Національний технічний університет «Дніпровська політехніка»
МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

Кваліфікаційна наукова праця
на правах рукопису

Онищенко Владислав Вячеславович

УДК 342.9+347.95

ДИСЕРТАЦІЯ

Нормативно-правове регулювання здійснення контролю за обробкою персональних даних

Подається на здобуття наукового ступеня **доктора філософії**
зі спеціальності 081 «Право»

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

_____ В.В. Онищенко

Науковий керівник – **Потіп Микола Миколайович**
доктор юридичних наук, професор

Дніпро – 2026

Анотація

Онищенко В.В. Нормативно-правове регулювання здійснення контролю за обробкою персональних даних. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття освітньо-наукового ступеня доктора філософії за спеціальністю 081 «Право». – Національний технічний університет «Дніпровська політехніка», Дніпро, 2026.

У дисертації проведено комплексне наукове дослідження інституту контролю за обробкою персональних даних в Україні.

Наукова новизна одержаних результатів полягає в тому, що дисертація є одним із перших комплексних наукових досліджень адміністративно-правового механізму контролю за обробкою персональних даних в Україні, визначення практичних проблем правозастосовної практики у цій сфері, а також розробки науково обґрунтованих пропозицій щодо їх усунення. У результаті дослідження сформульовано низку нових наукових положень, рекомендацій і висновків, зокрема:

вперше:

- запропоновано авторське визначення системи контролю за обробкою персональних даних як сукупності взаємопов’язаних і взаємодоповнювальних рівнів контролюючого впливу – загального регулятора, секторальних державних регуляторів, органів професійного самоврядування, етичних органів саморегулювання та внутрішнього самоконтролю володільця, що утворюють п’ятирівневу типологію суб’єктів, побудовану за критерієм природи суб’єкта та юридичної сили його рішень;

- обґрунтовано концепцію сферозалежного (секторального) контролю за обробкою персональних даних, відповідно до якої конфігурація контролю – коло суб’єктів, обсяг повноважень і застосовні форми – визначається сферою суспільних відносин, у межах якої здійснюється обробка, а компетенція секторальних суб’єктів щодо персональних даних має похідний характер і

виникає внаслідок перетину спеціальних правових режимів зі сферою персональних даних;

- доведено концептуальну некоректність кваліфікації судів як «суб'єктів контролю» за законодавством про захист персональних даних та запропоновано вживати щодо судів термін «суб'єкт судового захисту прав у сфері обробки персональних даних», що усуває концептуальну колізію між функціями контролю і правосуддя;

- виявлено нормативну неузгодженість між законодавчою категорією «спеціальних персональних даних» (стаття 7 Закону України «Про захист персональних даних») та підзаконною категорією «даних, що становлять підвищений ризик», а також обґрунтовано існування самостійної прогалини правового регулювання щодо статусу інформації про померлу особу;

удосконалено:

- підходи до класифікації контролю за обробкою персональних даних шляхом розмежування трьох самостійних класифікаційних площин – виду контролю, форми контролю та сфери суспільних відносин;

- систему підстав обробки персональних даних шляхом їх структурування у дві групи залежно від правової природи – підстави, що ґрунтуються на волевиявленні суб'єкта персональних даних, і підстави, що виникають із закону або об'єктивних обставин;

- розуміння повноважень Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних шляхом їх класифікації за функціональним призначенням;

дістали подальшої розробки:

- історико-правова реконструкція генези інституту контролю за обробкою персональних даних в Україні як зумовленого євроінтеграційними чинниками процесу;

- методологія здійснення нагляду за обробкою персональних даних шляхом обґрунтування необхідності переходу від перевірки окремих операцій обробки до системного аудиту архітектури систем штучного інтелекту та

розвитку технічної спроможності наглядового органу для незалежного тестування алгоритмічних систем;

сформульовано пропозиції щодо вдосконалення правового регулювання контролю за обробкою персональних даних. Зокрема розроблено конкретні законодавчі пропозиції у формі модельних норм змін до Закону України «Про охорону дитинства» та Закону України «Про медіа» (Додаток В), що є безпосереднім нормативним продуктом дисертаційного дослідження.

Встановлено наявність суттєвого дисбалансу між кількістю звернень щодо порушень та фактичними заходами реагування, що свідчить про обмежену ефективність існуючої моделі правозастосування. Досліджено виклики, зумовлені умовами воєнного стану, зокрема ризики кібератак, несанкціонованого поширення інформації та використання персональних даних у контексті інформаційної війни.

Проведено порівняльний аналіз із європейськими підходами до функціонування наглядових органів, що передбачають ширші повноваження щодо застосування санкцій. Обґрунтовано необхідність модернізації системи захисту персональних даних в Україні шляхом удосконалення механізмів юридичної відповідальності, розширення повноважень наглядового органу та підвищення його інституційної спроможності, що є необхідною умовою забезпечення ефективного захисту права на приватність в обставинах сучасних викликів.

Встановлено, що ключовими нормативними прогалинами є відсутність принципу підзвітності, обов’язкової оцінки впливу на захист даних (DPIA) та вимоги *privacy by design* як юридично обов’язкового стандарту, а також відсутність права наглядового органу на самостійне накладення адміністративного штрафу, що структурно послаблює превентивну функцію контролю.

У зв’язку з цим обґрунтовано комплекс взаємопов’язаних законодавчих заходів, зокрема завершення переходу від моделі Уповноваженого Верховної Ради України з прав людини до спеціалізованого незалежного органу захисту

персональних даних, з наділенням його повним обсягом контрольних повноважень за статтею 58 Регламенту (ЄС) 2016/679, включно з правом самостійного накладення адміністративного стягнення.

Запропоновано законодавче закріплення принципу підзвітності та обов'язкової процедури оцінки впливу на захист даних; запровадження вимоги *privacy by design* як юридично обов'язкового стандарту; диференціація санкцій пропорційно масштабу і тривалості порушення замість чинних фіксованих розмірів штрафів.

Ключові слова: адміністрування, адміністративні процедури, виконавче провадження, відповідальність, державний контроль, конфіденційна інформація, кібербезпека, захист інформації, пацієнт, персональні дані, правоохоронні органи, правопорушення, права людини, публічний інтерес, розмежування відповідальності, соціальна інформація, штучний інтелект.

Summary

Onyshchenko V.V. Normative and legal regulation of control over the processing of personal data. – Qualifying scientific work submitted as a manuscript.

Dissertation for obtaining the Doctor of Philosophy degree in Specialty 081 «Law». – Dnipro University of Technology, Dnipro, 2026.

The dissertation presents a comprehensive analysis of the development and current state of the legal framework governing personal data protection in Ukraine within the context of the evolution of constitutional guarantees of the right to respect for private life.

The scientific novelty of the obtained results lies in the fact that the dissertation is one of the first comprehensive studies of the administrative and legal framework governing the supervision of personal data processing in Ukraine. As a result of the study, a number of new scientific provisions, recommendations, and conclusions have been formulated, in particular:

For the first time:

an original definition of the system of supervision over personal data processing has been proposed as a set of interconnected and mutually complementary levels of supervisory oversight, comprising the general supervisory authority, sector-specific public regulators, professional self-governing bodies, ethical self-regulatory bodies, and the internal compliance mechanisms of the data controller. Together, these constitute a five-level typology of supervisory entities based on their legal status and the binding force of their decisions;

the concept of sector-specific supervision over personal data processing has been substantiated, according to which the configuration of the supervisory framework – including the competent supervisory entities, the scope of their powers, and the applicable forms of supervision – is determined by the specific sector in which the processing takes place, while the competence of sector-specific supervisory entities with regard to personal data is derivative in nature and arises from the interaction between sector-specific legal regimes and the personal data protection regime;

the conceptual incorrectness of classifying courts as supervisory entities under personal data protection legislation has been demonstrated, and it has been proposed that courts should instead be regarded as entities responsible for judicial protection of rights in the field of personal data processing, thereby eliminating the conceptual inconsistency between supervisory functions and the administration of justice;

a regulatory inconsistency has been identified between the statutory category of special categories of personal data (Article 7 of the Law of Ukraine «On Personal Data Protection») and the subordinate regulatory category of personal data posing a particular risk to the rights and freedoms of data subjects, and the dissertation substantiates the existence of a distinct legislative gap concerning the legal status of information relating to deceased persons.

Improved:

approaches to the classification of personal data processing supervision through distinguishing three independent analytical dimensions: the type of

supervision, the form of supervision, and the sector of social relations in which personal data are processed;

the system of legal bases for personal data processing by classifying them into two categories according to their legal nature: legal bases founded upon the will of the data subject, and legal bases arising directly from statutory provisions or objective legal circumstances;

the understanding of the powers of the Ukrainian Parliament Commissioner for Human Rights in the field of personal data protection by classifying such powers according to their functional purpose.

Further developed:

the historical and legal reconstruction of the genesis of the institution of supervision over personal data processing in Ukraine as a process driven by European integration;

the methodology for the supervision of personal data processing through substantiating the need to shift from reviewing individual processing operations to systemic audits of artificial intelligence system architectures, as well as strengthening the technical capacity of the supervisory authority to independently test algorithmic systems;

scientific proposals for improving the legal regulation of supervision over personal data processing. In particular, specific model legislative amendments to the Law of Ukraine «On Child Protection» and the Law of Ukraine «On Media» were developed (Appendix B), constituting a direct normative outcome of the dissertation research.

A significant imbalance between the number of complaints alleging personal data protection violations and the actual enforcement measures undertaken has been identified, demonstrating the limited effectiveness of the current enforcement model. The thesis also examines the challenges arising under martial law, including the risks of cyberattacks, unauthorised disclosure of information, and the use of personal data in the context of information warfare.

A comparative analysis of European approaches to the functioning of data protection supervisory authorities has been conducted, highlighting their broader investigative, corrective and enforcement powers. The thesis substantiates the need to modernise Ukraine's personal data protection framework by improving legal liability mechanisms, strengthening the powers of the supervisory authority, and enhancing its institutional capacity as a prerequisite for ensuring the effective protection of the right to privacy in the face of contemporary challenges.

The research establishes that the principal regulatory gaps in the Ukrainian personal data protection framework include the absence of the accountability principle, the mandatory requirement to carry out a Data Protection Impact Assessment (DPIA), and the legal obligation to implement the *privacy by design* principle, as well as the lack of competence of the supervisory authority to impose administrative fines directly, which structurally weakens the preventive function of regulatory oversight.

In this regard, the thesis substantiates a comprehensive package of interrelated legislative reforms, including the completion of the transition from the current model, under which supervisory functions are exercised by the Ukrainian Parliament Commissioner for Human Rights, to an independent specialised data protection authority in accordance with Draft Law № 6177. Such an authority should be vested with the full range of supervisory powers provided for in Article 58 of Regulation (EU) 2016/679 (General Data Protection Regulation)**,** including the power to impose administrative fines independently.

Furthermore, the thesis proposes the legislative incorporation of the accountability principle, the introduction of a mandatory Data Protection Impact Assessment (DPIA), the establishment of *privacy by design* as a legally binding requirement, and the replacement of the current fixed administrative fines with a proportionate sanctions regime based on the gravity, scale, and duration of the infringement.

Keywords: public administration; administrative procedures; enforcement proceedings; legal liability; state supervision; confidential information;

cybersecurity; information protection; patient; personal data; law enforcement authorities; administrative offence; human rights; public interest; allocation of liability; social information; artificial intelligence.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ:

1. Онищенко В.В. Право дитини на приватність у діяльності медіа: співвідношення свободи вираження поглядів та принципу забезпечення якнайкращих інтересів дитини. Правові новели. 2025. Випуск № 27. С. 401-411 URL.: https://legalnovels.in.ua/journal/27_2025/27_2025.pdf

2. Онищенко В.В. Контроль за обробкою персональних даних та адміністративна відповідальність за порушення законодавства про захист персональних даних в умовах війни. Юридичний науковий електронний журнал. 2025. №12. С. 524-527

3. Онищенко В.В. Проблемні аспекти інформаційного законодавства України: поширення інформації про померлого. Юридичний науковий електронний журнал. 2023. №6. С. 674-677

4. Онищенко В.В. Трансформація контролю за обробкою персональних даних в умовах застосування штучного інтелекту : International scientific conference. Riga, Latvia : Baltija Publishing, 2026. С. 276-280

5. Потіп М. М., Онищенко В. В. Обробка персональних даних в умовах воєнного стану. Молодь: наука та інновації : матеріали XII Міжнародної науково-технічної конференції студентів, аспірантів та молодих вчених. Дніпро : НТУ «Дніпровська політехніка», 2024. С. 171–172.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

Уповноважений Верховної Ради України з прав людини	Уповноважений, Омбудсман
Секретаріат Уповноваженого Верховної Ради України з прав людини	Офіс Омбудсмана, Секретаріат Уповноваженого
Європейський Суд з прав людини	ЄСПЛ
Суд справедливості Європейського Союзу	Суд ЄС, CJEU
Європейський Союз	ЄС
Національний орган захисту даних (Data Protection Authorities)	Наглядовий орган, DPA
Неурядова організація	НУО
Організація Об’єднаних Націй	ООН
Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв’язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)	GDPR, Регламент (ЄС) 2016/679
Конвенція № 108 про захист фізичних осіб у зв’язку з автоматизованою обробкою персональних даних 1981 р.	Конвенція № 108

Конвенція № 108 про захист фізичних осіб у зв’язку з автоматизованою обробкою персональних даних, зі змінами, внесеними Протоколом CETS № 223	Конвенція № 108+
Рамкова конвенція Ради Європи про штучний інтелект та права людини, демократію і верховенство права (CETS № 225)	Конвенція про штучний інтелект
Регламент (ЄС) 2024/1689 Європейського Парламенту і Ради від 13.06.2024 р., що встановлює гармонізовані правила щодо штучного інтелекту	Акт про штучний інтелект
Проєкт Закону про захист персональних даних (номер: 8153; дата реєстрації: від 25.10.2022; Євроінтеграційний)	Проєкт Закону України від 25.10.2022 року № 8153
Проект Закону про Національну комісію з питань захисту персональних даних та доступу до публічної інформації (номер: 6177; дата реєстрації: від 18.10.2021)	Проєкт Закону України від 18.10.2021 року № 6177

ВСТУП

Актуальність теми. Стрімка цифровізація суспільних відносин, широке впровадження технологій штучного інтелекту, розвиток хмарних сервісів та автоматизованого прийняття рішень істотно збільшили масштаби обробки персональних даних і водночас актуалізували питання забезпечення ефективного державного контролю за дотриманням законодавства у цій сфері. За сучасних умов персональні дані стали одним із ключових інформаційних ресурсів, а їх неправомірне використання створює ризики порушення права на приватність, дискримінації, маніпулювання поведінкою особи, кіберзлочинності та інших загроз правам людини.

Формування інституту захисту персональних даних в Україні пов’язане з розвитком конституційних прав і свобод людини та громадянина, і насамперед – із правом на повагу до приватного життя.

Сучасний етап розвитку правової системи України характеризується посиленням уваги до забезпечення фундаментальних прав і свобод людини, серед яких ключове місце посідає право на повагу до приватного життя. В умовах цифровізації суспільства та активного обігу інформації питання захисту персональних даних набуває особливої актуальності, трансформуючись із суто технічної категорії у фундаментальний правовий інститут.

Європейський вектор розвитку України зумовлює необхідність гармонізації національного законодавства із міжнародними стандартами, що, у свою чергу, актуалізує потребу ґрунтовного наукового аналізу та визначення ступеню ефективності діючих механізмів захисту персональних даних.

Особливої ваги питання ефективності контролю набуває в умовах поширення технологій штучного інтелекту та автоматизованого прийняття рішень, які створюють нові ризики для прав особи, що не охоплюються в повному обсязі чинною моделлю нагляду.

Додатковим чинником актуальності є умови воєнного стану, за яких ризики неправомірного використання персональних даних, кібератак і несанкціонованого поширення інформації не лише суттєво зростають, але й може зумовлювати тяжкі наслідки як для конкретної особи, так і національної безпеки. За цих обставин традиційне розуміння контролю за обробкою персональних даних як різновиду адміністративного нагляду виявляється недостатнім і вимагає перегляду на користь ризик-орієнтованої моделі гарантування інформаційних прав людини.

Попри формальне наближення законодавства України до стандартів GDPR, статистика за 2022–2024 роки засвідчує парадоксальну тенденцію: кількість звернень громадян щодо порушень захисту персональних даних зросла на 67%, тоді як кількість протоколів про адміністративні правопорушення за статтею 188-39 Кодексу України про адміністративні правопорушення скоротилася більш ніж на 77 відсотків. При цьому, лише 20–23% порушених справ завершилися накладенням реального стягнення.

Ця диспропорція не є ситуативною – вона відображає структурну неспроможність чинної моделі контролю реагувати на порушення в умовах цифровізації. Її причину не можна пояснити ані недостатністю законодавчої бази, ані браком інституційної волі.

Вона є наслідком концептуальної помилки в основі системи: контроль за обробкою персональних даних у вітчизняній моделі побудований за логікою класичного адміністративного нагляду, що передбачає реагування на вже вчинені порушення через державний примус. Ця логіка принципово не відповідає природі інформаційних відносин, де шкода від незаконної обробки є негайною, часто непоправною і такою, що виникає ще до необхідності суб’єкта персональних даних направляти звернення до наглядового органу.

Питання захисту персональних даних неодноразово ставали предметом наукових досліджень як вітчизняних, так і зарубіжних учених.

Проблематика обробки персональних даних, їх місця в системі забезпечення приватності фізичних осіб є предметом сталого наукового

інтересу вітчизняної юридичної науки. Значний внесок у розробку загальнотеоретичних і конституційно-правових засад обробки персональних даних, а також здійснення контролю за обробкою персональних даних, здійснили О.Г. Рогова, О.А. Баранова, В.М. Брижко, Ю.Є. Максименко.

У міжнародній доктрині питання приватності та захисту персональних даних досліджували Х. Хейманс, Г. Гонсалес Фустер, Л. А. Байгрейв, А. Рувруа, І. Пулле, А. Кавукян, С. Тейлор, М. Е. Абрамс.

Окрему групу наукових досліджень становлять праці, присвячені захисту персональних даних у зв'язку із запровадженням систем штучного інтелекту, які досліджували В. М. Фурашев, С. О. Дорогих, Ю. В. Деркаченко, Б. Д. Леонов, Д. В. Швець, Л. В. Куцак., А. О. Гачкевич, Н. А. Загребельна, І.М. Берназюк, О. М. Гумін, І. В. Басиста, Ж. В. Удовенко, М. А. Кулинич.

Жодна з цих концепцій не була застосована до аналізу української моделі контролю. Крім того, у наявних наукових працях проблематика контролю за обробкою персональних даних досліджується переважно фрагментарно – через опис окремих повноважень наглядового органу, порівняння окремих норм або огляд законодавства – без формування цілісної теоретико-методологічної концепції контролю.

Поза межами комплексного аналізу залишаються причинно-наслідкові зв'язки неефективності контролю, практика Суду Справедливості ЄС, а також виклики штучного інтелекту для самої моделі нагляду.

Центральна дослідницька прогалина, на усунення якої спрямована ця дисертація, полягає у відсутності наукової концепції, яка пояснювала б, чому контроль за обробкою персональних даних є особливим видом публічного контролю, що не може бути зведений до традиційних адміністративно-наглядових механізмів державного нагляду (контролю), і яка пропонувала б теоретичну модель, придатну для переходу від формально-адміністративної до ризик-орієнтованої моделі гарантування цифрових прав.

