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2022. Вип. 72, Том 2. С. 82-87. DOI: https://doi.org/10.24144/2307-3322.2022.72.46

83. Михайлик А. С. До питання нормативно-правового регулювання захисту персональних даних працівників. *Науковий вісник Ужгородського*

національного університету. 2022. № 72. С. 82-85. DOI: https://doi.org/10.24144/2307-3322.2022.72.46

84. Ненько С. С. Цифровізація публічного адміністрування як фактор модернізації адміністративно-правового забезпечення підприємництва. *Юридичний науковий електронний журнал*. 2025. № 9. С. 160-165. DOI: https://doi.org/10.32782/2524-0374/2025-9/33

85. Нестеренко К. В. Розвиток е-урядування в Україні: Дія. *Сучасне підприємництво: інновації, проєкти, сталий розвиток*: матеріали конф. Дніпро, 2022. С. 867-870.

86. Нестеренко О. Інформатизація державного управління: тернистий шлях піднесення. *Суспільство. Економіка. Цифровізація*. 2024. № 2 (02). С. 5-21 DOI: https://doi.org/10.31379/sed.2.2.2024.9

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

88. Пазюк А. В. Міжнародно-правовий захист права людини на приватність персоніфікованої інформації : дис. … канд. юрид. наук : 12.00.11. Київ. нац. ун-т ім. Т. Шевченка. Київ, 2004. 207 с.

89. Пальчик М. Л., Шкрібляк К. П., Березделецький Ю. М. Актуальні проблеми захисту персональних даних як напряму забезпечення національної безпеки України в умовах сучасних загроз. *Аналітико-порівняльне правознавство*. 2025. Випуск 6, Том 2. С. 425-434. DOI: https://doi.org/10.24144/2788-6018.2025.06.2.69

90. Переговори про вступ України до ЄС: повний гід у 12 питаннях. URL: https://eu-ua.kmu.gov.ua/news/peregovory-pro-vstup-ukrayiny-do-yes-povnyj-gid-u-12-pytannyah/ (дата звернення 26.04.2026)

91. Пилипчук В. Г., Брижко В. М. Трансформація системи захисту персональних даних та приватності в контексті євроінтеграції України. *Вісник Національної академії правових наук України*. 2017. № 3(90). С. 36-50. URL: http://nbuv.gov.ua/UJRN/vapny_2017_3_5 (дата звернення 26.04.2026)

92. Питання Єдиного державного вебпорталу електронних послуг та Реєстру адміністративних послуг: Постанова Кабінету Міністрів України від 04.12.2019 № 1137. URL: https://zakon.rada.gov.ua/laws/show/1137-2019-%D0%BF#Text (дата звернення 26.04.2026)

93. Питання Міністерства цифрової трансформації України: Постанова Кабінету Міністрів України від 18.09.2019 № 856. URL: https://www.kmu.gov.ua/npas/pitannya-ministerstva-cifrovoyi-t180919 (дата звернення 26.04.2026)

94. Повідомлення про обробку персональних даних / Єдиний державний веб-портал електронних послуг «Дія». URL: https://diia.gov.ua/policy (дата звернення 26.04.2026)

95. Пороскун С. С. Адміністративні процедури в умовах цифровізації: баланс між управлінською ефективністю та правовою визначеністю. *Часопис Київського університету права*. 2025. № 4. С. 76-83. DOI: https://doi.org/10.36695/2219-5521.4.2025.12

96. Постанова Броварського міськрайонного суду Київської області від 09.04.2020 у справі № 361/1579/20. URL: https://reyestr.court.gov.ua (дата звернення 26.04.2026)

97. Похиленко І. С. Правове регулювання захисту персональних даних. *Наукові праці Київського авіаційного інституту. Серія: Юридичний вісник «Повітряне і космічне право»*. 2023. № 4(69). С. 94-99. DOI: https://doi.org/10.18372/2307-9061.69.18322

98. Правовий висновок Ради Європи щодо законопроєкту № 8153. URL: https://rm.coe.int/opinion-on-the-draft-law-of-ukraine-on-personal-data-protection-/1680ad38c2 (дата звернення 26.04.2026)

99. Про адміністративні послуги: Закон України від 06.09.2012 № 5203-VI. URL: https://zakon.rada.gov.ua/laws/show/5203-17#Text (дата звернення 26.04.2026)