Зв'язок роботи з науковими програмами, планами, темами. Виконання дисертації корелюється із напрямами зобов'язань України,

передбаченими переговорною рамкою Європейського Союзу, схваленою рішенням Ради Європейського Союзу від 21 червня 2024 року, за кластером 1 «Основи процесу вступу до ЄС» та виконано відповідно до Дорожньої карти з питань верховенства права, Дорожньої карти з питань реформи державного управління, Дорожньої карти з питань функціонування демократичних інституцій, схвалених розпорядженнями від 14 травня 2025 року № 475-р, а також планів і пріоритетних напрямів наукових досліджень у галузі права.

Робота узгоджується з Перспективними напрямами дисертаційних досліджень за спеціальністю 081 «Право» і виконана в межах наукової теми кафедрі цивільного, господарського та екологічного права Навчально-наукового інституту гуманітарних та соціальних наук Національного технічного університету «Дніпровська політехніка». Тему дисертації затверджено Вченою радою Національного технічного університету «Дніпровська політехніка» (протокол № 11 від «29» листопада 2022 р.).

Мета дослідження і завдання дослідження. *Мета роботи* полягає у комплексному теоретико-правовому аналізі інституту контролю за обробкою персональних даних в Україні, визначенні поняття, видів і форм такого контролю, встановленні правового статусу та повноважень суб'єктів контролю, виявленні системних проблем механізму відповідальності за порушення законодавства у відповідній сфері, а також у розробленні науково обґрунтованих пропозицій щодо вдосконалення нормативно-правового регулювання та підвищення ефективності системи контролю за обробкою персональних даних в Україні з урахуванням міжнародних стандартів і зарубіжного досвіду.

Для досягнення визначеної мети поставлено такі завдання:

– дослідити та визначити поняття, сутність та критерії відмежування персональних даних від суміжних правових категорій;

– визначити правовий режим персональних даних і співвідношення законодавчого та підзаконного регулювання у цій частині;

– охарактеризувати систему принципів і підстав обробки персональних даних за законодавством України у порівнянні з вимогами GDPR;

– обґрунтувати концепцію контролю за обробкою персональних даних як особливого виду публічного контролю та визначити його місце в системі адміністративного права;

– розкрити поняття, види і форми контролю та запропонувати їх наукову класифікацію;

– проаналізувати систему суб'єктів контролю в Україні, встановити обсяг і межі їх повноважень та обґрунтувати правову природу судової діяльності у цій сфері;

– встановити систему видів юридичної відповідальності за порушення законодавства про обробку персональних даних і виявити проблеми правозастосовної практики на підставі статистичного аналізу;

– проаналізувати зарубіжний досвід контролю у моделях ЄС, США і КНР, а також практику Європейського суду з прав людини і Суду ЄС;

– виявити виклики технологій штучного інтелекту для системи контролю і визначити нові повноваження наглядового органу;

– запропонувати організаційні та нормативно-правові напрями забезпечення ефективності контролю, у тому числі конкретні модельні норми змін до законодавства України.

Об'єктом дослідження є суспільні відносини, що виникають у сфері організації та здійснення контролю за дотриманням законодавства про обробку персональних даних в Україні.

Предметом дослідження є нормативно-правове регулювання здійснення контролю за обробкою персональних даних.

Методи дослідження. Методологічний інструментарій дослідження обраного напряму включає формально-юридичний метод – для аналізу норм Закону України «Про захист персональних даних», Кодексу України про адміністративні правопорушення і GDPR (підрозділи 1.1., 1.3.), порівняльно-

правовий метод – для зіставлення моделей ЄС, США і КНР за єдиною системою критеріїв (підрозділ 3.1).

Також використано системно-структурний метод – не лише в контексті розгляду об’єкта як цілісної множини елементів, але й для побудови авторської моделі причинно-наслідкових зв’язків між нормативним дефіцитом, інституційною слабкістю і низькою санкційною ефективністю (підрозділи 1.2., 1.3.).

Поміж спеціально-юридичних методів застосовано історико-правовий метод, що використовується для вивчення еволюції правових інститутів в динаміці у сфері контролю за обробкою та захистом персональних даних, у тому числі в умовах воєнного стану (підрозділи 2.2, 3.3.).

На рівні емпіричного аналізу здійснено: аналіз судових рішень за статтями 188-39, 188-40 Кодексу України про адміністративні правопорушення, які знаходяться у відкритому доступі (на підставі моніторингу Єдиного державного реєстру судових рішень виявлено 167 рішень протягом 2022-2025 рр.); аналіз щорічних доповідей Уповноваженого за 2013–2025 роки; аналіз діяльності наглядових органів із персональних даних відповідно GDPR.

Нормативну основу дослідження становлять Конституція України, міжнародні правові акти, зокрема Конвенція Ради Європи про захист фізичних осіб у зв’язку з автоматизованою обробкою персональних даних, Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв’язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних), Директива (ЄС) 2016/680, закони України – насамперед Закон України «Про захист персональних даних», Закон України «Про інформацію», Закон України «Про Уповноваженого Верховної Ради України з прав людини», Кодекс України про адміністративні правопорушення, акти Президента України та Кабінету Міністрів України, а також інші підзаконні нормативно-правові акти з питань обробки та захисту

персональних даних. Використано міжнародні правові стандарти, практику Європейського суду з прав людини та Суду справедливості Європейського Союзу, а також законодавство окремих зарубіжних держав-членів Європейського Союзу, США та Китайської Народної Республіки.

Емпіричну базу дослідження становлять статистичні дані щорічних доповідей Уповноваженого Верховної Ради України з прав людини, матеріали Єдиного державного реєстру судових рішень України (систематизований аналіз рішень за статтями 188-39 та 188-40 Кодексу України про адміністративні правопорушення), рішення Європейського суду з прав людини і Суду Справедливості Європейського Союзу, рішення і керівні настанови європейських наглядових органів і Європейської ради із захисту даних, а також рішення національних наглядових органів окремих зарубіжних держав.

Наукова новизна одержаних результатів полягає в тому, що дисертація є одним із перших комплексних наукових досліджень, присвячених нормативно-правовому регулюванню здійснення контролю за обробкою персональних даних в Україні. У роботі комплексно досліджено теоретико-правові та організаційно-правові засади здійснення такого контролю, виявлено проблеми чинного нормативного регулювання та практики його реалізації, а також розроблено науково обґрунтовані пропозиції щодо вдосконалення законодавства й механізму здійснення контролю за дотриманням законодавства у сфері обробки персональних даних. У результаті дослідження сформульовано низку нових наукових положень, рекомендацій і висновків, зокрема:

уперше:

- запропоновано авторське визначення системи контролю за обробкою персональних даних як сукупності взаємопов’язаних і взаємодоповнювальних рівнів контролюючого впливу – загального регулятора, секторальних державних регуляторів, органів професійного самоврядування, етичних органів саморегулювання та внутрішнього самоконтролю володільця, – що

утворюють п’ятирівневу типологію суб’єктів, побудовану за критерієм природи суб’єкта та юридичної сили його рішень;

- обґрунтовано концепцію сферозалежного (секторального) контролю за обробкою персональних даних, відповідно до якої конфігурація контролю – коло суб’єктів, обсяг повноважень і застосовні форми – визначається сферою суспільних відносин, у межах якої здійснюється обробка, а компетенція секторальних суб’єктів щодо персональних даних має похідний характер і виникає внаслідок перетину спеціальних правових режимів зі сферою персональних даних;

- доведено концептуальну некоректність кваліфікації судів як «суб’єктів контролю» за законодавством про захист персональних даних та запропоновано вживати щодо судів термін «суб’єкт судового захисту прав у сфері обробки персональних даних», що точніше відображає правову природу судової діяльності й усуває концептуальну колізію між функціями контролю і правосуддя;

удосконалено:

- підходи до класифікації контролю за обробкою персональних даних шляхом розмежування трьох самостійних класифікаційних площин – виду контролю, форми контролю та сфери суспільних відносин – які в науковій літературі нерідко змішуються;

- систему підстав обробки персональних даних шляхом їх структурування у дві групи залежно від правової природи: підстави, що ґрунтуються на волевиявленні суб’єкта персональних даних, і підстави, що виникають із закону або об’єктивних обставин, незалежних від такого волевиявлення;

- розуміння повноважень Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних шляхом їх класифікації за функціональним призначенням;

дістали подальшої розробки:

- методологія здійснення нагляду за обробкою персональних даних – шляхом обґрунтування необхідності переходу від перевірки окремих операцій обробки до системного аудиту архітектури систем штучного інтелекту та розвитку технічної спроможності наглядового органу для незалежного тестування алгоритмічних систем;

- сформульовано пропозиції щодо вдосконалення правового регулювання контролю за обробкою персональних даних. Зокрема, розроблено конкретні законодавчі пропозиції у формі модельних норм змін до Закону України «Про охорону дитинства» та Закону України «Про медіа» (Додаток В), що є безпосереднім нормативним продуктом дисертаційного дослідження.

Практичне значення одержаних результатів полягає в тому, що викладені у дисертації пропозиції та зроблені висновки можуть використовуватися у:

- *науково-дослідній діяльності* – для розробки у подальшому теоретичних та прикладних питань адміністративно-правового механізму контролю за обробкою персональних даних, зокрема в частині трансформації методології нагляду та контролю в умовах поширення технологій штучного інтелекту;

- *правотворчій діяльності* – для вдосконалення Закону України «Про захист персональних даних» і Кодексу України про адміністративні правопорушення на основі розроблених у дисертації модельних норм, а також для підготовки законопроєкту про внесення змін до Закону України «Про медіа» та Закону України «Про охорону дитинства» щодо тесту пропорційності поширення персональних даних дитини;

- *практичній діяльності* – для підвищення ефективності контролю за додержанням законодавства про захист персональних даних;

- *освітньому процесі* – під час написання підручників, навчальних посібників, методичних матеріалів, викладання навчальних дисциплін:

«Конституційне право», «Інформаційне право», «Адміністративне право і процес».

Особистий внесок здобувача. Дисертація є результатом самостійних наукових досліджень здобувача. Сформульовані в ній теоретичні положення, висновки та пропозиції одержані здобувачем особисто внаслідок самостійного опрацювання нормативно-правових джерел, матеріалів правозастосовної практики та наукової літератури з питань контролю за обробкою персональних даних. Використання наукових здобутків інших авторів супроводжується посиланнями на відповідні джерела.

Тези наукової доповіді, опубліковані у співавторстві з М. М. Потіпом, відображають результат спільного дослідження, при цьому особисто здобувачем здійснено аналіз правових підстав обробки та обсягу персональних даних в умовах воєнного стану за статтею 11 Закону України «Про захист персональних даних» та оцінку положень проєкту Закону України від 25.10.2022 року № 8153.

Апробація результатів дослідження. Результати дослідження, його основні висновки та рекомендації оприлюднені на 2 науково-практичних конференціях, а саме: «Міжнародна науково-технічна конференція студентів, аспірантів та молодих вчених» 2024, (м. Дніпро, 2024); «International scientific conference» 2026, (Latvia, Riga, 2026).

Публікації. Основні результати наукового дослідження опубліковано у 5 працях, з-поміж них 3 наукових статей, що опубліковані у фахових наукових виданнях України і 2 публікації, які додатково відображають наукові результати дисертації, у збірниках тез доповідей на науково-практичних конференціях.

Структура та обсяг дисертації. Дисертація складається з вступу, трьох розділів, логічно об’єднаних у вісім підрозділів, висновків, списку використаних джерел та додатків. Загальний обсяг дисертації становить 255 сторінок, з них основного тексту 209 сторінок. Список використаних джерел налічує 204 найменування і займає 25 сторінок.

Розділ 1. Обробка персональних даних: теоретико-правова характеристика

1.1. Персонільні дані: поняття, сутність, відмежування від суміжних правових категорій

Правове регулювання обробки персональних даних ґрунтується насамперед на визначенні поняття «персональні дані», з'ясуванні їх юридичної природи, сутнісних ознак та критеріїв відмежування від суміжних правових категорій. Саме від правильного розуміння змісту цієї категорії залежить визначення меж дії законодавства про захист персональних даних, встановлення правового режиму відповідної інформації, а також окреслення обсягу прав і обов'язків суб'єктів правовідносин у сфері її обробки.

Окремі аспекти правового регулювання обробки персональних даних аналізуються у роботах О.Г. Рогової [1], М.М. Потіпа [2], О.А. Баранова [3], В.М. Брижка [4], Ю.Є. Максименка [5, с. 236]. У міжнародній доктрині Х. Хейманс [6, с. 133-134] розробив концепцію ЄС як «конституційного охоронця» інтернет-приватності, доводячи, що захист даних є не галузевим регуляторним завданням, а конституційним мандатом. Г. Гонсалес Фустер довела автономний характер права на захист даних, відмінного від права на приватність. Л. А. Байгрейв систематизував порівняльні моделі захисту даних [7]. А. Рувруа та І. Пулле сформулювали концепцію «інформаційного самовизначення» (*informational self-determination*) як теоретичної основи права на захист даних [8]. А. Кавукян у співавторстві з С. Тейлором і М. Абрамсом визначають модель підзвітного врядування та принципу приватності за задумом (*privacy by design*) [9].

Закон України «Про захист персональних даних» регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних. Зокрема, ним вводиться в обіг термін «персональні дані»,

зміст якого трактується як «відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована» [10].

Таким чином, ключовою ознакою персональних даних є їх здатність прямо або опосередковано ідентифікувати особу. Ключовим у вищенаведеному визначенні також є поняття «ідентифікована особа». Ідентифікація у загальному значенні означає [11, с. 151] процес ототожнення або встановлення тотожності особи шляхом її виокремлення серед інших суб'єктів.

В юридичній площині ідентифікація передбачає можливість безпомилкового встановлення конкретної особи на основі сукупності її атрибутів. Зазвичай до таких атрибутів відносять ім'я, прізвище, по батькові, реквізити документа, що посвідчує особу, а також унікальні цифрові ідентифікатори, зокрема реєстраційний номер облікової картки платника податків.

Для прикладу, законодавство України визнає багаторівневий характер ідентифікації. Відповідно до Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» [12] ідентифікація особи здійснюється шляхом порівняння наданих даних, у тому числі біометричних, з наявними відомостями у відповідних реєстрах.

Аналогічно, Закон України «Про електронну ідентифікацію та електронні довірчі послуги» визначає електронну ідентифікацію як процес використання ідентифікаційних даних в електронній формі, що однозначно визначають фізичну особу [13].

Таким чином, для ідентифікації особи не завжди є необхідним повний набір персональних ідентифікаторів, оскільки за певних умов достатньою є навіть обмежена сукупність даних, здатних у контексті конкретної інформаційної системи забезпечити виокремлення особи серед інших.

Рішення Конституційного суду України від 12 січня 2012 року розкриває перелік даних, що становлять інформацію про особисте та сімейне життя

особи. Такими є дані про національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, матеріальний стан, адресу, дату і місце народження, місце проживання та перебування тощо, дані про особисті майнові та немайнові відносини цієї особи з іншими особами, зокрема членами сім'ї, а також відомості про події та явища, що відбувалися або відбуваються у побутовому, інтимному, товариському, професійному, діловому та інших сферах життя особи, за винятком даних стосовно виконання повноважень особою, яка займає посаду, пов'язану зі здійсненням функцій держави або органів місцевого самоврядування [14].

Отже зазначена інформація відноситься до категорії інформації з обмеженим доступом (конфіденційною інформації) та може поширюватися тільки за згодою осіб, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Щодо класифікації персональних даних, слід зазначити, що як Законом (ст. 7), так і Директивою (ст. 8), Регламентом (ст. 9) та Конвенцією 108+ (ст. 6) із загального переліку персональних даних виділяються спеціальні (також їх часто характеризують, як чутливі) категорії персональних, обробка яких дозволяється лише в чітко визначених випадках [15].

Окрему категорію становлять персональні дані, щодо яких встановлено особливий правовий режим обробки. У доктрині та правозастосовній практиці такі дані традиційно визначаються як «чутливі» персональні дані. Відповідно до підходів, закріплених у пунктах 51–55 преамбули Регламенту (ЄС) 2016/679, такими є дані, які за своєю природою є особливо чутливими щодо основоположних прав і свобод особи, а їх обробка здатна створювати підвищені ризики дискримінації, порушення приватності та інших негативних наслідків.

Національне законодавство відтворює цей підхід у статті 7 Закону України «Про захист персональних даних», відносячи до спеціальних категорій персональних даних відомості про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних

партіях та професійних спілках, а також дані щодо засудження до кримінального покарання, стану здоров'я, статевого життя, біометричні та генетичні дані. За загальним правилом обробка таких даних забороняється, за винятком випадків, прямо передбачених законом.

Водночас нормативне регулювання не обмежується виключно законодавчим рівнем. Наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14 затверджено Порядок повідомлення про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, пункт 1.2 якого закріплює вичерпний перелік категорій даних, обробка яких визнається такою, що становить особливий ризик для прав і свобод особи [60], попри відсутність відповідного переліку в самому Законі України «Про захист персональних даних».

Порівняльний аналіз положень статті 7 Закону України «Про захист персональних даних» [10] та пункту 1.2 Порядку свідчить про те, що зазначені нормативні акти регулюють різні за обсягом категорії інформації, між якими водночас простежується значний ступінь нормативного узгодження поряд із розширенням змістового обсягу ризикових категорій на підзаконному рівні.

Між вказаними категоріями існує як значний ступінь нормативного узгодження, так і розширення змістового обсягу ризикових категорій персональних даних на підзаконному рівні. Водночас між ними простежується очевидний змістовний зв'язок, оскільки більшість категорій даних, визначених Законом України «Про захист персональних даних» як такі, що потребують особливого режиму обробки, були відтворені та деталізовані у підзаконному регулюванні.

По-перше, спостерігається повне співпадіння базових категорій даних, які визнаються чутливими. До таких категорій віднесено інформацію про расове чи етнічне походження, політичні, релігійні або світоглядні переконання, статеве життя, біометричні та генетичні дані, стан здоров'я.

Як визначено у Регламенті (ЄС) 2016/679, особливого захисту потребують персональні дані, що відносяться до категорії особливо чутливих.

Вказане обґрунтовано тим, що контекст їхньої обробки може створювати суттєві ризики щодо прав людини. Обробка спеціальних (чутливих) категорій персональних даних можлива, наприклад, без згоди об'єкта даних лише з метою забезпечення їх суспільних інтересів у медичній сфері [16].

По-друге, Порядок повідомлення про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних здійснює нормативну деталізацію окремих положень згаданого Закону. Так, якщо Закон України «Про захист персональних даних» оперує категорією «расове або етнічне походження», згаданий Порядок додатково розширює згадану категорію шляхом включення також національного походження особи, що посилює ідентифікаційний та соціокультурний аспект відповідної категорії даних.

Аналогічно, положення Закону України «Про захист персональних даних» щодо членства в політичних партіях та професійних спілках у Порядку були розширені шляхом включення інформації про членство не лише в політичних партіях, а й у політичних організаціях, релігійних організаціях та громадських організаціях світоглядної спрямованості. Такий підхід свідчить про прагнення охопити ширше коло даних, здатних розкривати ідеологічні, релігійні, суспільно-політичні чи інші переконання особи.

По-третє, найбільш суттєвою особливістю Порядку є включення до переліку даних, обробка яких становить особливий ризик для прав і свобод суб'єктів персональних даних, низки категорій, яка не передбачена статтею 7 Закону. Йдеться, зокрема, про відомості щодо притягнення особи до адміністративної відповідальності, застосування заходів у межах досудового розслідування або оперативно-розшукової діяльності, факти вчинення щодо особи насильства, а також дані про її місцеперебування та шляхи пересування.