100. Про адміністративну процедуру : Закон України від 17.02.2022 № 2073-IX. URL: https://zakon.rada.gov.ua/laws/show/2073-20#Text (дата звернення 26.04.2026)

101. Про введення воєнного стану в Україні: Указ Президента України від 24.02.2022 № 64/2022. URL: https://zakon.rada.gov.ua/laws/show/64/2022#Text (дата звернення 26.04.2026)

102. Про внесення змін до деяких законів України щодо діяльності Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних: Закон України від 13.05.2014 № 1262-VII. URL: https://zakon.rada.gov.ua/laws/show/1262-18 (дата звернення 26.04.2026)

103. Про внесення змін до деяких законів України щодо удосконалення порядку обробки та використання даних у державних реєстрах для військового обліку та набуття статусу ветерана війни під час дії воєнного стану: закон України від 16.01.2024 № 3549-IX. URL: https://zakon.rada.gov.ua/laws/show/3549-20#Text (дата звернення 26.04.2026)

104. Про внесення змін до деяких законодавчих актів України щодо удосконалення окремих питань мобілізації, військового обліку та проходження військової служби: Закон України від 11.04.2024 № 3633-IX. URL: https://zakon.rada.gov.ua/laws/show/3633-20#Text (дата звернення 26.04.2026)

105. Про внесення змін до постанов Кабінету Міністрів України від 8 вересня 2016 р. № 606 і від 4 грудня 2019 р. № 1137: Постанова КМУ від 01.10.2025 № 1244. URL: https://zakon.rada.gov.ua/laws/show/1244-2025-п#Text (дата звернення 26.04.2026)

106. Про внесення змін до постанови Кабінету Міністрів України від 8 вересня 2016 р. № 606 та визнання такими, що втратили чинність, деяких постанов Кабінету Міністрів України: постанова Кабінету Міністрів України від 17.01.2023 № 38. URL: https://zakon.rada.gov.ua/laws/show/38-2023-%D0%BF/ed20240412#Text (дата звернення 26.04.2026)

107. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення 26.04.2026)

108. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення 26.04.2026)

109. Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення 26.04.2026)

110. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення 26.04.2026)

111. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус: Закон України від 20.11.2012 № 5492-VI. URL: https://zakon.rada.gov.ua/laws/show/5492-17#Text (дата звернення 26.04.2026)

112. Про Єдину інформаційну систему соціальної сфери: Закон України від 18.09.2025 № 4607-IX. (набере чинності 27.05.2026). URL: https://zakon.rada.gov.ua/laws/show/4607-20#Text (дата звернення 26.04.2026)

113. Про запобігання корупції: Закон України від 14.10.2014 № 1700-VII. URL: https://zakon.rada.gov.ua/laws/show/1700-18#Text (дата звернення 26.04.2026)

114. Про затвердження документів у сфері захисту персональних даних: наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text (дата звернення 26.04.2026)

115. Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем: Постанова Кабінету Міністрів України від 29.03.2006 № 373. URL:

https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text (дата звернення 26.04.2026)

116. Про затвердження Порядку обробки та захисту персональних даних, володільцем яких є Міністерство цифрової трансформації України: наказ Мінцифри від 20.05.2020 № 72. URL: https://zakon.rada.gov.ua/laws/show/z0495-20#Text (дата звернення 26.04.2026)

117. Про затвердження Порядку обробки та захисту персональних даних, володільцем яких є Міністерство освіти і науки України: наказ МОН від 10.07.2023 № 836. URL: https://zakon.rada.gov.ua/laws/show/z1249-23 (дата звернення 26.04.2026)

118. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення 26.04.2026)

119. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення 26.04.2026)

120. Про Національну програму інформатизації: Закон України від 04.02.1998 № 74/98-ВР (втратив чинність). URL: https://zakon.rada.gov.ua/laws/show/74/98-вр#Text (дата звернення 26.04.2026)

121. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 26.04.2026)

122. Про особливості надання публічних (електронних публічних) послуг: Закон України від 15.07.2021 № 1689-IX. URL: https://zakon.rada.gov.ua/laws/show/1689-20#Text (дата звернення 26.04.2026)