На відміну від класичних «чутливих» персональних даних, визначених Законом, зазначені категорії інформації не характеризують внутрішні переконання, фізіологічні чи біологічні особливості особи, однак їх обробка

здатна створювати значні ризики для приватності, безпеки, репутації та реалізації інших прав людини.

Таким чином, якщо стаття 7 Закону України «Про захист персональних даних» встановлює спеціальний правовий режим щодо окремих категорій найбільш чутливих персональних даних, то Наказ Уповноваженого розширює сферу підвищеного захисту, охоплюючи також інші види інформації, обробка яких потенційно може спричинити істотне втручання у приватне життя особи, дискримінацію, стигматизацію або інші негативні наслідки для реалізації її прав і свобод.

Закладений у Порядку підхід щодо повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, фактично ґрунтується не лише на характеристиках окремих категорій персональних даних, а й на оцінці потенційного впливу їх обробки на права та свободи особи.

На відміну від статті 7 Закону України «Про захист персональних даних», яка зосереджується переважно на визначенні спеціальних категорій («чутливих») персональних даних, Порядок повідомлення про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних поширює підвищені вимоги також на відомості, ризикованість яких обумовлена можливими наслідками їх використання для суб'єкта персональних даних [60].

Такий підхід відображає окремі елементи, наближені до ризик-орієнтованої моделі регулювання, закріпленої у пунктах 75 та 76 преамбули GDPR [16] та яка побудована на концепції оцінки ризиків для прав і свобод фізичних осіб як одного з ключових елементів механізму захисту персональних даних.

Водночас у національному правовому регулюванні відсутність уніфікованого законодавчого визначення категорії «дані підвищеного ризику» може створювати певну правову невизначеність, оскільки межі між

«спеціальними персональними даними» та «ризиковими персональними даними» визначаються на різних нормативних рівнях.

Вказане породжує проблему нормативної неузгодженості між законом і підзаконним регулюванням та потребує усунення шляхом відповідного доповнення Закону України «Про захист персональних даних».

Центральною юридичною категорією у сфері захисту персональних даних є поняття їх обробки, яке визначає як предмет правового регулювання, так і межі відповідальності суб'єктів відповідних правовідносин (рис. 1).

Рис. 1. Складові обробки персональних даних (авт.)

Обробкою персональних даних є будь-яка дія 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, що визначено відповідно до статті 2 Закону України «Про захист персональних даних» [10].

Наведена дефініція має широкий нормативний обсяг і не обмежує поняття обробки лише операціями із систематизованими масивами даних, наприклад базами даних. Будь-яка із зазначених дій, вчинена щодо персональних даних навіть одного суб'єкта та у будь-якій формі, є обробкою у розумінні Закону України «Про захист персональних даних». Зазначене свідчить про те, що законодавець свідомо відмовився від обмежувального тлумачення, поширивши правовий режим обробки на весь спектр можливих операцій із персональними даними незалежно від їх масштабу, способу здійснення або технічного середовища.

Такий підхід відповідає концепції, закріпленій у Регламенті (ЄС) 2016/679, яким визначено будь-яку операцію або сукупність операцій, що здійснюються щодо персональних даних – автоматизованими чи неавтоматизованими засобами, як обробку персональних даних [16].

Важливим аналітичним завданням є розмежування суміжних правових категорій – «обробки», «використання» та «захисту» персональних даних, співвідношення між якими не є однозначним у доктрині та правозастосовній практиці.

Слід наголосити, що «використання» персональних даних розглядається як складова обробки персональних даних. Водночас у жодному випадку обробка не може розглядатися як складова використання, оскільки обробка має первинний характер щодо будь-яких подальших дій із даними.

Окрім того, розмежовуючи правові категорії, термін «захист» персональних даних необхідно розглядати як окремий напрям діяльності, що забезпечує режим їх охорони (створення володільцем персональних даних додаткових гарантій захисту – запровадження внутрішніх процедур, таких як відібрання зобов'язань про нерозголошення персональних даних, розмежування доступу до персональних даних працівників володільця персональних даних в залежності від функціонального розподілу). Тоді як «використання» становить один із елементів ширшої категорії «обробка персональних даних».

При цьому «захист персональних даних», в залежності від суті заходів, які в кожному конкретному випадку вживаються володільцем персональних даних, можуть як відноситися до згаданих категорій («використання», «обробка персональних даних»), так і не включатися до них.

Суб'єктний склад правовідносин у сфері обробки персональних даних визначається через категорії «володільця» та «розпорядника» персональних даних, розмежування між якими має принципове значення для розподілу прав, обов'язків і відповідальності у відповідних правовідносинах.

Володільцем персональних даних є фізична або юридична особа, яка визначає мету обробки та встановлює склад персональних даних, процедури їх обробки, якщо інше не визначено на законодавчому рівні [10].

Частиною четвертою статті 4 Закону України «Про захист персональних даних» передбачено, що за дорученням володільця персональних даних, обробка персональних даних може здійснюватися третьою особою – розпорядником персональних даних. Вказане реалізується на практиці шляхом укладання договору (в письмовій формі). Вимог щодо нотаріального посвідчення договору законодавство прямо не встановлює. При цьому, розпорядник персональних даних не може виходити за межі умов обробки персональних даних, встановлених у договорі, а тому має обробляти персональні дані виключно з тією метою та у тому обсязі, що прямо визначені договором. Отже, розпорядник персональних даних позбавлений права виходити за межі повноважень, які були йому делеговані на підставі договору.

Таким чином, практичне значення розмежування між володільцем і розпорядником персональних даних виявляється, зокрема, у механізмі договірного делегування повноважень щодо обробки.

Отже відповідно до GDPR – «processor», розпорядником персональних даних (відповідно) є суб'єкт, який здійснює обробку персональних даних від імені володільця та виключно в межах його інструкцій або приписів закону. Його правовий статус є похідним, а функціональна автономія обмежена рамками повноважень, які були йому делеговані [16].

В той час, відповідно до національного законодавства, розпорядником персональних даних є «фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця» [10]. Відповідно до статті 4 Закону України «Про захист персональних даних», розпорядником персональних даних, володільцем яких є орган державної влади чи орган місцевого самоврядування, крім цих органів, може бути лише підприємство державної або комунальної форми власності, що належить до сфери управління цього органу [10].

Для ілюстрації наведених положень показовими є наведені далі ситуації, що мають практичне застосування. Так, у відносинах між підприємством, що надає житлово-комунальні послуги, та приватною компанією, якій доручено ведення обліку наданих послуг і здійснених споживачами платежів, підприємство виступає володільцем персональних даних, тоді як компанія, що забезпечує технічну реалізацію відповідного реєстру в межах визначеної мети та на підставі договору, є розпорядником.

Аналогічним чином, у відносинах між банком та компанією, якій доручено стягнення простроченої заборгованості, остання обробляє персональні дані боржників виключно в межах повноважень, наданих банком, і не набуває щодо таких даних жодних самостійних прав, що також кваліфікує її як розпорядника.

Таким чином, Закон України «Про захист персональних даних» встановлює ключові аспекти щодо поняття розпорядника та його відносин із володільцем, які однак не є достатніми та потребують суттєвого доповнення.

Зокрема, чинне законодавство України закріплює концептуально обґрунтовану систему розмежування між володільцем і розпорядником персональних даних, яка в цілому узгоджується з підходами права ЄС.

Водночас аналіз наведених положень свідчить про їхню недостатню деталізацію в частині розподілу відповідальності між суб’єктами, які здійснюють обробку персональних даних, зокрема у випадках залучення розпорядників персональних даних або транскордонної передачі даних.

Європейський суд з прав людини у своїй практиці, зокрема у справах «S. and Marper v. the United Kingdom» [96], «Bărbulescu v. Romania» [17] послідовно підкреслює, що обробка персональних даних у розумінні статті 8 Конвенції про захист прав людини і основоположних свобод охоплює будь-яке збирання, зберігання або використання інформації, здатної прямо чи опосередковано ідентифікувати особу, незалежно від її обсягу чи систематизації [19].

У цьому контексті принципового значення набуває теза про те, що обробка персональних даних не обмежується лише операціями з формалізованими структурами даних. Будь-яка дія з інформацією про фізичну особу – навіть у випадку одиничного факту збирання або перегляду даних щодо одного суб'єкта – становить обробку у розумінні як національного, так і європейського правового регулювання.

На відміну від GDPR, який у статтях 28–29 детально регулює зміст договору між контролером і обробником, встановлює обов'язкові договірні умови та закріплює механізм відповідальності обробника, Закон України «Про захист персональних даних» обмежується загальними положеннями, що зумовлює значні прогалини у правозастосовній практиці та потребує системного законодавчого вдосконалення.

1.2. Нормативно-правове регулювання здійснення обробки персональних даних

Нормативно-правове регулювання обробки персональних даних в Україні доцільно розглядати не як статичний перелік чинних актів, а як результат еволюції наглядової моделі, що формувалася під впливом двох чинників – похідного характеру права на захист даних щодо права на приватність та зовнішньої євроінтеграційної умовності. Саме у взаємодії цих чинників виявляється засаднича суперечність вітчизняного регулювання, яка визначає його ефективність: розрив між формальною гармонізацією із європейськими стандартами та субстанційною спроможністю наглядового

механізму. Послідовний аналіз нормативної основи дозволяє виявити цей розрив і окреслити напрями його подолання.

Право на захист персональних даних не має автономного характеру: історично і догматично воно сформувалося як складова ширшого права на повагу до приватного життя, гарантованого статтею 8 Конвенції про захист прав людини і основоположних свобод [18].

Стаття 8 Конвенції про захист прав людини і основоположних свобод не лише проголошує основоположний принцип недоторканності приватного життя, але й розкриває його та конкретизує через такі складові, як приватне і сімейне життя, житло та кореспонденцію, кожна з яких підлягає самостійному правовому захисту.

Р.О. Стефанчук, диферінціюючи недоторканість особи, розмежовує її складові за наступними вимірами: а) фізичну (тілесну, соматичну) недоторканність; б) психічну недоторканність; в) моральну недоторканність [37, с. 99]. В працях окремих науковців, недоторканість особи розмежовують на більш вузькі категорії – на фізичну та психічну.

На думку автора, вказані підходи засвідчують ….. . Водночас в контексті структури, відображеної у Конституції України [19], положення якої формують багаторівневу систему гарантій приватності, а також зважаючи на їхній взаємоз’вязок із положеннями статті 8 Конвенції, можливо виділити наступні взаємопов’язані виміри. Фізичний вимір приватності гарантує стаття 28, яка, закріплюючи повагу до гідності людини, встановлює неприпустимість медичних, наукових та інших дослідів без вільної згоди особи та запроваджує принцип інформованої згоди.

Територіальну складову приватності особи забезпечує стаття 30 через принцип недоторканності житла. Інформаційний вимір приватності формулюють положення статті 32, які з одного боку утворюють гарантії приватності у комунікації (таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції), а з іншої – забороняють втручання в особисте і сімейне життя, а також збирання, зберігання, використання та

поширення конфіденційної інформації про особу без її згоди, закріплюючи тим самим принцип контролю особи над власними персональними даними [20].

Похідний характер права на захист персональних даних має пряме методологічне значення для розуміння контролю: оскільки захист даних є складовою приватності, контроль за обробкою не може зводитися до формального адміністрування, а має забезпечувати дієвий захист приватності у кожному з чотирьох вимірів. Цей висновок є відправним для обґрунтованої надалі тези про сферозалежний характер контролю та для аналізу секторальних режимів захисту даних (зокрема медійного, детально наведеного у підрозділі 2.1 – авт.).

На міжнародному рівні нормативне закріплення захисту даних як складової приватності вперше відбулося в актах Ради Європи. Конвенція про захист осіб у звязку з автоматизованою обробкою персональних даних [21] стала першим юридично обов’язковим міжнародним інструментом у цій сфері: вона закріпила вимоги справедливої та безпечної обробки даних виключно для визначених цілей і на законних підставах, а також право особи знати про обробку своїх даних, мати до них доступ, виправляти та видаляти дані, що обробляються незаконно.

Додатковий протокол до Конвенції № 108 від 8 листопада 2001 року щодо органів нагляду та транскордонних потоків даних [22] запровадив принципово важливу вимогу – наявність наглядових органів, що виконують свої функції у повній незалежності, як елемента ефективного захисту осіб. Аналогічну вимогу містила стаття 28 Директиви 95/46/ЄС [15].

Таким чином, ще до ухвалення національного закону європейський стандарт визначив інституційну форму контролю – незалежний наглядовий орган. Ця обставина є ключовою для розуміння подальшої еволюції української моделі: інституційний дизайн контролю був не самостійним вибором національного законодавця, а транспонованим зовнішнім

стандартом, що згодом зумовило характерний для нього розрив між формою та змістом.

Рухаючись євроінтеграційному напрямку, Україна у 2010 році ратифікувала Конвенцію № 108 та Додатковий протокол до неї, взявши на себе зобов'язання забезпечити захист персональних даних як невід'ємний елемент права на приватність. 1 червня 2010 року було прийнято, а 1 січня 2011 року введено в дію Закон України «Про захист персональних даних».

Визначальним етапом став Закон України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» [23]. Згідно з пояснювальною запискою [24], його ухвалення зумовлювалося двома взаємопов'язаними чинниками: реалізацією Національного плану з виконання Плану дій щодо лібералізації Європейським Союзом візового режиму для України, затвердженого Указом Президента України від 22 квітня 2011 року № 494 [25], та потребою приведення законодавства у відповідність до Конвенції № 108 і Додаткового протоколу. Прикметно, що обидва чинники мали зовнішнє походження, а створення ефективного механізму захисту даних було, серед іншого, умовою надання Україні безвізового режиму.

Концептуальною новелою цього Закону стало закріплення принципу інституційної незалежності наглядового органу та відмова від дисперсної моделі контролю на користь централізованої: єдиним уповноваженим органом у сфері захисту персональних даних визначено Уповноваженого Верховної Ради України з прав людини.

Закон України «Про захист персональних даних» суттєво розширив його повноваження – здійснення парламентського контролю через планові і позапланові перевірки володільців та розпорядників, видання обов'язкових до виконання приписів про усунення порушень, надання рекомендацій, моніторинг нових технологічних практик обробки даних та участь у формуванні державної політики.

Водночас трансформовано модель адміністративно-деліктного реагування: складання протоколів про адміністративні правопорушення покладено на уповноважених представників Секретаріату Уповноваженого з подальшим направленням матеріалів до суду; внесено зміни до Кодексу України про адміністративні правопорушення в частині перегляду складів правопорушень і посилення санкцій. Запроваджено також обов'язок повідомляти Уповноваженого про обробку, що становить підвищений ризик для прав і свобод фізичних осіб, та обов'язкове утворення структурних підрозділів або призначення відповідальних осіб із захисту даних, що заклало підвалини внутрішнього контролю за обробкою персональних даних.

Попри безсумнівне значення Закону України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних», який заклав організаційно-правові засади централізованого незалежного нагляду та забезпечив змістовну гармонізацію зі стандартами Ради Європи, критичний аналіз виявляє засадничий розрив між формою та змістом цієї моделі, що простежується за трьома напрямами.

По-перше, обрана інституційна форма – покладення наглядових функцій на Уповноваженого з прав людини – відрізняється від поширеної у державах Європейського Союзу моделі спеціалізованого незалежного органу із захисту даних. Поєднання загальної правозахисної компетенції омбудсмена як конституційного органу парламентського контролю за додержанням прав людини і громадянина з вузькоспеціалізованим наглядом за обробкою даних об'єктивно обмежує спроможність контролю – інституційну, кадрову та експертну.

По-друге, обраний адміністративно-деліктний механізм розщеплює виявлення порушення (Секретаріат Уповноваженого) та застосування санкції (суд), що подовжує процедуру та послаблює невідворотність відповідальності. Конституційні вади цієї конструкції докладніше проаналізовано у підрозділі 2.3 на прикладі статей 188-39 та 188-40 Кодексу України про адміністративні правопорушення.

По-третє, європейський вектор розвитку, відносно якого здійснювалася гармонізація законодавства, відтоді суттєво змістився. У 2016 році ухвалено GDPR, що замінив Директиву 95/46/ЄС та наділив наглядові органи розгорнутим набором повноважень – розслідувальних, корективних і дозвільних (стаття 58 GDPR) [16]; у 2018 році відкрито для підписання Модернізовану Конвенцію 108+ (Протокол CETS № 223) [26], яка розширила й деталізувала повноваження наглядових органів та інтегрувала принципи прозорості, пропорційності, підзвітності, мінімізації даних і конфіденційності за дизайном.

Сукупність цих обставин дозволяє сформулювати робочу концепцію дослідження: ефективність контролю за обробкою персональних даних в Україні лімітується не відсутністю нормативного регулювання, а розривом між формальною гармонізацією (наявністю норм, що відтворюють європейські стандарти) та субстанційною наглядовою спроможністю (інституційною, процедурною та санкційною здатністю забезпечити їх дотримання). Цей розрив є наскрізним предметом подальшого аналізу та кількісно операціоналізується у розділі 3.

Водночас реформування механізмів контролю за обробкою персональних даних в Україні як відбувалося, так і відбувається переважно під зовнішнім нормативним тиском, а також реалізується на виконання Євроінтеграційних вимог, однак не як результат органічного розвитку внутрішньої правозахисної системи.

Х. Хейманс розробив концепцію ЄС як «конституційного охоронця» приватності. На думку автора, концепція Х. Хейманса виправдано розглядає DPA «новою гілкою влади» з конституційним мандатом. Однак, на відміну від науковця, на нашу думку, конституційний статус DPA є недостатнім без операційної моделі ризик-орієнтованого контролю: навіть конституційно закріплена інституція може бути неефективною, якщо її інструментарій залишається реактивним.

Усунення зазначеної суперечності потребує комплексу взаємопов’язаних нормативно-правових та інституційних заходів:

1) ратифікація та імплементація Модернізованої Конвенції 108+ (Протокол CETS № 223), що дозволить розширити й деталізувати повноваження наглядового органу та інтегрувати у національне право сучасні принципи обробки – підзвітність, конфіденційність за дизайном, оцінку впливу на захист даних;

2) завершення переходу від моделі омбудсмена до спеціалізованого незалежного наглядового органу із захисту даних – відповідно до підготовленого проєкту Закону про Національну комісію з питань захисту персональних даних та доступу до публічної інформації – або, як мінімум, наділення наявного органу повним обсягом повноважень за статтею 58 GDPR, включно з прямими корективними та санкційними повноваженнями;

3) ухвалення оновленого, гармонізованого з GDPR закону про захист персональних даних, розширення прав суб’єктів персональних даних та посилення обов’язків володільців персональних даних;

4) реформування адміністративно-деліктного механізму з усуненням конституційних вад розщепленої моделі та забезпеченням невідворотності й пропорційності відповідальності.

Запропоновані заходи спрямовані не на формальне доповнення нормативного масиву, а на зменшення розриву між нормою та її дотриманням, тобто на підвищення саме субстанційної спроможності контролю – центральної проблеми, дослідженню якої присвячено наступні розділи.

Стаття 5(1) GDPR закріплює вичерпний перелік принципів: законність, справедливість і прозорість (lawfulness, fairness and transparency); обмеження мети (purpose limitation); мінімізація даних (data minimisation); точність (accuracy); обмеження зберігання (storage limitation); цілісність і конфіденційність (integrity and confidentiality); підзвітність (accountability) [16].