123. Про особливості надання публічних (електронних публічних) послуг: Закон України від 15.07.2021 № 1689-IX. URL: https://zakon.rada.gov.ua/laws/show/1689-20#Text (дата звернення 26.04.2026)

124. Про правовий режим воєнного стану: Закон України від 12.05.2015 № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text (дата звернення 26.04.2026)

125. Про публічні електронні реєстри : Закон України від 18.11.2021 № 1907-IX. URL: https://zakon.rada.gov.ua/laws/show/1907-20#Text (дата звернення 26.04.2026)

126. Про схвалення Концепції розвитку електронного урядування в Україні: розпорядження КМУ від 13.12.2010 № 2250-р. URL: https://zakon.rada.gov.ua/laws/show/2250-2010-р#Text (дата звернення 26.04.2026)

127. Про центральні органи виконавчої влади: Закон України від 17.03.2011 № 3166-VI. URL: https://zakon.rada.gov.ua/laws/show/3166-17#Text (дата звернення 26.04.2026)

128. Проект Закону «Про захист персональних даних» : реєстр. № 8153 від 25.10.2022. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/40707 (дата звернення 26.04.2026)

129. Проект Закону «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації»: реєстр. № 6177 від 18.10.2021. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/27996 (дата звернення 26.04.2026)

130. Прозора робота з реєстрами: у системі «Трембіта» фіксуватимуть, хто і коли переглядав персональні дані українців / Міністерство цифрової трансформації України. 2023. URL: https://www.kmu.gov.ua/news/prozora-robota-z-reiestramy-u-systemi-trembita-fiksuvatymut-khto-i-koly-perehliadav-personalni-dani-ukraintsiv (дата звернення 26.04.2026)

131. Расторгуєва Н. Система органів державної влади, відповідальних за реалізацію інтеграції acquis communautaire в Україні. *Вісник Луганського ННІ ім. Е.О. Дідоренка.* 2024. № 4. С. 9-20. DOI: https://doi.org/10.32782/2786-9156.108.4.9-20

132. Регламент Європейського Парламенту і Ради (ЄС) 2024/1689 від 13.06.2024 про гармонізацію норм щодо штучного інтелекту (EU AI Act). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689 (дата звернення 26.04.2026)

133. Редзюк В., Дармостук Д. Цифрові платформи для надання державних послуг: досвід України та світу. *Публічне управління: концепції, парадигма, розвиток, удосконалення.* 2024. № 9. С. 168-175. DOI: https://doi.org/10.31470/2786-6246-2024-9-168-175

134. Різак М. В. Особливості адміністративно-правового забезпечення відносин обігу та обробки персональних даних в Україні. *Науковий вісник публічного та приватного права*. 2017. № 6(2). С. 118-121. URL: http://nbuv.gov.ua/UJRN/nvppp_2017_6(2)__23 (дата звернення 26.04.2026)

135. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20.01.2012 № 2-рп/2012. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12#Text (дата звернення 26.04.2026)

136. Рішення Конституційного Суду України у справі за конституційним поданням Уповноваженого Верховної Ради України з прав людини щодо відповідності Конституції України окремих положень абзацу першого пункту 40 розділу VI «Прикінцеві та перехідні положення» Бюджетного кодексу України від 11.10.2018 № 7-р/2018. URL: https://zakon.rada.gov.ua/laws/show/v007p710-18#Text (дата звернення 26.04.2026)

137. Рішення Конституційного Суду України у справі К. Г. Устименка від 30.10.1997 № 5-зп. URL: https://zakon.rada.gov.ua/laws/show/v005p710-97#Text (дата звернення 26.04.2026)

138. Рішення Сумського окружного адміністративного суду від 04.08.2022 у справі № 480/3676/22 (суддя О.О. Осіпова). Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/105583888

139. Розріз «Трембіти»: як працюють державні електронні реєстри. *Liga.net Projects.* 2024. URL: https://projects.liga.net/trembita (дата звернення 26.04.2026)

140. Руденко Л.Д.. Організаційно-правовий механізм цифровізації діяльності органів публічного адміністрування. *Академічні візії.* 2025. №40. URL: https://academy-vision.org/index.php/av/article/view/1725 (дата звернення 26.04.2026)