Порівняно з цим масивом нормативних вимог, стаття 6 Закону України «Про захист персональних даних» лише фіксує вимоги відкритості і прозорості, цільового використання, точності й актуальності даних, відповідності обсягу даних меті обробки. Однак принципи законності та справедливості не виокремлені як такі, хоча їх зміст частково охоплюється нормами щодо підстав обробки.

Натомість принципи підзвітності та ризик-орієнтованого підходу в українському законодавстві фактично відсутні: Закон України «Про захист персональних даних» покладає обов'язки переважно ex post (відповісти на скаргу, виконати припис наглядового органу), а не ex ante (системно оцінити ризики й запровадити відповідні заходи).

Принцип мінімізації даних заслуговує окремої уваги. Стаття 6 Закону України «Про захист персональних даних» передбачає, що склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети.

Формулювання є коректним, однак принципово відрізняється від підходу GDPR у механізмі забезпечення: GDPR вимагає, щоб мінімізація даних була закладена в архітектуру системи обробки – принцип «захисту даних вже на стадії проєктування та за замовчуванням» (*privacy by design* and by default, стаття 25 GDPR) [16]. Українське законодавство такої вимоги не містить, обмежуючись декларативним формулюванням, яке не виключає збирання надмірних даних «на майбутнє».

При цьому критично важливо зауважити на відсутності в українському законодавстві процедури оцінки впливу на захист даних (Data Protection Impact Assessment – DPIA).

Стаття 35 GDPR зобов'язує контролера проводити оцінку впливу на захист даних у випадках, коли передбачувана обробка може становити високий ризик для прав і свобод суб'єктів даних [16]. Найбільш подібним до вказаної процедури аналогом у Законі України «Про захист персональних даних» є повідомлення Уповноваженого про обробку, що становить

особливий ризик (стаття 9 Закону). Однак вказаний механізм є суттєво вужчим за змістом і не вимагає системного аналізу ризиків та обов'язкового вжиття заходів щодо їх мінімізації.

Принцип обмеження мети також потребує критичного аналізу. Відповідно до статті 6 Закону мета обробки має бути сформульована у відповідних документах, що регулюють діяльність володільця. У разі зміни мети – необхідна нова згода суб'єкта або законодавча підстава. GDPR, на відміну від цього, допускає подальшу сумісну обробку на підставі структурованого тесту сумісності (стаття 6 (4) GDPR), що враховує зв'язок між первісною і новою метою, контекст збору даних, характер даних, можливі наслідки для суб'єктів і наявність гарантій [16]. Відсутність подібного механізму в українському законодавстві призводить до неоднозначної правозастосовної практики

Викладене дозволяє стверджувати, що система принципів обробки персональних даних, закріплена в українському законодавстві, має суттєві структурні розбіжності з міжнародними стандартами, насамперед у частині принципу підзвітності, ризик-орієнтованого підходу та privacy by design. Ці розбіжності є не технічними деталями, а концептуальними прогалинами, що знижують ефективність правового регулювання в умовах цифрового середовища.

У законі визначено вимоги до обробки персональних даних та їх захисту. Частиною п'ятою статті 6 Закону України «Про захист персональних даних» передбачено, що обробка персональних даних здійснюється виключно на підставі згоди особи або закону.

Частина п'ята статті 6 цього Закону України «Про захист персональних даних» встановлює загальний принцип, відповідно до якого обробка персональних даних може здійснюватися виключно на підставі згоди суб'єкта персональних даних або закону. Зазначена норма є вихідним положенням, що визначає допустимі межі обробки та реалізується через систему конкретних підстав, закріплених у статті 11 Закону України «Про захист персональних

даних». Обробка, що не підпадає під жодну з передбачених підстав, є незаконною незалежно від наявності будь-якого іншого обґрунтування.

Водночас наявність підстави з числа передбачених статтею 11 Закону України «Про захист персональних даних» є необхідною, але не достатньою умовою правомірності обробки – така обробка повинна також відповідати загальним принципам, закріпленим у статті 6 Закону України «Про захист персональних даних», а щодо спеціальних категорій персональних даних – і вимогам статті 7 Закону України «Про захист персональних даних».

Система підстав обробки персональних даних є центральним елементом правового регулювання, оскільки саме наявність законної підстави визначає межу між правомірним і незаконним втручанням у право на приватність. Порівняльний аналіз підстав, закріплених у статті 11 Закону України «Про захист персональних даних», і підстав, визначених статтею 6 GDPR, виявляє як структурну подібність, так і суттєві змістовні відмінності [16].

Підстави обробки персональних даних доцільно систематизувати у дві групи залежно від їх правової природи. До першої групи можна віднести підстави, що ґрунтуються на волевиявленні суб'єкта персональних даних, в той час як до другої – підстави, що виникають із закону або об'єктивних обставин, незалежних від такого волевиявлення.

До першої групи належать: згода суб'єкта персональних даних, а також укладення та виконання правочину, стороною якого є суб'єкт або який укладено на його користь чи для здійснення заходів, що передують його укладенню на вимогу суб'єкта.

Згода суб'єкта персональних даних є основоположною та найбільш поширеною правовою підставою обробки. Відповідно до статті 2 Закону України «Про захист персональних даних», згода визначається як добровільне волевиявлення фізичної особи – за умови її поінформованості – щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про її надання.

Згода як підстава обробки є найбільш дискусійною. Визначення згоди в Законі України «Про захист персональних даних» як «добровільного волевиявлення фізичної особи (за умови її поінформованості)» [10] – загалом відповідає концептуальній основі статті 4(11) GDPR, яка вимагає, щоб згода була вільно наданою, конкретною, поінформованою та однозначною [16].

Проте між двома підходами існує принципова операційна відмінність: GDPR у статті 7 встановлює деталізовані умови дійсності згоди, зокрема заборону «пакетної» згоди на численні цілі обробки одночасно, вимогу рівноцінності відмови від надання згоди та її надання, а також доведення контролером факту отримання згоди.

Жодна з цих умов не закріплена з відповідним рівнем операційної деталізації у Законі України «Про захист персональних даних».

Таким чином, юридично дійсна згода має відповідати трьом обов'язковим та невід'ємними ознаками:

– добровільність;

– поінформованість;

– зовнішня форма, що дає змогу зробити висновок про надання згоди.

Перша – добровільність. В контексті недопустимості застосування прямого примусу очевидним є те, що згода не може вважатися добровільною, якщо надавалася під тиском з боку представників володільця персональних даних чи інших осіб. Опосередкований примус має місце у випадках, коли отримання особою певної послуги або реалізація її прав ставиться у залежність від надання згоди на обробку персональних даних. Така ситуація є характерною для відносин із структурною нерівністю між суб'єктом і володільцем, де суб'єкт фактично позбавлений реальної альтернативи.

Друга ознака – поінформованість: до надання згоди суб'єкт повинен отримати достовірну інформацію про суб'єктний склад обробки, її мету, склад даних, коло осіб, яким дані передаватимуться, а також про права, передбачені статтею 12 Закону України «Про захист персональних даних».

Закон України «Про захист персональних даних» не встановлює обов'язкової форми надання такої інформації, проте з позицій правової визначеності та доказової достатності володілець повинен мати можливість підтвердити факт її надання.

Третя ознака – належна зовнішня форма, що дає змогу зробити висновок про надання згоди: вона може бути письмовою або вчиненою іншим способом, проте повинна бути достатньо визначеною для правового підтвердження.

Проблема добровільності згоди у відносинах структурної нерівності, для прикладу, між роботодавцем і працівником, надавачем послуг та особою, яка звертається за послугою, може хибно трактуватися як своєрідний «примус» до надання згоди. Зокрема, у Щорічній доповіді за 2013 рік, Уповноваженим Верховної Ради України з прав людини зафіксовано системну проблему, яка набула ознак структурного порушення принципу добровільності згоди: особа фактично позбавлялась можливості отримати медичну допомогу, соціальний захист чи освітні послуги без надання згоди на обробку персональних даних [27].

Така практика суперечить сутності згоди як правового інструменту, що передбачає вільне волевиявлення суб'єкта персональних даних, і кваліфікується у доктрині як «примусова згода», несумісна з вимогами як Конвенції 108+, так і подальших положень GDPR щодо добровільності.

ЄДСПЛ у рішеннях Peruzzo and Martens v. Germany [28] та Vukota-Bojić v. Switzerland [29] послідовно підкреслював, що добровільність згоди не може презюмуватися у відносинах залежності. Стаття 7 GDPR прямо передбачає, що при оцінці вільного характеру згоди слід ураховувати, чи не зумовлено виконання договору наданням згоди на обробку, яка не є необхідною для виконання договору.

Укладення та виконання правочину як підстава обробки персональних даних є самостійною правовою категорією, хоча за своєю природою тяжіє до групи волевиявлення. Цивільно-правова вимога вільного волевиявлення

учасника правочину, що відповідає його внутрішній волі, зближує цю підставу зі згодою у її класичному розумінні.

Відмінність полягає в тому, що сам факт укладення договору є достатньою підставою для обробки персональних даних у межах, необхідних для його виконання, – незалежно від окремого волевиявлення щодо такої обробки.

Практика Європейської ради із захисту даних [30] свідчить, що необхідність обробки для виконання договору слід тлумачити вузько: обробка є необхідною лише тоді, коли без неї договір об'єктивно не може бути виконаний. Відсутність подібних роз`яснень в українській правозастосовній практиці залишає цю підставу де-факто відкритою для розширювального тлумачення, що створює ризики надмірної обробки персональних даних.

Таким чином, обидві підстави першої групи об'єднує те, що правомірність обробки визначається через автономію волі суб'єкта. Водночас між ними існує суттєва відмінність у режимі правового контролю: згода може бути відкликана в будь-який момент, тоді як обробка в рамках виконання договору обумовлена договірними зобов'язаннями та припиняється із їх виконанням або припиненням договору.

Різниця між правочином та згодою, як окремою підставою для обробки персональних даних, лише в тому, що сам по собі договір (незалежно від змісту його положень) є підставою для обробки даних особи, незалежно надання чи ненадання окремої згоди.

До другої групи підстав належать: дозвіл на обробку, наданий відповідно до закону для здійснення повноважень володільця; необхідність виконання законного обов'язку володільця; захист законних інтересів володільця або третьої особи; а також захист життєво важливих інтересів суб'єкта персональних даних.

Дозвіл, наданий законом для здійснення повноважень володільця, охоплює випадки, коли визначені законом повноваження суб'єкта публічного або приватного права об'єктивно передбачають обробку персональних даних.

Вказане положення Закону дозволяє обробляти персональні дані не лише у випадках, коли на це є пряма вказівка закону, а й коли це об'єктивно обумовлюється повноваженнями державного органу.

Наявність таких повноважень є достатньою підставою для обробки, проте лише в обсязі, необхідному для їх реалізації. Ця підстава є переважно публічно-правовою за сферою застосування та охоплює обробку, що здійснюється органами державної влади та місцевого самоврядування в межах компетенції, визначеної законом.

Необхідність виконання законного обов'язку володільця є суміжною, але самостійною підставою, яка поширюється на ширше коло суб'єктів – не лише на органи публічної влади, а й на приватних осіб. Відмінність від попередньої підстави полягає в тому, що тут йдеться про виконання обов'язку, а не про реалізацію дискреційних повноважень: відтак обробка є не лише допустимою, а й юридично необхідною для виконання припису закону.

Захист законних інтересів володільця або третьої особи є підставою субсидіарного характеру, що може застосовуватися лише за умови, що потреби захисту основоположних прав і свобод суб'єкта персональних даних не переважають відповідних інтересів. Ця підстава передбачає проведення обов'язкового балансового тесту та не може використовуватися для систематичної обробки без належного обґрунтування в кожному конкретному випадку.

Захист життєво важливих інтересів суб'єкта. За загальним правилом вказана підстава передбачає, що на момент, коли виникла потреба захисту життєво важливих інтересів суб'єкта персональних даних, яка потребує, серед іншого, здійснення обробки його персональних даних, отримати згоду неможливо. Ця підстава має не закономірний, а ситуативний, подекуди вимушений характер, а тому не може бути підставою для систематичного здійснення обробки персональних даних. Об'єктивними ситуаціями, за яких використовується вказана підстава, у тому числі є перебування у безпорадному стані, зокрема без свідомості, а також нездатність особи

усвідомлювати наслідки вчинення своїх дій тощо. Попри те, що життєво важливі інтереси суб'єкта персональних даних окремо не визначені у статті 8 статті 8 Конвенції про захист прав людини і основоположних свобод [19], такі інтереси вважаються включеними в поняття «правомірна підстава» у Конвенції 108+, яка врегульовує питання правомірності обробки персональних даних [31].

Таким чином, підстави другої групи є різними за функціональним призначенням та умовами застосування, однак їх об'єднує те, що правомірність обробки в цих випадках визначається не волевиявленням суб'єкта, а об'єктивними правовими або фактичними обставинами. З огляду на це до них висуваються підвищені вимоги правової визначеності та пропорційності.

Обробка повинна додатково відповідати принципам, розглянутим у попередньому підрозділі, а щодо спеціальних категорій даних – вимогам статті 7 Закону України «Про захист персональних даних». Ця ієрархія вимог часто ігнорується у правозастосовній практиці: факт наявності законної підстави сприймається як вичерпна відповідь на питання про правомірність обробки, тоді як відповідність принципам мінімізації, пропорційності та підзвітності залишається поза увагою.

Таким чином, система підстав обробки персональних даних в українському законодавстві є концептуально коректною, але операційно недостатньою. Відсутність деталізованих механізмів оцінки дійсності згоди, методології балансового тесту для законного інтересу та обмежень щодо розширювального тлумачення підстави виконання договору створює структурні умови для правозастосовних зловживань і нівелювання реального захисту суб'єктів даних.

Поширення персональних даних є однією з форм їх обробки та регулюється статтею 14 Закону України «Про захист персональних даних». Відтак поширення (передача) персональних даних повинна здійснюватися за згодою суб'єкта персональних даних або на підставі, конкретно визначеній

законом. Поширення має здійснюватися виключно у випадках, визначених у статті 7 та статті 11 Закону України «Про захист персональних даних».

Так, без згоди суб'єкта, поширення даних допускається лише у випадках, прямо визначених законом, і виключно в інтересах національної безпеки, економічного добробуту або прав людини – як вичерпних легітимних цілей такого втручання.

Доступ третіх осіб до персональних даних регулюється статтею 16 Закону України «Про захист персональних даних». Порядок такого доступу визначається умовами згоди суб'єкта або вимогами закону; щодо даних, які перебувають у володінні розпорядника публічної інформації.

Доступ не надається, якщо запитувач відмовляється від зобов'язань щодо виконання вимог Закону України «Про захист персональних даних» або не може їх забезпечити. Ця конструкція відтворює конституційну формулу статті 32 і є концептуально правильною. Однак вона описує лише один зі способів передачі даних третім особам – той, що здійснюється через механізм «запит – відповідь» за статтею 16 Закону України «Про захист персональних даних».

Аналіз правозастосовної практики свідчить, що поза цим механізмом функціонують щонайменше два інших способи передачі персональних даних третім особам, які Закон України «Про захист персональних даних» не регулює належним чином. Перший – передача на підставі договору між володільцем і третьою особою, що де-факто відбувається у широкому спектрі комерційних відносин (аутсорсинг, хмарні сервіси, рекламні мережі). Другий – на підставі положень законодавства, які санкціонують пряму та автоматичну передачу персональних даних (зазвичай між державними органами), щодо яких Закон не встановлює жодних спеціальних вимог та будь-яких процедурних гарантій для суб'єкта.

У першому випадку Закон України «Про захист персональних даних» не містить вимог щодо мінімального змісту договорів про обробку даних – на відміну від статті 28 GDPR [16], яка детально регулює відносини контролера і

процесора. У другому – відсутність будь-яких спеціальних вимог до автоматизованого міжвідомчого обміну даними є особливо критичною в умовах розгортання масштабної цифрової інфраструктури держави (реєстри, «Дія», «Резерв+», інтегровані інформаційні ресурси).

Право доступу суб'єкта до власних персональних даних є невід'ємним елементом права на інформаційну автономію і водночас процесуальним інструментом реалізації інших прав – права на виправлення, знищення та заперечення проти обробки.

Законодавча модель, закріплена у статті 16 Закону України «Про захист персональних даних», формально забезпечує це право, однак страждає від тих самих лакун, що й інші елементи регулювання: декларативність без операційних механізмів.

Зокрема, Закон України «Про доступ до публічної інформації» не встановлює вимог до форми відповіді на запит суб'єкта, не визначає обсягу інформації, яку зобов'язаний надати володілець, і не регулює ситуацій, коли дані оброблялися автоматизованими системами.

Стаття 15 GDPR, натомість, встановлює деталізований стандарт: суб'єкт має право отримати підтвердження факту обробки, копію даних, інформацію про цілі обробки, одержувачів, строки зберігання, джерела збору та логіку автоматизованого прийняття рішень. Цей стандарт є операційним мінімумом, забезпечення якого вимагає від контролера реальної прозорості, а не формальної відповіді на запит.

Окремою проблемою, що виявляється при аналізі режиму доступу до персональних даних, є нормативна колізія між статтею 7 Закону України «Про доступ до публічної інформації» та статтею 21 Закону України «Про інформацію» [32] у частині визначення конфіденційної інформації. Перший акт застосовує суб'єктивно-вольовий підхід – конфіденційність визначається волевиявленням особи. Другий закріплює об'єктивно-категоріальний підхід – конфіденційною є будь-яка інформація про фізичну особу за самою її предметною природою. Ця колізія породжує неоднакову правозастосовну

практику, зокрема щодо меж доступу до відомостей про осіб, які обіймають публічні посади.

Аналіз статті 16 Закону України «Про захист персональних даних» свідчить про те, що вона врегульовує переважно процедуру «запит – відповідь», залишаючи поза межами спеціального регулювання щонайменше два інших способи передачі персональних даних третім особам: на підставі договору та на підставі нормативних положень, що передбачають пряму або автоматичну передачу даних між суб'єктами – зокрема між органами державної влади. Відсутність спеціальних вимог до зазначених способів передачі є законодавчою прогалиною, що потребує усунення.

Процедура реалізації права доступу здійснюється у формі запиту. Запит повинен містити ідентифікаційні відомості заявника – фізичної або юридичної особи, – відомості про суб'єкта, щодо якого запитуються дані, опис запитуваних відомостей, а також підстави або мету запиту.

Зазначення мети та правових підстав є обов'язковим реквізитом, оскільки лише за їх наявності володілець може прийняти обґрунтоване рішення щодо передачі даних.

Відсутність таких відомостей є самостійною підставою для відмови у задоволенні запиту. Суб'єкт персональних даних, на відміну від третіх осіб, має право на отримання будь-яких відомостей про себе у будь-якого суб'єкта відносин у сфері персональних даних – за умови належного підтвердження своєї особи відповідно до частини шостої статті 16 Закону України «Про захист персональних даних» [10].

Окремої уваги в контексті правового регулювання доступу до інформації, а також відмежування суміжних категорій інформації з обмеженим доступом, є питання правового режиму інформації (відомостей) про померлих осіб, оскільки його правове регулювання перебуває на перетині права на доступ до інформації, права на приватність та захисту персональних даних, а також не містить єдиного підходу у правозастосуванні.

Обробка, використання та поширення інформації про померлу особу суб'єктами владних повноважень становлять складну правову проблему, яка має істотне значення для забезпечення соціальних, майнових та інших прав і законних інтересів фізичних осіб, особливо в умовах повномасштабного збройного вторгнення Російської Федерації в Україну та ведення активних бойових дій на території держави. Родичі загиблих військовослужбовців і цивільних осіб стикаються із системною відсутністю уніфікованої процедури отримання відповідних відомостей, що суттєво ускладнює реалізацію їхніх прав [42, с. 674]. Незважаючи на практичну значущість зазначеної проблематики, чинне законодавство України – зокрема, Закон України «Про поховання та похоронну справу» [36] та Закон України «Про інформацію» [36] – не містить конкретної процедури отримання інформації про померлу особу, що є самостійною законодавчою прогалиною.

Конституційно-правовою основою права на доступ до інформації є стаття 34 Конституції України, яка гарантує кожному право на свободу думки і слова, на вільне вираження своїх поглядів і переконань, а також право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб на свій вибір [19]. Стаття 40 Конституції України додатково закріплює право кожної особи направляти письмові звернення або особисто звертатися до органів державної влади, органів місцевого самоврядування та посадових і службових осіб цих органів. Вказаному праву кореспонує обов'язок згаданих суб'єктів розглянути звернення і дати обґрунтовану відповідь у встановлений законом строк, що визначено цією ж статтею Основного Закону.

Слід наголосити, що конституційне право на доступ до інформації може бути обмежено виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної

конфіденційно, або для підтримання авторитету і неупередженості правосуддя [19].

Загальні засади інформаційних відносин, включно зі створенням, збиранням, одержанням, зберіганням, використанням, поширенням, охороною та захистом інформації, регулює Закон України «Про інформацію». Водночас цей закон є переважно декларативним і не передбачає конкретних механізмів доступу до інформації. Протягом останніх двох десятиліть законодавець розробив і прийняв низку спеціальних нормативно-правових актів, які є процедурними за своєю суттю, а також конкретизуючи конституційні положення, передбачають механізми доступу до інформації у відповідних сферах.

Спеціальний порядок реалізації права на доступ до інформації регламентується насамперед Законами України «Про захист персональних даних» [10], «Про виконавче провадження», Про доступ до публічної інформації» [171], «Про адміністративну процедуру», «Про доступ до судових рішень» [33], «Про Національний архівний фонд та архівні установи» [34], «Про звернення громадян» [77], «Про доступ до архівів репресивних органів комуністичного тоталітарного режиму 1917–1991 років» [35] та іншими нормативно-правовими актами.

Питань, пов’язаних із доступом до відомостей про померлих, побіжно торкається стаття 7 Закону України «Про поховання та похоронну справу», яка встановлює, що надання інформації про померлу особу здійснюється відповідно до Закону України «Про інформацію», та закріплює обов’язок держави забезпечувати гарантії конфіденційності такої інформації [36].

Водночас ні Закон України «Про поховання та похоронну справу», ні Закон України «Про інформацію», ні будь-який інший нормативно-правовий акт не визначають ні детальних гарантій забезпечення конфіденційності інформації про померлого, ні конкретної процедури доступу до таких відомостей, ні кола уповноважених суб’єктів, ні підстав та строків надання відповідної інформації.

Ключовою теоретико-правовою проблемою є визначення правового статусу відомостей про померлу особу в системі суміжних правових категорій – персональних даних, публічної інформації та конфіденційної інформації.

Відтак, оперуючи поняттям персональних даних як такими, що є відомостями чи їх сукупністю про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована, треба звернути увагу саме на суб'єктність людини як учасника цивільних відносин.

Зокрема, Р.О. Стефанчук, аналізуючи теоретичні конструкції охорони нематеріальних благ після смерті особи, піддав критиці підходи, за якими такі блага нібито здатні «відділятися» від особи-носія. На противагу згаданій концепції, науковець пропонує розглядати як специфічний об'єкт правової охорони добре ім'я померлої фізичної особи – благо, що виникає в момент смерті особи та стосовно якого виникають і здійснюються посттанативні особисті немайнові права носіями яких є, насамперед, близькі особи померлого [37, с. 156-157].

Вказана позиція узгоджується із положеннями статей 24-25 Цивільного кодексу України, згідно із якою цивільна правоздатність фізичної особи – тобто здатність мати цивільні права та обов'язки – виникає у момент народження і припиняється в момент смерті [38].

Отже раніше згаданий механізм подання запиту щодо доступу до персональних даних, передбачений статтею 13 Закону України «Про захист персональних даних», не може бути застосований для отримання відомостей про померлу особу: зі смертю фізичної особи вона перестає бути суб'єктом правовідносин у сфері персональних даних, а отже, і суб'єктом відповідного права на захист.

Таким чином, між правовим режимом доступу до персональних даних фізичної особи та інформації про особу, яка померла, існує принципова відмінність. Натомість інформація про померлу особу, що була отримана, створена або перебуває у володінні суб'єкта владних повноважень, набуває статусу публічної в розумінні статті 1 Закону України «Про доступ до

публічної інформації» як задокументована інформація, що виникла в процесі виконання суб'єктом владних повноважень своїх обов'язків або знаходиться в його володінні [170].

Водночас публічний статус такої інформації не є беззаперечною ознакою її відкритості та не становить підстави для її надання без застосування встановлених законом обмежень. Розпорядник інформації на виконання вимог частини другої статті 6 Закону України «Про доступ до публічної інформації» зобов'язаний вилучити з-поміж усього обсягу запитуваної інформації відомості з обмеженим доступом – конфіденційну, таємну та службову інформацію – і надати лише ту частину документа, доступ до якої не обмежено [39].

Відповідно, у разі, коли запитувачем інформації про померлу особу є член її сім'ї, близька особа або родич, застосування Закону України «Про доступ до публічної інформації» не забезпечує досягнення кінцевої мети запитувача – отримання повного обсягу відомостей, – оскільки передбачає обов'язкове вилучення конфіденційної інформації незалежно від ступеня спорідненості запитувача з померлим.

Окремої уваги заслуговує нормативна колізія між визначеннями конфіденційної інформації у двох спеціальних законах. Частина перша статті 7 Закону України «Про доступ до публічної інформації» визначає конфіденційну інформацію як таку, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, і яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов.

Цей підхід є суб'єктивно-вольовим: конфіденційність визначається через волевиявлення особи. Натомість частина друга статті 21 Закону України «Про інформацію» встановлює, що конфіденційною є інформація про фізичну особу незалежно від її волевиявлення, – закріплюючи тим самим об'єктивно-категоріальний підхід, за яким конфіденційність відомостей визначається самим їх предметом.

Н.В. Коваленко підкреслює, що будь-яка інформація не є загальним юридичним терміном і не має загальних властивостей об'єктів цивільного права [40, с. 79-80], а згаданий вид інформації як багатогранний об'єкт може перехрещуватися у правовідносинах в залежності від сфери таких правовідносин. При цьому слід наголосити, що конфіденційна інформація як різновид інформації з обмеженим доступом, законодавчо відокремлена від таких категорій інфомрації, яка таємна та службова інформація.

За відсутності спеціального нормативного регулювання Уповноважений Верховної Ради України з прав людини, реалізуючи функції парламентського контролю за дотриманням права людини на доступ до інформації на підставі статті 17 Закону України «Про доступ до публічної інформації», а також повноваження щодо надання рекомендацій у сфері захисту персональних даних, закріплені Законом України «Про захист персональних даних», здійснив спробу надати оцінку правовим аспектам поширення інформації про померлого.

У листі-роз'ясненні від 25 січня 2018 року № 2/9-К306655.17/26-131 Уповноважений сформулював позицію, відповідно до якої відомості про померлу особу, що була членом сім'ї або близьким родичем запитувача, можуть одночасно розглядатися суб'єктом владних повноважень як персональні дані самого запитувача – зокрема, якщо запитувана інформація за своєю суттю стосується спільних особистих майнових або немайнових відносин чи подій, що відбувалися у спільному житті цих осіб [41].

За таких умов надання інформації є правомірним за умови підтвердження запитувачем факту родинного зв'язку шляхом надання копій відповідних документів, а також підтвердження того, що запитувана інформація є необхідною для реалізації його прав, свобод і законних інтересів.

Вимога ідентифікації запитувача та підтвердження родинних відносин відповідає положенням статті 7 Закону України «Про поховання та похоронну справу» [36] в частині забезпечення гарантій конфіденційності інформації про померлого, а також виключає сферу застосування Закону України «Про доступ

до публічної інформації», нормами якого не передбачено обов'язку розпорядника інформації ідентифікувати особу запитувача.

Запропонований механізм є логічним та таким, що відповідає усталеній державно-правовій практиці позасудової реалізації інформаційних прав громадян, оскільки пряма заборона надання такої інформації зазначеному колу осіб у нормах Закону України «Про інформацію», Цивільного та Сімейного кодексів України [38] відсутня.

Відтак можна прийти до висновку щодо правомірності надання даних про померлу особу у випадку вилучення розпорядником інформації з документів інформації з обмеженим доступом (для необмеженого кола осіб) або надання повної інформації про померлу особу (для членів сім'ї та близьким особам померлого) [42].

Зокрема, надання відомостей про померлу особу необмеженому колу осіб є допустимою за умови застосування розпорядником інформації передбаченого частиною другою статті 6 Закону України «Про доступ до публічної інформації» механізму вилучення з копій запитуваних документів інформації з обмеженим доступом [171].

Показово, що в окремих сегментах національного законодавства модель диференційованого доступу до відомостей про померлих осіб уже реалізована.

Так, відповідно до частини четвертої статті 16 Закону України «Про Національний архівний фонд та архівні установи» доступ до документів Національного архівного фонду, що містять конфіденційну інформацію про особу, обмежується на 75 років від часу їх створення; раніше цього строку доступ здійснюється з дозволу особи, а в разі її смерті – з дозволу спадкоємців, або якщо інформація є суспільно необхідною [34]. Наведена норма закріплює темпоральний критерій обмеження доступу, перехід повноваження надавати дозвіл до спадкоємців та суспільну необхідність як самостійну підставу розкриття, а отже, може слугувати нормативним орієнтиром при конструюванні загального режиму доступу до інформації про померлих осіб.

Наведена доктринальна конструкція має безпосереднє значення для сфери захисту персональних даних: вона підтверджує, що правова охорона відомостей про померлу особу не може будуватися за моделлю суб'єктивного права самого померлого, а має конструюватися через права та законні інтереси живих осіб (членів сім'ї, близьких родичів) або через суспільний інтерес.

Саме такий підхід відображено й у праві Європейського Союзу: відповідно до пункту 27 преамбули GDPR, Регламент не застосовується до персональних даних померлих осіб, однак держави-члени можуть встановлювати власні правила щодо обробки таких даних [16].

Усунення зазначених прогалин та встановлення єдиної правозастосовної практики питання доступу до інформації про померлих осіб можливе шляхом внесення відповідних змін до Закону України «Про поховання та похоронну справу» як нормативно-правового акту, який має характер спеціального у цій сфері.

На думку автора, таке врегулювання має охоплювати: визначення правового статусу інформації про померлу особу та її співвідношення з категоріями конфіденційної інформації і персональних даних; встановлення вичерпного кола суб'єктів, які мають право на доступ до повного обсягу відповідних відомостей, із визначенням переліку документів, що підтверджують таке право; закріплення диференційованих підстав і режимів доступу залежно від статусу запитувача – члена сім'ї, близького родича, третьої особи або представника наукової чи журналістської спільноти; встановлення строків розгляду відповідних запитів та порядку оскарження відмови у їх задоволенні [42].

Висновки до розділу І

1. Доведено, що ключовою ознакою персональних даних є їх здатність прямо або опосередковано ідентифікувати особу, а ідентифікація не потребує повного набору персональних ідентифікаторів – за певних умов достатньою є

обмежена сукупність даних, здатних у контексті конкретної інформаційної системи забезпечити виокремлення особи.

Виявлено нормативну неузгодженість між законодавчою категорією «спеціальних персональних даних» (стаття 7 Закону України «Про захист персональних даних») та підзаконною категорією «даних, що становлять підвищений ризик»: розбіжність юридичної сили джерел цих категорій унеможливлює їх системне співвіднесення і породжує правову невизначеність обсягу підвищених гарантій захисту. Окремо обґрунтовано існування самостійної прогалини правового регулювання щодо статусу інформації про померлу особу, зумовленої механічним поширенням на посмертні відомості режиму, розрахованого на живих суб'єктів персональних даних. Викладене засвідчує, що коректне розмежування персональних даних від суміжних категорій є функціональною, а не термінологічною передумовою розбудови диференційованої моделі контролю, оскільки саме межі предмета обробки визначають межі предмета контролю.

2. Досліджено співвідношення конституційних гарантій приватності (статті 28, 30–32 Конституції України) з міжнародно-правовими джерелами регулювання обробки персональних даних та встановлено похідний характер права на захист даних відносно права на повагу до приватного життя. Доведено пряме методологічне значення цього висновку: оскільки захист даних є складовою приватності одразу у декількох вимірах (фізичному, територіальному, комунікаційному, інформаційному), контроль за обробкою не може обмежуватися формальним адмініструванням і повинен забезпечувати ефективний захист кожного з цих вимірів.

Обґрунтовано, що система принципів обробки персональних даних, закріплена у національному законодавстві, має суттєві структурні розбіжності з міжнародними стандартами – насамперед у частині принципу підзвітності, ризик-орієнтованого підходу та *privacy by design*.

Встановлено, що ця розбіжність знижує ефективність правового регулювання в умовах цифрового середовища, оскільки саме вона визначає,

чи будується законодавство на реактивному, чи на превентивному фундаменті, що є першим емпіричним підтвердженням центральної гіпотези дисертації на рівні джерел регулювання. Зокрема, на відміну від GDPR, законодавство України не містить вимоги проведення оцінки впливу на захист даних, а аналог цієї вимоги – повідомлення Уповноваженого про обробку підвищеного ризику – є суттєво вужчим за обсягом та змістом.

Розділ 2. Здійснення контролю за обробкою персональних даних: правореалізація та правозастосування

2.1. Поняття, види та форми контролю за обробкою персональних даних

У вітчизняному законодавстві та наукових працях поняття «контролю» у контексті здійснення суб'єктами владних повноважень своїх функцій, як правило, ототожнюється з інститутом державного або владного контролю. Так, Н. М. Крестовська зазначає, що контрольну гілку державної влади становлять органи, що перевіряють законність діяльності державних органів, підприємств та установ, а також у визначених законом випадках – усіх інших суб'єктів права [43, с. 52-54].

Ф. Ф. Бутинець розкриває юридичний зміст контролю як одного з видів реалізації повноважень державних і недержавних утворень, тлумачачи його як систематичне спостереження і перевірку процесу функціонування відповідного об'єкта з метою виявлення відхилень від заданих параметрів [44, с. 9-10]. Автор стверджує, що сутність контролю полягає безпосередньо у тому, що наглядовий орган здійснює перевірку з урахуванням того, чи виконує об'єкт управління його настанови.

М. М. Терещенко визначає державний контроль як форму реалізації державного управління, що забезпечує перевірку виконання законів та інших нормативних актів із метою недопущення відхилень від встановлених норм і правил. Автор розглядає контроль як особливу функцію держави, яка виражається в діяльності її органів і спрямована на отримання та аналіз інформації про процеси та явища, що відбуваються в суспільстві, встановлення порушень і відхилень від нормативних і індивідуальних приписів [45, с. 120].

Узагальнюючи наведене, доктрина адміністративного права традиційно визначає контроль як систематичну та ініціативну діяльність уповноваженого суб'єкта щодо встановлення відповідності об'єкта контролю законодавчим нормам із можливістю безпосереднього впливу.

Водночас ні спеціальне інформаційне законодавство, ні загальне вітчизняне законодавство не містять окремого нормативного визначення поняття контролю за обробкою персональних даних. У літературі такий контроль подеколи ототожнюють із державним наглядом (контролем), що є хибним з огляду на таке. По-перше, Закон України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності» визначає державний нагляд (контроль) як діяльність уповноважених законом органів виконавчої влади та місцевого самоврядування щодо виявлення і запобігання порушенням вимог законодавства суб'єктами господарювання [46].

По-друге, за правовим статусом, визначеним статтями 55 та 101 Конституції України, а також законами України «Про Уповноваженого Верховної Ради України з прав людини» [78] та «Про захист персональних даних», Уповноважений є окремою посадовою особою, що здійснює діяльність незалежно від інших державних органів, не належить ні до органів виконавчої влади, ні до органів місцевого самоврядування, а отже, не може бути віднесений до органів державного нагляду (контролю) у розумінні згаданого нормативно-правового акту.

Цю тезу підтверджує й те, що в умовах воєнного стану Офіс Омбудсмана фактично залишається єдиним суб'єктом, який на постійній основі продовжує здійснювати заходи контролю, тоді як урядові контролюючі органи припинили виконання відповідних функцій на підставі Постанови Кабінету Міністрів України 13 березня 2022 року № 303 «Про припинення заходів державного нагляду (контролю) в умовах воєнного стану» [47].

Таким чином, сутність поняття «контроль за обробкою персональних даних» не є співмірною до загального визначення державного контролю. Вказане обґрунтовується наступним.

По-перше, об'єкт контролю є динамічним і технологічно непрозорим. На відміну від будівельної конструкції чи харчового продукту, алгоритм обробки персональних даних не може бути перевірений зовнішнім спостерігачем без спеціальних технічних інструментів і доступу до

внутрішньої архітектури системи. Класична перевірка є неспроможною виявити порушення у системах профілювання, автоматизованого прийняття рішень або навчання моделей штучного інтелекту.

По-друге, шкода від порушення є миттєвою і часто непоправною. На відміну від порушення у сфері стандартів будівництва або безпечності харчових продуктів, яке можна усунути після виявлення, незаконне поширення персональних даних або неправомірне формування профілю особи створює наслідки – стигматизацію, дискримінацію, репутаційну шкоду – які не завжи можуть бути скасовані ретроактивно. Це вимагає превентивної, а не реактивної моделі контролю.

По-третє, суб'єктний склад контрольних відносин є багаторівневим і транскордонним. Обробка персональних даних нерідко здійснюється ланцюгом суб'єктів (для прикладу, такими як володілець персональних даних, розпорядник персональних даних, зокрема які забезпечують використання хмарної інфраструктури та розміщені у різних юрисдикціях). Відтак класична модель нагляду «наглядовий орган – підконтрольний суб'єкт» є архітектурно неспроможною у цих умовах.

Отже в українській правовій системі контроль за обробкою персональних даних має окремі індивідуальні ознаки, які визначаються сферою суспільних відносин, обсягом та характером контрольних заходів, колом осіб щодо яких заходи контролю здійснюються, та, власне, особливим складом уповноважених суб'єктів контролю.

З урахуванням цього у межах дослідження вперше пропонується авторське визначення цього поняття: контроль за обробкою персональних даних – це здійснювана на систематичній основі або за зверненням діяльність уповноважених суб'єктів, спрямована на встановлення відповідності обробки персональних даних вимогам законодавства та на захист прав суб'єктів персональних даних, із застосуванням засобів впливу.

Запропоноване визначення відмежовує контроль за обробкою даних від державного нагляду (контролю) за ознаками: ширшого кола суб'єктів, що не

зводиться до органів виконавчої влади, сферозалежним характером його конфігурації та настання юридичних наслідків у вигляді застосування засобів впливу – від юридичних санкцій до репутаційного чи морально-етичного осуду.

Звідси випливає, що контроль за обробкою персональних даних належить до правових явищ, зміст яких не вичерпується діяльністю єдиного спеціально уповноваженого органу.