141. Рудниченко А.Ю. Актуальні питання правового регулювання штучного інтелекту в ЄС, Україні та США. *Аналітично-порівняльне правознавство.* 2025. Вип. 4, Том 1. С. 423-428. DOI: https://doi.org/10.24144/2788-6018.2025.04.1.65

142. Рябець К. О. Значення вебпорталу «Дія. Цифрова освіта» в публічному управлінні цифровою трансформацією. Науковий вісник: Державне управління. 2024. № 1 (15). С. 243-258. DOI: https://doi.org/10.32689/2618-0065-2024-1(15)-243-258

143. Рядінська В., Плугатар Т. Правове регулювання цифровізації публічного управління в Європейському Союзі. *Академічні візії.* 2025. № 39. DOI: https://doi.org/10.5281/zenodo.14869566

144. Clarifying "personal data" and the role of anonymisation in data protection law. *Computer Law & Security Review*. 2024. URL: https://www.sciencedirect.com/science/article/pii/S0267364923001425 (дата звернення 26.04.2026)

145. Савченко О. С. Систематизація наукових підходів до поняття «цифровізація у публічному управлінні». *Держава та регіони. Серія: Публічне управління і адміністрування*. 2022. № 2 (76). С. 72-76. DOI: https://doi.org/10.32840/1813-3401.2022.2.12

146. Світличний В.А. Захист персональних даних в умовах воєнного стану в Україні. *Право і безпека.* 2023. № 3 (90). С. 226-236. DOI: https://doi.org/10.32631/pb.2023.3.19

147. Семчук Н. О. Гармонізація кримінального законодавства України зі стандартами ЄС у сфері захисту персональних даних. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2026. Том 4, № 93. С. 193-199. DOI: https://doi.org/10.24144/2307-3322.2026.93.4.28

148. Середа І. Л. Персональні дані в умовах воєнного стану: конституційно-правові обмеження та гарантії. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Том 90. Ч. 1. С. 327-335. DOI: https://doi.org/10.24144/2307-3322.2025.90.1.43

149. Система електронної взаємодії державних електронних інформаційних ресурсів «Трембіта». *Вікіпедія.* URL: https://uk.wikipedia.org/wiki/Система_електронної_взаємодії_державних_електронних_інформаційних_ресурсів_«Трембіта» (дата звернення 26.04.2026)

150. Сорокіна Н., Філатов В. Цифровізація публічного управління в Україні: теоретичний аспект. *Аспекти публічного управління*. 2025. Том 13, № 1. С. 77-81. DOI: https://doi.org/10.15421/152509

151. Теремецький В. І. Загальна характеристика охорони бази персональних даних за законодавством України. *Підприємництво, господарство і право*. 2015. № 10. С. 3-5. URL: https://pgp-journal.kiev.ua/archive/2015/10_2015.pdf (дата звернення 26.04.2026)

152. Тимченко М. С. Розвиток сервісу «Дія» в умовах війни. *Публічне управління та регіональний розвиток*. 2022. № 17. С. 834-866. DOI: https://doi.org/10.34132/pard2022.17.09

153. Тур О. М. Практика е-урядування на місцевому рівні в Україні: соціально-економічний аспект. *Сталий розвиток економіки*. 2023. № 2 (47). С. 231-239. DOI: https://doi.org/10.32782/2308-1988/2023-47-33

154. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. Ратифікована Законом України від 16.09.2014 № 1678-VII. URL: https://zakon.rada.gov.ua/laws/show/984_011 (дата звернення 26.04.2026)

155. Хартія основних прав Європейського Союзу від 07.12.2000 (зі змінами від 12.12.2007). URL: https://eur-lex.europa.eu/legal-content/UK/TXT/?uri=CELEX:12012P/TXT (дата звернення 26.04.2026)

156. Хохлачова Ю. Є. та ін. Моделі цифрових платформ е-урядування та їх адаптація до реінжинірингу послуг. *Телекомунікаційні та інформаційні технології*. 2025. № 4 (89). С. 203-214. DOI: https://doi.org/10.31673/2412-4338.2025.048924

157. Худолєй Я.Г., Загребельна Н.А. Захист персональних даних у період дії в Україні правового режиму воєнного стану: загальнотеоретичні аспекти. *Legal Bulletin.* 2023. № 8. С. 75-82. DOI: https://doi.org/10.31732/2708-339X-2023-08-75-82

158. Цьоменко А. Персональні дані громадян та їхня класифікація в сучасній доктрині адміністративного права. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки*. 2023. № 1(53). С. 41-45. DOI: https://doi.org/10.17721/1728-2217.2023.53.41-45

159. Шелемеха О. О., Волох О. К. Адміністративно-правовий статус Міністерства цифрової трансформації України. *Адміністративно-правове забезпечення діяльності публічної адміністрації*: Матеріали XIX науково-практичного семінару (Київ, 20 червня 2024 року). С. 203-210.

160. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання та захисту прав і свобод людини і громадянина в Україні за 2023 рік. URL: https://ombudsman.gov.ua/report-2023/ (дата звернення 26.04.2026)

161. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини за 2024 рік. Розділ 9. Інформаційні права. URL: https://ombudsman.gov.ua/report-2024/informatsiini-prava (дата звернення 26.04.2026)

162. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини за 2023 рік. Розділ 9. Інформаційні права. URL: https://ombudsman.gov.ua/report-2023/rozdil-9-informatsiini-prava (дата звернення 26.04.2026)

163. Яворська О. С. Захист персональних даних у цифровому середовищі: досвід ЄС. *Юридичний науковий електронний журнал.* 2024. № 9. С. 117-119. DOI: https://doi.org/10.32782/2524-0374/2024-9/26

164. Яруліна Н. Технології е-урядування як запорука ефективної взаємодії держави та суспільства. *Інтеграція освіти, науки та бізнесу в сучасному середовищі: літні диспути* : тези доповідей І Міжнародної науково-практичної інтернет-конференції, м. Дніпро, 1-2 серпня 2019 р. С. 851–856.

165. Andrusyshyn B. I., Bilozorov Ie. V., Opolska N. M., Kupina,L. F., Tokarchuk O. V. Definition and Protection of Personal Data Peculiarities: Ukrainian and European Experience. *Informatologia*. 2022. № 55(1-2). pp. 136-148. DOI: https://doi.org/10.32914/i.55.1-2.11

166. Council of Europe. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. CETS No. 223. Strasbourg, 10 October 2018. URL: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (дата звернення 26.04.2026)

167. Council of the European Union. Conference on Accession to the European Union – Ukraine. Negotiating Framework. AD 9/24 CONF-UA 2/24. Brussels, 21 June 2024. URL: https://www.consilium.europa.eu/media/hzmfw1ji/public-ad00009en24.pdf (дата звернення 26.04.2026)

168. European Commission. First report on the application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680. COM(2022) 364. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022DC0364 (дата звернення 26.04.2026)

169. European Court of Human Rights (Grand Chamber). Case of Amann v. Switzerland. Application no. 27798/95. Judgment of 16 February 2000. URL: https://hudoc.echr.coe.int/eng?i=001-58497 (дата звернення 26.04.2026)

170. European Court of Human Rights (Grand Chamber). Case of S. and Marper v. the United Kingdom. Applications nos. 30562/04 and 30566/04.

Judgment of 4 December 2008. URL: https://hudoc.echr.coe.int/eng?i=001-90051 (дата звернення 26.04.2026)

171. European Court of Human Rights. Case of Leander v. Sweden. Application no. 9248/81. Judgment of 26 March 1987. URL: https://hudoc.echr.coe.int/eng?i=001-57519 (дата звернення 26.04.2026)

172. European Court of Human Rights. Case of M.K. v. France. Application no. 19522/09. Judgment of 18 April 2013. URL: https://hudoc.echr.coe.int/eng?i=001-118278 (дата звернення 26.04.2026)

173. Gellert R. Comparing definitions of data and information in data protection law and machine learning: A useful way forward to meaningfully regulate algorithms? *Regulation & Governance*. 2022. № 16(1). pp. 156-176. DOI: https://doi.org/10.1111/rego.12349

174. Gellert R. Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies. *International Data Privacy Law*. 2021. № 11(2). P. 196-208. DOI: https://doi.org/10.1093/idpl/ipaa023

175. Irti C. Personal Data, Non-personal Data, Anonymised Data, Pseudonymised Data, De-identified Data. *Privacy and Data Protection in Software Services*. 2021. pp. 49-57. DOI: https://doi.org/10.1007/978-981-16-3049-1_5