Попри усталене уявлення, що такий контроль реалізується насамперед Уповноваженим Верховної Ради України з прав людини, а захист прав суб'єктів даних забезпечується судом, фактична система контролю є складнішою та структурно неоднорідною. Її неоднорідність зумовлена тим, що право на захист персональних даних не є відокремленим, самодостатнім правом, а становить складову ширшого права на повагу до приватного життя, гарантованого статтею 8 Конвенції про захист прав людини і основоположних свобод [19].

Саме тому обробка персональних даних відбувається не в абстрактному правовому просторі, а в межах конкретних сфер суспільних відносин – медійної, банківської, медичної, адвокатської, трудової тощо, кожна з яких має власний правовий режим та власну логіку допустимого втручання у приватність.

Для прикладу, можна розглянути системи таких сфер, як медійна, банківська, медична, адвокатська, трудова тощо, кожна з яких має власний правовий режим та власну логіку допустимого втручання у приватність, а відповідно і власний склад контролюючих суб'єктів.

Для коректного відображення цієї структури доцільно розмежувати три самостійні класифікаційні площини, які в науковій літературі нерідко змішуються: види контролю, форми контролю та сферу суспільних відносин як наскрізний чинник їх конфігурації.

Найзагальніший поділ контролю за обробкою персональних даних здійснюється за критерієм належності суб'єкта контролю до підконтрольної особи.

Означений принцип достатньою мірою корелюється із визначеним у першій редакції Закону України «Про захист персональних даних» переліком осіб, які здійснюють контроль за обробкою персональних даних.

За цим критерієм розрізняють зовнішній і внутрішній контроль. Зовнішній контроль здійснюється незалежним зовнішнім суб'єктом, який не входить до структури володільця (розпорядника) персональних даних. *Внутрішній контроль* здійснюється в межах самого володільця – за ініціативою його керівництва та, як правило, силами спеціально призначеної посадової особи (зокрема, відповідального за захист персональних даних) на підставі внутрішніх політик і процедур. *Зовнішній контроль*, своєю чергою, здійснюється з метою об'єктивної оцінки діяльності володільця або розпорядника персональних даних незалежним суб'єктом, який не бере участі у внутрішній організації процесів обробки даних, та спрямований на забезпечення дотримання вимог законодавства, захист прав суб'єктів персональних даних і запобігання неправомірному використанню інформації, може застосовувати зовнішні санкції до суб'єкта щодо якого контрольні функції реалізуються (так званий об'єкт перевірки).

За критерієм природи суб'єкта, що здійснює контроль, доцільно виокремлювати наступні види: державний контроль, що здійснюється органами державної влади загальної компетенції (національним наглядовим органом таким як Уповноважений Верховної Ради України з прав людини в Україні або Національна комісія з питань інформатики і свобод у Франції); секторальний контроль спеціальних державних регуляторів у межах окремої сфери; самоврядний професійний контроль з боку органів самоврядування професійних спільнот; саморегулювання, тобто контроль з боку етичних органів, утворених самою професійною спільнотою, рішення яких мають морально-етичну силу; а також громадський контроль, що здійснюється як

громадянами в індивідуальному порядку, так і громадськими та іншими недержавними організаціями у межах статутної діяльності, а також медіа, які виконують функцію суспільного нагляду за діяльністю органів влади та інших суб’єктів.

Зазначені різновиди різняться не лише суб’єктом, але й природою владного впливу – від застосування юридичних санкцій до суто репутаційного чи морально-етичного осуду.

Форму контролю розмежовують за способом проведення – на виїзний, що здійснюється безпосередньо за місцезнаходженням володільця або розпорядника, та невиїзний (безвиїзний, документальний), що здійснюється за місцем розташування контролюючого суб’єкта на підставі поданих документів, пояснень і відомостей.

Поряд із формою контроль класифікують за іншими, самостійними критеріями: за стадією здійснення – на попередній, поточний та наступний; за підставою (приводом) ініціювання – на ініціативний, що здійснюється за власною ініціативою контролюючого суб’єкта, та контроль за скаргою, ініційований зверненням суб’єкта персональних даних або іншої заінтересованої особи.

За періодичністю та підставами призначення виділяють планові та позапланові заходи контролю; за послідовністю проведення – на первинний та повторний (зокрема спрямований на перевірку усунення раніше виявлених порушень); за обсягом предмета – на цільовий (тематичний), що стосується окремої операції чи аспекту обробки, та загальний (комплексний), що охоплює обробку персональних даних у повному обсязі.

Зазначені форми, стадії та підстави є відносно універсальними, однак їх застосовність і співвідношення суттєво різняться залежно від сфери: там, де переважає попередній контроль (наприклад, через попереднє погодження умов обробки), ризики для приватності мінімізуються ще до моменту втручання, тоді як домінування наступного контролю переносить акцент на реагування за вже наявними наслідками.

Окремої уваги заслуговує визначення сфери суспільних відносин як чинник контролю. Так, сфера суспільних відносин – є тим чинником, що надає системі контролю секторального характеру.

Її значення зумовлене тим, що в окремих сферах персональні дані тісно переплітаються із суміжними правовими режимами захищеної інформації, розглянутих у підрозділі 1.1.

Так, у банківській сфері обробка персональних даних значною мірою охоплюється режимом банківської таємниці [48]. Контроль у цій сфері – у межах захисту прав споживачів фінансових послуг та регулювання поведінки банків і небанківських фінансових установ – здійснює Національний банк України. Особливість секторального контролю тут полягає в тому, що банківська таємниця є ширшою за персональні дані категорією, оскільки охоплює, зокрема, відомості про операції та рахунки, у тому числі юридичних осіб [49]; тому наглядовий вплив Національного банку поширюється на обробку персональних даних лише в тій частині, у якій вона перетинається з режимом банківської таємниці та вимогами щодо захисту прав клієнтів. Інструментами контролю виступають банківський нагляд, а формами реалізації контрольно-наглядових повноважень – перевірки та виїзне інспектування, передбачені банківським законодавством [50, с. 5].

В адвокатській діяльності суміжним правовим режимом захисту персональних даних є адвокатська таємниця, контроль за дотриманням якої забезпечують органи адвокатського самоврядування. Зокрема, кваліфікаційно-дисциплінарна комісія адвокатури здійснює розгляд та притягнення адвоката до відповідальності за розголошення адвокатської таємниці або вчинення дій, що призвели до її розголошення [51].

Ця сфера контролю має самоврядну професійну природу: заходи контролю реалізуються не державним органом, а корпоративною спільнотою, і спрямовані радше на дисциплінарне реагування, ніж на захист персональних даних як такий. Як і в банківській сфері, мандат щодо персональних даних тут є похідним – він виникає лише в точці перетину адвокатської таємниці з

відомостями, що є персональними даними. У сфері медіа діє спеціальний режим, встановлений законодавством про медіа, який розглянуто далі як розгорнутий ілюстративний приклад.

Принципово важливо наголосити, що компетенція цих секторальних суб'єктів щодо персональних даних має похідний (вторинний) характер: вона виникає не з мандата на захист персональних даних як такого, а внаслідок перетину відповідного спеціального режиму (банківської, адвокатської таємниці, стандартів журналістської етики) зі сферою персональних даних та права на приватність.

Відмежування персональних даних від суміжних категорій, набуває практичного виміру: воно пояснює, чому той самий масив відомостей може одночасно перебувати у фокусі наглядового органу у сфері захисту даних і секторального регулятора у відповідній сфері.

Узагальнення викладеного дозволяє запропонувати п'ятирівневу типологію суб'єктів контролю за обробкою персональних даних, побудовану за критерієм природи суб'єкта та юридичної сили його рішень:

1) загальний регулятор (наглядовий орган) – Уповноважений Верховної Ради України з прав людини, що здійснює контроль за додержанням законодавства про захист персональних даних незалежно від сфери суспільних відносин;

2) секторальні державні регулятори, наділені санкційними повноваженнями у межах окремої сфери, – зокрема, Національна рада України з питань телебачення і радіомовлення у сфері медіа та Національний банк України у банківській сфері;

3) органи професійного самоврядування, що реалізують дисциплінарний контроль у межах відповідної професії, – зокрема, органи адвокатського самоврядування;

4) етичні органи саморегулювання, рішення яких мають морально-етичну, а не юридичну силу та спрямовані на формування професійних стандартів;

5) внутрішній самоконтроль володільця персональних даних – посадові особи, відповідальні за захист персональних даних особи, а також внутрішні політики та процедури обробки персональних даних.

Громадський контроль посідає в наведеній класифікації особливе місце. На відміну від інших видів, він не прив'язаний до окремої сфери, а здійснюється одночасно у двох площинах: щодо кожної окремої сфери (наприклад, моніторинг медійних, фінансових чи медичних практик) і щодо системи захисту даних загалом – як нагляд суспільства за тим, наскільки ефективно держава та інші суб'єкти забезпечують право на приватність.

Водночас громадськість не наділена владними повноваженнями отримувати доступ до персональних даних, проводити перевірки чи застосовувати санкції. Показовим прикладом є те, що попри широке залучення Уповноваженим Верховної Ради України з прав людини представників НУО до проведення моніторингових візитів та перевірок, що визначено низкою Регламентів Офісу Омбудсмана, Порядком здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних, затвердженого Наказом Уповноваженого Верховної Ради України з прав людини 08.01.2014 року № 1/02-14 [60] не передбачено залучення громадськості до вказаних заходів контролю.

З огляду на це громадський контроль є особливою формою квазіконтролю: він не замінює формальних контрольних механізмів, а діє опосередковано – через виявлення та оприлюднення порушень, формування суспільного запиту та ініціювання реагування уповноважених суб'єктів. Саме ця подвійність – наскрізність за відсутності владних повноважень – виправдовує виокремлення громадського контролю як самостійного елемента системи, що не зводиться до жодного з владних рівнів типології, наведеної раніше.

Слід наголосити, що запропонована вище типологія не передбачає ієрархічного підпорядкування рівнів: вони не заміщують, а доповнюють один одного, утворюючи в сукупності багаторівневу систему контролю.

Окремо від неї перебуває судовий захист, який, як обґрунтовано далі у підрозділі 2.2, є самостійною формою захисту прав суб'єктів персональних даних.

Принагідно слід наголосити, що наведена типологія відображає чинну модель контролю. У разі реалізації підготовлених окремих реформ та прийняття законопроєктів, які наразі перебувають на розгляді у Верховній Ради України, суттєво може бути реконфігуровано як суб'єктний склад (ідеться про можливе створення спеціалізованого незалежного наглядового органу відповідно до проєкту Закону про Національну комісію з питань захисту персональних даних та доступу до публічної інформації [52]),обсяг повноважень наглядового органу (наділення наглядового органу повним обсягом повноважень за статтею 58 GDPR), а також перегляду змісту окремих складових контролю, що перетинаються з іншими правовими категоріями (визначення у проєкті нового Цивільного кодексу України права на забуття як самостійної особистої немайнової гарантії [53]).

Найбільш показовою для ілюстрації запропонованої моделі є сфера медіа, у якій одночасно представлені чотири з п'яти виокремлених рівнів контролю та яка водночас породжує особливо гострі питання захисту прав найбільш вразливих суб'єктів даних – дітей.

У межах запропонованої секторальної моделі медіа постають не лише як володільці персональних даних (мова йдеться про категорію персональних даних, яка охоплює не співпробітників та контрагентів медіа, а фізичних осіб щодо яких здійснюється обробка персональних даних з метою поширення в медіа), але і як елемент багаторівневої системи контролю, у якій поєднуються державний секторальний регулятор, професійне самоврядування, етичні органи саморегулювання та внутрішній контроль редакцій.

Розгляд цієї сфери дозволяє продемонструвати, як абстрактна типологія втілюється у конкретному правовому режимі, і виявити прогалини, що потребують усунення.

Така публічність створює значні ризики для реалізації фундаментального права дитини на приватність, особливо у випадках, коли медіа висвітлюють історії дітей із метою привернення уваги до суспільно важливих проблем, не враховуючи потенційних негативних наслідків для самих дітей.

Особливої гостроти питання набуває з огляду на чутливість обробки персональних даних у медіа. А саме, виразно постає проблема недопущення перевищення контролюючим органом меж своєї діяльності та сприйняття контрольних заходів як одного зі способів тиску з боку держави.

Водночас дедалі частіше об’єктом журналістського інтересу стають діти – як учасники або свідки подій, пов’язаних із порушенням прав людини, насильством, переміщенням унаслідок збройного конфлікту, інституційним доглядом або іншими соціально чутливими обставинами.

Відео- та фотозйомка як форми фіксації зображення особи розглядаються в сучасному правовому дискурсі як різновид діяльності, пов’язаної зі збиранням та подальшою обробкою персональних даних. Така діяльність підпадає під сферу регулювання Закон України «Про захист персональних даних» [10], який визначає правові підстави, принципи та межі допустимого втручання у сферу приватності.

Право на свободу вираження поглядів закріплене у статті 10 Європейській конвенції з прав людини [19]. Воно є одним із ключових елементів демократичного суспільства та передбачає свободу отримувати й поширювати інформацію без втручання з боку держави. Водночас це право не є абсолютним.

Частина друга статті 10 передбачає можливість обмеження права на свободу вираження, зокрема для захисту прав інших осіб [19].

Контроль за дотриманням вимог щодо обробки персональних даних дітей у медіа реалізується одночасно на кількох рівнях запропонованої у підрозділі 2.1 типології.

На рівні секторального державного регулятора відповідні повноваження здійснює Національна рада України з питань телебачення і радіомовлення, уповноважена реагувати на порушення законодавства про медіа; згідно з пунктом 11 частини десятої статті 110 Закону України «Про медіа» [54], до значних порушень належить розголошення інформації про дитину без письмової згоди хоча б одного з батьків або інших законних представників, окрім випадків, коли це здійснюється в найкращих інтересах дитини.

На рівні саморегулювання діють етичні органи журналістської спільноти. Ще у 2011 році Уповноважений Верховної Ради України з прав людини [55] наголошувала на необхідності розроблення та запровадження Кодексу поведінки для засобів масової інформації на виконання Закону України «Про захист персональних даних». Так, Кодекс етики українського журналіста був затверджений 12 грудня 2013 року на пленумі Національної спілки журналістів України [56] та вимагає особливої обережності при висвітленні питань, пов’язаних із дітьми, та неприпустимості розкриття імен неповнолітніх, причетних до протизаконних дій чи подій, пов’язаних із насильством; рішення таких органів мають морально-етичну, а не юридичну природу.

На рівні громадського контролю діють медійні об’єднання, неурядові організації та експертні спільноти. На рівні внутрішнього самоконтролю ключову роль відіграють редакційні політики.

Додаткові запобіжники передбачені профільним законодавством. Стаття 10 Закону України «Про охорону дитинства» [57] забороняє розголошення чи публікацію будь-якої інформації про дитину, що може спричинити їй шкоду, без згоди законного представника дитини.

Проведений аналіз дозволяє стверджувати, що контроль за обробкою персональних даних має сферозалежний (секторальний) характер: його

конфігурація – коло суб'єктів, обсяг повноважень та застосовні форми – визначається сферою суспільних відносин, у межах якої здійснюється обробка.

Запропоновано п'ятирівневу типологію суб'єктів контролю (загальний регулятор; секторальні державні регулятори; органи професійного самоврядування; етичні органи саморегулювання; внутрішній самоконтроль володільця), у якій компетенція секторальних суб'єктів щодо персональних даних має похідний характер та виникає внаслідок перетину спеціальних правових режимів зі сферою персональних даних.

Отже, сфера медіа є репрезентативним прикладом цієї моделі, оскільки в ній одночасно діють чотири рівні контролю, включаючи секторальний державний регулятор (Національна рада України з питань телебачення і радіомовлення), професійне самоврядування, етичні органи саморегулювання та внутрішній контроль редакцій.

Вказане засвідчує, що визначення законності та допустимості публікації інформації про неповнолітню особу не може зводитися лише до формальної перевірки двох обставин – наявності згоди на обробку персональних даних чи існування суспільного інтересу. Йдеться про багаторівневу оцінку, в межах якої критерії суспільної значущості, необхідності та пропорційності застосовуються послідовно й доповнюються аналізом того, у який спосіб інформацію було одержано, в якій формі її подано та які наслідки її оприлюднення може мати для дитини.

Разом із тим, у діяльності медіа важливо також запровадити ряд внутрішніх запобіжників, спрямованих на інтеграцію у редакційну політику медіа процедур Child safeguarding. Важливим елементом, на думку автора, є й громадський контроль – залучення членів громадянського суспільства (зокрема, з числа представників неурядового сектору) задля проведення оцінки ризиків порушення прав дитини внаслідок публікації, з'ясування обґрунтованості або надмірності втручання у приватне життя.

2.2. Система суб'єктів контролю за дотриманням законодавства про обробку персональних даних в Україні

Характерно, що у перший рік дії Закону України «Про захист персональних даних» здійснення контролю у цій сфері набуло ознак паралельної інституційної конструкції. Так, парламентський контроль здійснювався Уповноваженим Верховної Ради України з прав людини на підставі статті 22 вказаного Закону (у першій редакції – від 01 червня 2010 року), тоді як спеціалізований контроль за додержанням законодавства про захист персональних даних відповідно пунктів першого та другого цієї ж статті – здійснювався Державною службою України з питань захисту персональних даних [58] як уповноваженим державним органом з питань захисту персональних даних, а також іншими органами державної влади та органами місцевого самоврядування. При цьому взаємодія між зазначеними суб'єктами носила неформальний характер і лише перебувала на стадії організаційного оформлення [55].

Важливим етапом інституційного розвитку української системи контролю за обробкою персональних даних стало передання з 1 січня 2014 року функцій контролю за додержанням законодавства у цій сфері Уповноваженому Верховної Ради України з прав людини, що відповідає європейській моделі незалежного наглядового органу. Передумовою зазначеному стала ратифікація Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних.

Державна служба України з питань захисту персональних даних як урядовий орган, діяльність якого спрямовувалась і координувалася Кабінетом Міністрів України через Міністра юстиції України [59], у зв'язку із чим його незалежність не була абсолютною, зважаючи на координацію дій Урядом, підзвітність та залежну від Уряду систему фінансування, процедуру

призначення та звільнення (Президентом України за поданням Прем'єр-міністра України).

Покладання функцій наглядового органу у сфері захисту персональних даних на Уповноваженого Верховної Ради України з прав людини призвело до наділення Омбудсмана України широкими повноваженнями у сфері захисту персональних даних, які у статті 23 Закону України «Про захист персональних даних» перелічені як чотирнадцять пунктів повноважень.

На практиці, функції здійснення контролю за захистом персональних даних виконує відділ у сфері захисту персональних даних Департаменту моніторингу інформаційних прав, а також регіональні представництва Уповноваженого Верховної Ради України з прав людини.

Надалі запропоновано класифікацію повноважень Уповноваженого, з огляду на функціональне призначення, юридичну природу наслідку для, стадію контрольного циклу, на якій повноваження реалізується (превентивна, розслідувальна, коригувальна, постконтрольна).

Так, до владно-розпорядчих повноважень (пункти 5, 10) віднесено право видавати обов'язкові для виконання приписи про запобігання або усунення порушень, включно зі зміною, видаленням чи знищенням даних, забороною надання даних третій особі, зупиненням чи припиненням обробки (п. 5), а також право складати протоколи про адміністративну відповідальність і направляти їх до суду (п. 10). Саме ця група становить ядро примусового впливу як наглядового органу.

Зважаючи на те, що Уповноважений є єдиним органом, який здійснює контроль за захистом персональних даних, реалізуючи зазначені вище функції та здійснюючи аналіз правозастосування, основних проблем у законодавстві, Уповноваженому надані повноваження надавати рекомендації щодо практичного застосування законодавства про захист персональних даних, роз'яснювати права і обов'язки [166]. Відтак дорадчо-роз'яснювальні повноваження (пункти 6, 9, 11) передбачають як надання рекомендацій щодо практичного застосування законодавства (п. 6), висновків щодо проєктів

кодексів поведінки (п. 9), так і інформування про законодавство та права суб'єктів (п. 11).

Ці повноваження не породжують обов'язкових наслідків і функціонують у режимі м'якого впливу. Водночас вказані повноваження кореспондуються безпосередньо метою парламентського контролю за додержанням конституційних прав і свобод людини і громадянина, які здійснює Уповноважений та визначені у статті 3 Закону (зокрема, сприяння правовій інформованості населення).

Повноваження щодо розгляду звернень (п. 1) передбачають отримання пропозицій, скарг, звернень та прийняття рішень за результатами їх розгляду – окрема процесуальна група, що формує канал доступу суб'єкта даних до захисту.

Координаційно-інституційні повноваження (п. 7) визначають взаємодію зі структурними підрозділами та відповідальними особами володільців/розпорядників, оприлюднення інформації про них – повноваження, спрямоване на побудову інституційної мережі контролю на рівні підконтрольних суб'єктів.

Нормотворчі повноваження (п. 4) виходять за межі суто контрольної функції й передбачають право Уповноваженого затверджувати нормативно-правові акти у сфері захисту персональних даних у випадках, передбачених Законом України «Про захист персональних даних».

Водночас повноваження законодавчої ініціативи (п. 8) включають у себе можливість звернення з пропозиціями щодо прийняття або зміни нормативно-правових актів до Верховної Ради України, Президента України, Кабінету Міністрів України, інших державних або органів місцевого самоврядування, а також їхніх посадових осіб – повноваження непрямого впливу на нормотворчий процес.

Аналітичні повноваження (п. 12) передбачають моніторинг нових практик, тенденцій і технологій захисту персональних даних – превентивно-дослідницька функція.

Повноваження із міжнародного співробітництва (пункти 13, 14) включають в себе організацію взаємодії з іноземними суб'єктами, виконання Конвенції №108 та Додаткового протоколу, участь у роботі міжнародних організацій.

Насамкінець, розслідувальні повноваження (пункти 2, 3) охоплюють право проведення виїзних і невиїзних, планових і позапланових перевірок із забезпеченням доступу до приміщень (п. 2), а також право вимагати й отримувати доступ до будь-якої інформації, документів, баз даних, картотек, включно з інформацією з обмеженим доступом (п. 3). Це класичні інструменти встановлення фактичних обставин, що передують застосуванню коригувального заходу.

Рис. 2. Види та типи перевірок щодо обробки персональних даних (авт.)

Слід зауважити, що структура повноважень за статтею 23 Закону України «Про захист персональних даних» [10] в розслідувальному та дорадчому вимірах загалом відповідає універсальному стандарту, втіленому в статті 58 GDPR, однак демонструє системне ослаблення в коригувально-

санкційному вимірі (відсутність права самостійного накладення штрафу, недеталізована шкала заходів) і водночас непропорційне розширення в нормотворчому вимірі, що не має прямого відповідника в жодній із трьох порівнюваних юрисдикцій і потребує окремого критичного осмислення з позицій доктрини інституційної незалежності наглядового органу.

Процедура організації та проведення перевірок регулюється Порядком здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних, затверджений наказом Уповноваженого від 08.01.14 №1/2-14 [60].

Предметом перевірки та/або моніторингового візиту є додержання суб'єктом перевірки під час здійснення обробки персональних даних вимог Конституції України, Закону України «Про захист персональних даних», Типового порядку обробки персональних даних, затверджений наказом Уповноваженого від 08.01.14 №1/2-14 (далі – Типовий порядок), а також чинних міжнародних договорів України у сфері захисту персональних даних, згода на обов'язковість яких надана Верховною Радою України.

Планові перевірки проводяться відповідно до планів, які підлягають затвердженню Уповноваженим Верховної Ради України з прав людини, у якому зазначаються категорії суб'єктів перевірок або конкретні суб'єкти. Після затвердження Омбудсманом України, відповідний план підлягає розміщенню на веб-сайті в мережі Інтернет.

Чіткий перелік, коли працівники Секретаріату Уповноваженого можуть здійснювати позапланові виїзні та безвиїзні перевірки, визначений у підпункті 4.1 Порядку контролю, зокрема такі перевірки можуть проводитись за наявності наступних підстав [60]:

- ініціатива Уповноваженого Верховної Ради України з прав людини щодо необхідності здійснення контрольного заходу;
- самостійне виявлення Омбудсманом України фактів ймовірного порушення вимог законодавства у сфері захисту персональних даних, у тому

числі під час здійснення аналізу системних проблем забезпечення права на приватність та повагу до приватного і сімейного життя;

- отримання інформації про можливі порушення законодавства про захист персональних даних із відкритих джерел, зокрема медіа;
- надходження обґрунтованих звернень фізичних або юридичних осіб щодо можливого порушення володільцями та/або розпорядниками персональних даних вимог законодавства;
- встановлення, що на письмовий запит Уповноваженого під час проведення безвиїзної перевірки суб'єктом перевірки подані недостовірності відомостей (або неможливість на підставі таких відомостей оцінити дотримання вимог законодавства);
- здійснення контролю за виконанням приписів про усунення порушень, виданих за результатами попередніх перевірок.

Важливо звернути увагу, що позапланова перевірка у сфері захисту персональних даних є формою зовнішнього контролю, у межах парламентського контролю, що застосовується не лише як реакція на вже встановлені порушення, а й як превентивний механізм запобігання порушенням права особи на приватність.

У межах здійснення контрольних повноважень уповноважені посадові особи Секретаріату Уповноваженого наділені правом доступу до документів та інформації, необхідних для проведення перевірки, у тому числі інформації з обмеженим доступом, а також мають право отримувати доступ до приміщень, у яких здійснюється обробка персональних даних, та отримувати належним чином засвідчені копії документів.

За результатами проведеної перевірки відповідними посадовими особами складається акт, де уповноваженою особою Офісу Омбудсмана зазначається інформація щодо отриманих у ході перевірки документів та інформації щодо встановлених під час перевірки фактів та обставин, висновків щодо наявності та/або відсутності порушень законодавства про захист персональних даних [60].

Припис про усунення порушення законодавства з питань захисту персональних даних виноситься у зв’язку з наявними порушеннями вимог законодавства, метою винесення якого є усунення таких порушень, виправлення порушення, усунення обставин, що спричинили вчинення порушення та/або можуть вчинюватися в майбутньому [60].

Водночас відповдіно до профільного законодавства [10], Уповноваженим Верховної Ради України з прав людини також можуть надаватися рекомендації щодо організації обробки та захисту персональни даних.

Як вже зазначалося, окрім Уповноваженого Верховної Ради України з прав людини, відповідно до статті 22 Закону України «Про захист персональних даних», контроль за додержанням законодавства про захист персональних даних здійснюють суди [78].

Отже Закон України «Про захист персональних даних» формально відносить суди до переліку суб’єктів контролю за додержанням законодавства про захист персональних даних поряд з Уповноваженим Верховної Ради України з прав людини.

Подібна законодавча конструкція, однак, приховує концептуальну підміну: ототожнення двох принципово різних правових функцій – адміністративного контролю як безперервної, ініціативної, наглядової діяльності та правосуддя як реактивної форми вирішення вже виниклого юридичного спору. Включення судів до переліку суб’єктів контролю є юридично некоректним узагальненням, яке потребує доктринального уточнення.

У вітчизняній адміністративно-правовій доктрині державний контроль традиційно визначається через сукупність ознак, які формують його як самостійний вид публічно-владної діяльності: систематичність (постійний, а не одноразовий характер), ініціативність (контролюючий суб’єкт діє за власною ініціативою, а не за зверненням), превентивність (спрямованість на запобігання порушенням до їх настання), а також можливість прямого

втручання в діяльність підконтрольного суб’єкта без попереднього юридичного спору.

Саме ці риси характеризують діяльність Уповноваженого Верховної Ради України з прав людини: проведення планових і позапланових перевірок, моніторинг практики обробки персональних даних, видання приписів про усунення порушень.

Натомість судова діяльність структурно протилежна. Суд, як справедливо зазначають дослідники адміністративного судочинства, реалізує функцію *правосуддя* – особливого виду державної діяльності, що полягає в розгляді та вирішенні правового спору на засадах змагальності, диспозитивності та незалежності [61]. Принципова відмінність контролю від судового розгляду полягає в тому, що контроль є превентивно-наглядовим і реалізується незалежно від волевиявлення підконтрольної чи зацікавленої особи, тоді як судовий розгляд ініціюється виключно актом волевиявлення заінтересованої сторони (позовом, скаргою, заявою).

Відповідно, суд апріорі не може вважатися органом контролю в адміністративно-наглядовому значенні, оскільки: (а) не діє за власною ініціативою (принцип диспозитивності прямо це виключає); (б) не здійснює постійного моніторингу сфери обробки персональних даних; (в) його втручання має казуальний, а не системний характер – стосується конкретного правовідношення, а не галузі загалом.

Функціональне навантаження Уповноваженого Верховної Ради України з прав людини в досліджуваній сфері охоплює: виявлення порушень (через перевірки та моніторинг), отримання й аналіз інформації про стан обробки персональних даних, оперативне реагування (приписи, протоколи про адміністративні правопорушення), а також формування єдиної правозастосовної практики для суб’єктів обробки. Це класична модель адміністративного нагляду, відома міжнародному праву захисту даних як діяльність наглядового органу (DPA).

Суди, своєю чергою, виконують функції: розгляду конкретного спору, оцінки доказів у межах предмета доказування, встановлення факту порушення в межах заявлених вимог та застосування юридичних наслідків (відновлення права, стягнення компенсації, притягнення до відповідальності).

Структурну обмеженість такої моделі визнає й сама держава: у Білій книзі з регулювання штучного інтелекту наголошено, що в цифровому середовищі заборона та подальший судовий захист не забезпечують ефективного контролю [62, с. 16].

Окремо слід наголосити на принциповій відмінності – об'єкті контролюючого впливу. Омбудсман України контролює діяльність суб'єкта обробки персональних даних як таку – тобто оцінює систему, процеси, технічні й організаційні заходи. Судовий орган натомість контролює законність поведінки сторін виключно в межах конкретної справи й тільки тих фактичних обставин, які стали предметом судового розгляду. Він не оцінює систему обробки персональних даних загалом, навіть якщо з матеріалів справи випливають системні недоліки – для цього в нього немає ні процесуального інструментарію, ні легітимації.

Принципи змагальності та диспозитивності, закріплені в процесуальному законодавстві [187], є структурним обмежувачем будь-якої спроби розглядати суд як орган контролю.

Змагальність передбачає, що тягар ініціювання процесу, формулювання вимог і доведення обставин справи покладається на сторони, а суд виконує роль арбітра, обмеженого межами заявлених вимог (за виключенням окремих категорій справ з офіційним з'ясуванням обставин).

Змоделюємо ситуацію: особа вважає, що її персональні дані обробляються незаконно або поширені без правової підстави, однак: не звертається до Уповноваженого; не подає позов; не звертається до правоохоронних органів. У цій ситуації об'єктивне порушення законодавства про захист персональних даних існує, проте жоден суд не може самостійно його виявити, розпочати провадження і припинити порушення.

Це прямо суперечить самій природі контролю, якому за визначенням властива активна позиція суб’єкта контролю.

Особливого аналізу потребує участь суду в розгляді справ про адміністративні правопорушення у сфері захисту персональних даних.

Зокрема, звернення до практики судового контролю за постановами органів публічної адміністрації [63, с. 123] дозволяє екстраполювати загальні висновки й на цю сферу: суд, розглядаючи протокол про адміністративне правопорушення, перевіряє законність і обґрунтованість конкретного акта притягнення до відповідальності – повноту з’ясування обставин, достатність доказової бази, дотримання процедурних вимог.

Вказане може вважатися судовим контролем за законністю акта правозастосування, однак не може вважатися самостійним контролем за станом дотримання законодавства про захист персональних даних загалом.

При цьому, навіть якщо вважати відсоток протоколів про адміністративні правопорушення, за якими суд не ухвалив рішення про притягнення особи до відповідальності таким, що свідчить про якість роботи суб’єкта владних повноважень, який складає протоколи (за аналогією з висновками щодо практики Національної поліції України), сам суд при цьому не формує і не реалізує наглядову політику в галузі захисту персональних даних – він лише оцінює правомірність конкретного акта реагування на конкретне порушення, а межі повноважень суду обмежені.

Щодо співвідношення повноважень Уповноваженого та суду при вирішенні питання про відповідальність за порушення законодавства про захист персональних даних слід звернути увагу на наступному. Дійсно, пунктом 8 статті 8 Закону України «Про захист персональних даних» передбачено, право особи на оскарження обробки своїх персональних даних до Уповноваженого або до суду [10].

Втім, звернення до Уповноваженого є позасудовим способом захисту, який не скасовує право звернення до суду. Реалізуючи функцію парламентського контролю Уповноважений не діє як судовий орган влади, не

підміняє його, отже – не виконує функцію суду, діючи у межах власних повноважень та завдань.

Розмежування повноважень Уповноваженого та суду в частині притягнення до адміністративної відповідальності чітко визначені Кодексом України про адміністративні правопорушення, пунктом 8-1 частини першої статті 255 якого уповноважені особи Секретаріату Уповноваженого або представники Уповноваженого наділені правом складати протоколи про адміністративні правопорушення за статтею 188-40 Кодексу України про адміністративні правопорушення, а повноваження з розгляду справ, відповідно до положень Кодексу України про адміністративні правопорушення, віднесено до компетенції суддів районних, районних у місті, міських чи міськрайонних судів.

При цьому, враховуючи, що при вирішенні питання про притягнення особи до адміністративної відповідальності, Уповноважений, уповноважені особи Секретаріату Уповноваженого та представники Уповноваженого обмежені, зокрема, правом на складання протоколів (формуванням справ про адміністративні правопорушення [64].

Отже, відповідно до усталеної практики, Уповноважений є ініціатором притягнення до адміністративної відповідальності.

У кримінально-правовому вимірі суд відіграє роль гаранта прав особи при розгляді справ про незаконне втручання в приватне життя, незаконне збирання, використання чи поширення персональних даних (статті Кримінального кодексу України, що кореспондують зі статті 32 Конституції України). Однак і тут функціональна природа судової діяльності залишається незмінною: суд реагує на вже виявлене, оформлене у процесуальний спосіб (обвинувальний акт, заява потерпілого) порушення, але не здійснює системного контролю за діяльністю суб’єктів обробки персональних даних.

Шкелебей О.В. приходить до висновку, що ключовими суб’єктами реалізації судового контролю в публічно-правових відносинах є адміністративні суди [65, с. 267-268]. Їх діяльність спрямована на вирішення

спорів між громадянами та суб'єктами владних повноважень, а також на перевірку законності рішень, дій чи бездіяльності останніх.

Особливий акцент доречно поставити на тому, що адміністративні суди не лише відновлюють порушені права, але й формують практику застосування норм права, що сприяє зміцненню правопорядку. Відтак, судовий контроль в адміністративному судочинстві виступає важливим елементом демократичного суспільства, який забезпечує належне функціонування механізму захисту прав людини у публічно-правовій сфері.

Показовим у цьому контексті є інститут судового контролю на стадії досудового розслідування – діяльність слідчого судді, який санкціонує процесуальні дії, пов'язані з втручанням у приватну сферу (доступ до речей і документів, негласні слідчі (розшукові) дії), та перевіряє законність такого втручання [66].

Цей вид судового контролю принципово відрізняється від адміністративно-наглядового контролю: він є вузько процесуальним, спрямованим на санкціонування конкретної процесуальної дії в межах конкретного кримінального провадження, а не на оцінку стану дотримання прав суб'єктів персональних даних у суспільстві загалом.

Очевидним є висновок, що слідчий суддя не може з власної ініціативи виявити випадок незаконної обробки персональних даних і розпочати провадження – він діє виключно в реактивному режимі, в межах уже розпочатого кримінального провадження.

Окремої уваги заслуговує специфічний інститут – судовий контроль за виконанням судових рішень, закріплений у статтях 381-1–382-3 [67] Кодексу адміністративного судочинства України та відповідному розділі Цивільному процесуальному кодексі України [187].

Аналіз новел процесуального законодавства свідчить, що цей контроль включає повноваження суду зобов'язати суб'єкта владних повноважень подати звіт про виконання рішення, накласти штраф за невиконання, визнати протиправними дії, вчинені на виконання рішення суду [68]. Однак цей

контроль виникає лише після ухвалення рішення у справі, тобто є похідним від акта правосуддя, а не самостійною формою нагляду за сферою обробки персональних даних; стосується виключно виконання конкретного судового рішення, а не стану дотримання законодавства про захист персональних даних загалом.

Отже, контроль за виконанням рішення є контролем за власною діяльністю суду (за дотриманням обов'язковості судового акта), а не контролем за сферою захисту персональних даних як такою.

Ототожнення цих понять є методологічною помилкою, що змішує предмет контролю (виконання конкретного акта) з об'єктом галузевого регулювання (стан дотримання прав суб'єктів персональних даних).

Таким чином, пропонується вживати щодо суду термін не «суб'єкт контролю», а «суб'єкт судового захисту прав у сфері обробки персональних даних», що точніше відображає правову природу його діяльності та усуває концептуальну колізію між функціями контролю і правосуддя.

Відповідна термінологічна й змістова корекція законодавчої конструкції статті профільного закону є одним із напрямів удосконалення національного механізму захисту персональних даних, дослідженню яких присвячено розділ 3 цієї дисертаційної роботи.

2.3. Відповідальність за порушення законодавства про обробку персональних даних

Відповідно до статті 28 Закону України «Про захист персональних даних», порушення законодавства з питань захисту персональних даних тягне за собою відповідальність, встановлену законом.

Ця норма має бланкетний характер: вона не утворює самостійного складу правопорушення, а відсилає до галузевого законодавства, в якому й закріплено конкретні підстави, суб'єктів та санкції.

Аналіз нормативного матеріалу та правозастосовної практики свідчить, що з чотирьох видів відповідальності, перелічених у статті 28 Закону України

«Про захист персональних даних», реальним, статистично та судово підтвердженим механізмом реагування на порушення законодавства про обробку персональних даних є адміністративна відповідальність.

Так, особи, винні в порушенні законодавства про захист персональних даних, притягаються до дисциплінарної, цивільно-правової, адміністративної або кримінальної відповідальності згідно із законом.

Дисциплінарна відповідальність реалізується виключно в межах загальних норм трудового законодавства та локальних актів роботодавця, без спеціального складу, пов'язаного з персональними даними, а цивільно-правова відповідальність – у межах загальних деліктних норм Цивільного кодексу України, без сформованої судової практики саме у сфері персональних даних. Підтвердженням вказаному є і те, зокрема, що жодна з опрацьованих щорічних доповідей Уповноваженого Верховної Ради України з прав людини за 2013–2025 роки [69] не містить аналізу цивільних справ про відшкодування шкоди, завданої порушенням законодавства про захист персональних даних.

Кримінальна відповідальність реалізується через суміжні склади Кримінального кодексу України (статті 182, 361-2, 362) [70]. Статтею 182 Кримінального кодексу України передбачає відповідальність за порушення недоторканності приватного життя, а саме це стосується незаконного збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації, крім випадків, передбачених іншими статтями цього Кодексу, караються штрафом від п'ятисот до однієї тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або арештом на строк до шести місяців, або обмеженням волі на строк до трьох років.