176. Negroponte, Nicholas. *Being Digital*. Knopf Doubleday Publishing Group, 1995. 272 p.

177. Parkinson B. Personal Data: Definition and Access (PhD thesis). 2018. University of Southampton. URL: https://eprints.soton.ac.uk/427140/ (дата звернення 26.04.2026)

178. Personal data non grata. *Юридична газета.* 2018. URL: https://yur-gazeta.com/golovna/personal-data-non-grata.html (дата звернення 26.04.2026)

179. Phillips M. International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR). *Human Genetics*. 2018. 137, 575-582. DOI: https://doi.org/10.1007/s00439-018-1919-7

180. 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 (General Data Protection Regulation). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 (дата звернення 26.04.2026)

181. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). *Official Journal of the European Union.* L 152, 3 June 2022. P. 1-44. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R0868 (дата звернення 26.04.2026)

182. Ruohonen J., Mickelsson S. Reflections on the Data Governance Act. *ArXiv preprint.* 2023. URL: https://arxiv.org/pdf/2302.09944 (дата звернення 26.04.2026)

183. Shpakovych O., Shevchuk O., Melotíková P. Data Protection in Ukraine and in the Czech Republic, a few Remarks on the Data Protection Authority. *European Studies – the Review of European law, Economics and Politics.* 2023. Vol. 10. No. 2. P. 221-245. DOI: https://doi.org/10.2478/eustu-2023-0019

184. UN Human Rights Council. Resolution 28/16: The right to privacy in the digital age (A/HRC/RES/28/16, 26 March 2015). URL: https://undocs.org/A/HRC/RES/28/16 (дата звернення 26.04.2026)

185. Walters R. Definitions Personal Data – Information. In: *Cybersecurity and Data Laws of the Commonwealth.* 2023. pp. 75-99. DOI: https://doi.org/10.1007/978-981-99-3935-0_3

186. Yeung K., Bygrave L. A. Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship. *Regulation & Governance*. 2022. № 16(1). pp. 137-155. DOI: https://doi.org/10.1111/rego.12401

ДОДАТКИ

Додаток А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Костюк Д. І. Адміністративні процедури обробки персональних даних у системах міжвідомчого електронного обміну. *Приватне право і підприємництво*. 2026. Вип. 26. С. 178–185. DOI: https://doi.org/10.32849/2409-9201.2026.26.19. URL: https://ppp-journal.kiev.ua/index.php/26-2026

2. Костюк Д. І. Нормативно-правове регулювання обробки персональних даних у публічних електронних реєстрах України. *Актуальні проблеми правознавства*. 2026. № 1 (45). С. 98–105. DOI: https://doi.org/10.35774/app2026.01.098. URL: https://appj.wunu.edu.ua/index.php/appj/article/view/2265

3. Костюк Д. І. Правовий статус платформи «Дія» як суб'єкта обробки персональних даних. *Журнал східноєвропейського права*. 2026. № 145. С. 321–328. DOI: https://doi.org/10.71404/2409-6415.145.36. URL: https://easternlaw.com.ua/wp-content/uploads/2026/04/kostiuk_145.pdf

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Костюк Д. І. Імплементація стандартів конвенції 108+ та GDPR в адміністративне законодавство України. *Україна в умовах реформування правової системи: сучасні реалії та міжнародний досвід*: матеріали IX Міжнародної науково-практичної конференції (м. Тернопіль, 2–3 травня 2025 р.). Тернопіль: ЗУНУ, 2025. С. 346–348. URL: https://confuf.wunu.edu.ua/index.php/confuf/article/view/1732/1711

2. Костюк Д. І. Наглядовий орган у сфері захисту персональних даних: стандарти незалежності та перспективи інституційної реформи в Україні. *Людина, суспільство, держава: актуальні питання правового регулювання взаємодії*: тези доп. учасників. II наук.-практ. конф. (Київ, 21 лист. 2025 р.).

Київ: 2025. С. 65–67. DOI: https://doi.org/10.71404/PPSS.2025.3.18. URL: https://library.pp-ss.pro/index.php/ndippsn_20251121/article/view/kostiuk/pdf

3. Костюк Д. І. Персональні дані як об’єкт адміністративно-правової охорони. *Актуальні проблеми приватного та публічного права* : матеріали VIII Міжнародної науково-практичної конференції присвяченої 97-річчю від дня народження члена-кореспондента НАПрН України, академіка Міжнародної кадрової академії, заслуженого діяча науки України, доктора юридичних наук, професора О. І. Процевського, Харків, 27 березня 2026 року. Харківський національний педагогічний університет імені Г. С. Сковороди, Україна. Видавництво: ХНПУ імені Г. С. Сковороди, 2026. С. 505–507.

Додаток Б

ЗАТВЕРДЖУЮ

Директор Науково-дослідного
Інституту публічної політики і
соціальних наук
доктор юридичних наук, професор

М. В. Завальний

«____» _____ 2026 р.

АКТ
про впровадження у науково-дослідну діяльність
Науково-дослідного інституту публічної політики і соціальних наук
результатів дисертації Костюка Дмитра Ігоровича
«Адміністративно-правове забезпечення захисту персональних даних в умовах цифровізації публічного управління»,
поданої на здобуття ступеня доктора філософії
в галузі знань 08 «Право» за спеціальністю 081 «Право»

Комісія у складі:
голова - директор Науково-дослідного інституту публічної політики і соціальних наук, доктор юридичних наук, професор Завальний Михайло Володимирович;
члени комісії:
- заступник директора Науково-дослідного інституту публічної політики і соціальних наук, кандидат юридичних наук, старший науковий співробітник Голубов Артем Євгенович;
- вчений секретар Науково-дослідного інституту публічної політики і соціальних наук, доктор юридичних наук, професор Кухарєв Олександр Євгенович,

Повідомляємо спеціалізовану вчену раду про те, що результати дисертації Костюка Дмитра Ігоровича «Адміністративно-правове забезпечення захисту персональних даних в умовах цифровізації публічного управління», поданої на здобуття ступеня доктора філософії в галузі знань 08 «Право» за спеціальністю 081 «Право», спрямовані на розкриття поняття та правової природи персональних даних як об'єкта адміністративно-правової охорони, визначення їх місця у системі об'єктів публічного суб'єктивного права та формулювання авторського визначення персональних даних у контексті цифровізації публічного управління, розгляд цифровізації публічного управління як чинника якісної трансформації правовідносин у

сфері захисту персональних даних, визначення нових типів правовідносин, що виникають унаслідок цифровізації, виявлення системних правових ризиків, пов'язаних із масштабною обробкою персональних даних у цифровому публічному управлінні, дослідження системи суб'єктів забезпечення захисту персональних даних у сфері публічного управління, визначення їх правового статусу, повноважень та особливостей взаємодії, розкриття змісту адміністративних процедур обробки персональних даних у системах цифрового публічного управління та визначення вимог до їх правового регулювання, аналіз міжнародно-правових стандартів захисту персональних даних, визначення механізмів їх впливу на національне адміністративне законодавство та виявлення системних прогалин імплементації цих стандартів в Україні тощо використовуються Науково-дослідним інститутом публічної політики і соціальних наук під час розроблення пропозицій та рекомендацій щодо удосконалення чинного національного законодавства.

Пропозиції та рекомендації щодо удосконалення законодавства і практики його застосування у сфері забезпечення захисту персональних даних в умовах цифровізації публічного управління, зокрема щодо реформування адміністративної відповідальності за порушення законодавства про захист персональних даних, удосконалення процедурного механізму притягнення до відповідальності, вирішення правових проблем захисту персональних даних у системах електронних публічних послуг, а також гармонізації адміністративного законодавства України у сфері захисту персональних даних із правом ЄС, взято за основу для подальшої законопроєктної роботи.

Результати дисертаційного дослідження Костюка Дмитра Ігоровича «Адміністративно-правове забезпечення захисту персональних даних в умовах цифровізації публічного управління», поданого на здобуття ступеня доктора філософії в галузі знань 08 «Право» за спеціальністю 081 «Право», мають належний теоретичний рівень і практичну спрямованість та сприятимуть підвищенню якості національного законодавства у сфері адміністративно-правового забезпечення захисту персональних даних в умовах цифровізації публічного управління.

Члени комісії:

А. Є. Голубов

О. Є. Кухарєв