Ті самі дії, вчинені повторно, або якщо вони заподіяли істотну шкоду охоронюваним законом правам, свободам та інтересам особи, - караються арештом на строк від трьох до шести місяців або обмеженням волі на строк від трьох до п'яти років, або позбавленням волі на той самий строк).

Також варто зауважити, що за незаконний вплив у будь-якій формі на Президента України, Голову Верховної Ради України, народного депутата України, Прем'єр-міністра України, члена Кабінету Міністрів України, Уповноваженого Верховної Ради України з прав людини або його представника, з метою перешкодити виконанню ними службових обов'язків або добитися прийняття незаконних рішень відповідно до статті 344 Кримінального кодексу України карається штрафом від 200 до 300 неоподатковуваних мінімумів доходів громадян або арештом на строк від 3 до 6 місяців, або обмеженням волі на строк до 2 років, або позбавленням волі на той самий строк.

Аналіз правозастосовної практики, відображеної у щорічних доповідях Уповноваженого [69; 71; 72; 73; 74; 83; 102; 181], свідчить про те, що стаття 182 Кримінального кодексу України застосовується переважно як інструмент реагування на ситуації, які за формальними ознаками підпадають під дію статті 188-39 Кодексу України про адміністративні правопорушення, але мають додаткову ознаку суспільної небезпечності, що виключає кваліфікацію як адміністративного правопорушення.

Так, у 2022 році за фактом неправомірного поширення персональних даних (розголошення медичної документації в соціальній мережі та оформлення фіктивних трудових відносин з використанням персональних даних іншої особи) відповідними управліннями поліції відкрито кримінальні провадження за частиною першою статті 182 Кримінального кодексу України. У листопаді 2023 року за фактом розміщення відеозапису, що містив персональні дані пацієнтів і свідчив про розголошення лікарської таємниці медичними працівниками, Головним управлінням Національної поліції в Одеській області відкрито кримінальне провадження за частиною першою статті 182 Кримінального кодексу України [73]. У 2024 році аналогічні кримінальні провадження відкрито за фактами незаконного оприлюднення в мережі Інтернет паспортних даних та адреси проживання заявника, а також за

фактом використання персональних даних громадянина для оформлення фіктивних трудових відносин з метою уникнення оподаткування [73].

Поряд зі статтею 182 Кримінального кодексу України, статті 361-2 та 362 цього ж Кодексу передбачають відповідальність за несанкціоноване розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах, автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, а також за несанкціоновані дії з такою інформацією, вчинені особою, яка має право доступу до неї [70].

Викладена в щорічній доповіді Уповноваженого за 2024 рік інформація про наймасштабнішу кібератаку на державні реєстри Міністерства юстиції України 19 грудня 2024 року, за фактом якої Службою безпеки України розпочато досудове розслідування, ілюструє застосування суміжних статей Кримінального кодексу України (зокрема статті 361) до посягань на інформаційні системи, що містять персональні дані в масовому масштабі [73].

Водночас стаття 188-39 Кодексу України про адміністративні правопорушення встановлює адміністративну відповідальність громадян, посадових осіб та суб'єктів підприємницької діяльності. Вказаним положенням передбачено відповідальність за:

1) неповідомлення або несвоєчасне повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних або про зміну відомостей, які підлягають повідомленню згідно із законом, повідомлення неповних чи недостовірних відомостей [80];

2) невиконання законних вимог (приписів) Уповноваженого Верховної Ради України з прав людини або визначених ним посадових осіб секретаріату Уповноваженого Верховної Ради України з прав людини щодо запобігання або усунення порушень законодавства про захист персональних даних [80];

3) недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до

незаконного доступу до них або порушення прав суб'єкта персональних даних [80];

4) повторне вчинення зазначених вище порушень, вчинених протягом року та за яке особу вже було піддано адміністративному стягненню.

Деталізуючи склад адміністративного правопорушення, передбаченого частиною 1 статті 188-39 Кодексу України про адміністративні правопорушення, слід зазначити, що його застосування пов'язане, зокрема, з невиконанням встановленого законом обов'язку щодо інформування Уповноваженого Верховної Ради України з прав людини про окремі випадки обробки персональних даних. Такий обов'язок закріплений у статті 9 Закону України «Про захист персональних даних», відповідно до якої володілець персональних даних має повідомити Уповноваженого про здійснення обробки персональних даних, якщо така діяльність може створювати підвищений ризик для прав і свобод суб'єктів персональних даних [10].

Вказаний механізм деталізовано Уповноваженим Верховної Ради України з прав людини у Порядку повідомлення про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, а також про структурний підрозділ або відповідальну особу, що забезпечує організацію роботи у сфері захисту персональних даних, затвердженому наказом від 8 січня 2014 року № 1/02-14 [74]. Таким чином, обов'язок повідомлення Уповноваженого виникає не щодо будь-якої діяльності з обробки персональних даних, а лише у випадках, коли характер такої обробки обумовлює потенційно підвищений рівень втручання у права та законні інтереси суб'єктів персональних даних.

Склад адміністративного правопорушення, передбаченого частиною 2 статті 188-39 Кодексу України про адміністративні правопорушення зводиться безпосередньо до умисного невиконання суб'єктом обробки персональних даних приписів, які були винесені внаслідок перевірок Омбудсмана України [80].

В контексті диспозиції цієї частини статті важливо розмежовувати вимоги Уповноваженого або уповноважених ним посадових осіб Секретаріату Уповноваженого, визначені у приписах та вимоги, визначені в листах та актах реагування (поданнях Уповноваженого), складених відповідно до статті 15 Закону України «Про Уповноваженого Верховної Ради України з прав людини» [78].

Відтак попередньо проаналізовані частини статті 188-39 Кодексу України про адміністративні правопорушення стосуються порушення володільцями персональних даних своїх зобов'язань перед Уповноваженим як контролюючим органом.

Натомість частина четверта статті 188-39 Кодексу України про адміністративні правопорушення визначає адміністративну відповідальність за порушення, які безпосередньо пов'язані із процесом здійснення обробки персональних даних та виконанням вимог щодо їх належного захисту [80].

Диспозиція цієї частини має дворівневу конструкцію та охоплює такі взаємопов'язані складові як «недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних» та «незаконного доступу до них або порушення прав суб'єкта персональних даних».

З аналізу наведених положень вбачається, що вказані елементи для настання адміністративної відповідальності мають перебувати у причинно-наслідковому зв'язку.

Тобто, конкретна дія або бездіяльність володільця персональних даних має призвести до настання щонайменше одного з двох видів наслідків:

(а) незаконного доступу (зокрема третіх суб`єктів) до персональних даних;

(б) інших порушень прав суб'єкта персональних даних.

Отже порушення можна класифікувати на самостійні – такі, що здійснюються самі по собі (як окрема самостійна дія щодо персональних

даних), наприклад неповідомлення Уповноваженого про обробку чутливих даних.

До другої категорії можна віднести такі, що виникають внаслідок безпосереднього порушення норм та недотримання процедур щодо обробки персональних даних, передбачених чинним законодавством.

Одним з таких випадків, для прикладу, є порушення суб'єктом, який здійснює обробку персональних даних, порядку розгляду запитів про доступ до персональних даних. Зокрема, для задоволення відповідного запиту та надання (поширення) інформації (персональних даних) у відповідь, запитувачем мають бути дотримані всі вимоги, визначені у статті 16 Закону України «Про захист персональних даних» [10]. Так, необґрунтований запит на доступ до персональних даних сам по собі не тягне адміністративної відповідальності, якщо підстави для надання інформації таки були. Однак, якщо підстави для надання персональних даних відсутні, відповідних працівників володільця персональних даних буде притягнуто до адміністративної відповідальності за частиною четвертою статті 188-39 Кодексу України про адміністративні правопорушення [80].

Прикладом незаконного поширення персональних даних також оприлюднення документів у відкритому доступі без забезпечення попереднього вилучення інформації, яка дозволяє ідентифікувати фізичну особу, що призводить до незаконного поширення персональних даних невизначеному колу осіб [75].

За видами конкретних порушень положень Закону, які у розумінні статті 188-39 Кодексу України про адміністративні правопорушення кваліфікуються як окремі правопорушення у сфері законодавства про захист персональних даних, можна навести [80]:

неповідомлення суб'єкта про збір персональних даних;

незаконну обробку (і зокрема поширення) персональних даних, яка не пов'язана з порушенням порядку захисту;

обробку персональних даних на підставі згоди з порушенням основних вимог, що ставляться до неї (поінформованість, добровільність, наявність документів, що підтверджують її надання);

ненадання відомостей щодо порядку обробки персональних даних; ненадання відомостей про порядок доступу до персональних даних; брак обліку операцій, пов'язаних з обробкою персональних даних; відмову змінити/видалити персональні дані, що не відповідають дійсності, непризначення відповідальної особи; нечітке визначення її обов'язків, порушення умов щодо призначення розпорядника тощо.

Натомість доволі часто у окремих статтях та наукових публікаціях [76] хибно визначають окремі порушення вимог Закону, пов'язуючи їх із можливим настанням адміністративної відповідальності.

Важливо зауважити, що окремі порушення, такі як відмова в наданні доступу суб'єктові до його персональних даних, надання неповних відомостей чи надання відповіді з порушенням строків, визначених для надання відповіді, хоча і фактично призводять до порушення визначеного у статті 8 Закону України «Про захист персональних даних» [10] права особи на доступ до своїх персональних даних, однак не тягне «незаконного доступу до них або порушення прав суб'єкта персональних даних» у взаємозв'язку із «недодержанням порядку захисту персональних даних», що у сукупності не підпадає під диспозицію статті 188-39 Кодексу України про адміністративні правопорушення.

Про проблему відсутності відповідальності за порушення права особи на доступ до своїх персональних даних окремо було наголошено Уповноваженим у Щорічній доповіді за 2023 рік [72].

Вказане обґрунтовує необхідність внесення змін до статті 188-39 Кодексу України про адміністративні правопорушення та доповнення її новою частиною, що передбачає відповідальність за порядок розгляду запиту на доступ до персональних, а також інших порушень Закону, такими як:

неповідомлення суб'єкта про збір персональних даних;

обробку персональних даних на підставі згоди з порушенням основних вимог, що ставляться до неї (поінформованість, добровільність, наявність документів, що підтверджують її надання);

ненадання відомостей щодо порядку обробки персональних даних; ненадання відомостей про порядок доступу до персональних даних;

брак обліку операцій, пов'язаних з обробкою персональних даних; відмову змінити/видалити персональні дані, що не відповідають дійсності, непризначення відповідальної особи, нечітке визначення її обов'язків;

порушення умов щодо призначення розпорядника тощо.

Наразі ж, існуюча система обмежує суб'єкта персональних даних трьома варіантами дій під час обрання способу захисту своїх прав у випадках, коли за порушення їхніх прав володільцями персональних даних, такі дії володільця не охоплюються диспозицією 188-39 Кодексу України про адміністративні правопорушення:

1) оскаржити в судовому порядку;

2) оскаржити в порядку, визначеному Законом України «Про звернення громадян» [77] – до вищої посадової особи;

3) звернутися із скаргою до Уповноваженого Верховної Ради України з прав людини.

Лише у випадку, якщо під час здійснення Уповноваженим Верховної Ради України з прав людини провадження за відповідною скаргою суб'єкта персональних даних, посадовими особами Секретаріату Уповноваженого Верховної Ради України з прав людини будуть підтверджені порушення прав суб'єктів та недотримання вимог Закону України «Про звернення громадян», за які Кодексом України про адміністративні правопорушення чітко не передбачена адміністративна відповідальність (для прикладу, необгрунтована відмова до доступу до власних персональних даних), то настання адміністративної відповідальності можливе лише внаслідок невиконання вимог Уповноваженого Верховної Ради України з прав людини або посадових осіб Секретаріату Уповноваженого Верховної Ради України з прав людини.

Зокрема, стаття 188-40 Кодексу України про адміністративні правопорушення передбачає окремий, формально самостійний склад – невиконання законних вимог Уповноваженого або представників Уповноваженого [10]. В якості невиконання законних вимог розцінюються наступні дії працівників володільця:

- ненадання під час перевірки документів або інформації;
- відмова в наданні документів/інформації у відповідь на запит;
- недопущення до проведення перевірки;
- ненадання доступу до приміщень;
- ненадання доступу до інформації/документів, що є в електронному вигляді (огляду електронних пристроїв);
- тривале створення штучних перешкод у незабезпеченні доступу до об'єкта перевірки (або його окремих приміщень) під різними приводами (відсутність на робочому місці уповноваженої особи, неможливість знайти ключі від приміщень тощо).

Зазначене створює правову невизначеність, суттєво обмежує дієвість, призводить до неефективності заходів адміністративного впливу та унеможливлює притягнення до відповідальності у випадку умисного ухилення володільцями персональних даних від співпраці з Уповноваженим, як те визначено у статті 22 Закону України «Про Уповноваженого Верховної Ради України з прав людини» [78].

Зіставлення складів статей 188-39 та 188-40 Кодексу України про адміністративні правопорушення дає підстави вважати, що об'єктивна сторона статті 188-40 фактично є похідною щодо статті 188-39 – вона передбачає відповідальність не за неправомірну обробку персональних даних, а перешкоджання діяльності контролюючого органу під час реагування на таку обробку (або на інше порушення інформаційних прав).

Стаття 188-40 Кодексу України про адміністративні правопорушення відіграє роль «процесуальної» санкції, спрямованої на забезпечення дієвості контрольних повноважень Уповноваженого, тоді як стаття 188-39 Кодексу

України про адміністративні правопорушення є «матеріальною» санкцією за власне порушення режиму обробки персональних даних.

Важливим елементом адміністративної відповідальності та правових розбіжностей у правозастосовчій практиці національної системи здійснення Уповноваженим Верховної Ради України з прав людини парламентського контролю за захистом персональних даних є визначення поняття «представник Уповноваженого» та «законна вимога».

Якщо диспозиція статті 188-39 Кодексу України про адміністративні правопорушення оперує дефініцією «визначена Уповноваженим посадова особа Секретаріату Уповноваженого Верховної Ради України з прав людини», то, як вже зазначалося, стаття 188-40 Кодексу України про адміністративні правопорушення передбачає відповідальність виключно за «невиконання законних вимог Уповноваженого Верховної Ради України з прав людини або представників Уповноваженого Верховної Ради України з прав людини» [80].

Водночас проаналізувавши положення статті 11 Закону України «Про Уповноваженого Верховної Ради України з прав людини» [78], яким визначено право Уповноваженого призначати своїх представників у межах виділених коштів, затверджених Верховною Радою України, а також Положення про представників Уповноваженого Верховної Ради України з прав людини, затверджене наказом Уповноваженого Верховної Ради України з прав людини від 20 жовтня 2022 року № 84.15/22 [79], яким визначено особливості організації діяльності та межі повноважень, а також основні завдання, функції та права представників Уповноваженого, можна прийти до висновку, що правова природа та обсяг повноважень працівників Секретаріату Уповноваженого та представників Уповноваженого є різною за обсягом та змістом.

На практиці виникають обставини, коли здійснювати перевірку, як те передбачено Порядком здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних, затвердженого Наказом Уповноваженого Верховної

Ради України з прав людини 08.01.2014 № 1/02-14 [51], може представник Уповноваженого, який, як вже було зазначено раніше, не є працівником Секретаріату Уповноваженого, що вже створює ситуацію, що не охоплюється диспозицією статті 188-40 Кодексу України про адміністративні правопорушення [80].

З аналізу Єдиного державного реєстру судових рішень виявлено випадки, коли відповідні протоколи були складені за невиконання вимог керівника Секретаріату, що не відповідає диспозиції статті 188-40 Кодексу України про адміністративні правопорушення. Однак судом було визнано такий протокол, що відповідає вимогам законодавства, оскільки за наказом Уповноваженого, обов'язки представника Уповноваженого з питань захисту персональних даних тимчасово виконувала заступник Керівника Секретаріату Уповноваженого [81].

Окремо, слід наголосити, що Закон України «Про Уповноваженого Верховної Ради України з прав людини» [78] визначає процедуру внесення Уповноваженим актів реагування (подання) для вжиття відповідних заходів у місячний строк щодо усунення виявлених порушень прав і свобод людини і громадянина. Водночас згаданий нормативно-правовий акт не містить такої дефініції як «вимога Уповноваженого» та оперує такими категоріями як «рекомендації» або «пропозиції».

Показовим прикладом, що акумулює в собі одразу кілька структурних дефектів у статті 188-40 Кодексу України про адміністративні правопорушення та суміжних положень Закону України «Про Уповноваженого Верховної Ради України з прав людини», є Конституційна скарга Матвійчук Олександри В'ячеславівни (вх. № 18/335 від 10 вересня 2024 року), у якій Заявниця оспорює конституційність статті 188-40 Кодексу України про адміністративні правопорушення у поєднанні зі статтею 22 Закону України «Про Уповноваженого Верховної Ради України з прав людини», якими встановлено обов'язок співпраці з Уповноваженим та

відповідальність за невиконання вимог «Уповноваженого або його представників» [82].

Згадана скарга прямо порушує питання про те, чи відповідає стаття 188-40 Кодексу України про адміністративні правопорушення у частині визначення суб'єктного складу вимогам частини першої статті 8 та статті 19 Конституції України.

Це твердження кореспондує з доктринальною проблемою конструкції статті 188-40 Кодексу України про адміністративні правопорушення, оскільки зазначена норма встановлює відповідальність за «невиконання законних вимог», проте критерії «законності» таких вимог законодавчо не конкретизовані.

Відсутній нормативно закріплений перелік форм вимог, порядку їх пред'явлення та документального оформлення, що унеможливлює перевірку їх правомірності.

Фактично, конструкція норми перекладає на особу, яка притягається до відповідальності, тягар доведення незаконності вимоги вже після порушення провадження про адміністративне правопорушення, що суперечить загальним засадам адміністративної відповідальності.

Таким чином, згадана конституційна скарга є концентрованим виразом системної недосконалості статті 188-40 Кодексу України про адміністративні правопорушення, таких як: (1) невизначеності суб'єктного складу; (2) відсутності чітких критеріїв «законності» вимог; (3) похідного («процесуального») характеру норми, що породжує передчасну відповідальність; (4) недостатності процесуальних гарантій для особи, стосовно якої здійснюється контроль.

Ці недосконалості у своїй сукупності унеможливлюють формування єдиної та передбачуваної правозастосовної практики і обумовлюють необхідність системного вдосконалення як самої статті 188-40 Кодексу України про адміністративні правопорушення, так і регуляторної бази

здійснення Уповноваженим контролю за дотриманням законодавства про захист персональних даних.

Що стосується санкційної диференціації, то санкції за статтею 188-39 Кодексу України про адміністративні правопорушення диференційовано залежно від суб'єкта та частини статті [80]: за частиною першою – штраф на громадян від ста до двохсот неоподатковуваних мінімумів доходів громадян (далі – НМДГ) і на посадових осіб, громадян – суб'єктів підприємницької діяльності – від двохсот до трьохсот нмдг; за частиною четвертою – штраф на громадян від ста до п'ятисот нмдг і на посадових осіб, громадян – суб'єктів підприємницької діяльності – від трьохсот до однієї тисячі нмдг; за повторне порушення (частина п'ята) – підвищені санкції, до двох тисяч нмдг для посадових осіб та суб'єктів підприємницької діяльності.

За статтею 188-40 Кодексу України про адміністративні правопорушення передбачено санкції у вигляді накладення штрафу на посадових осіб, громадян – суб'єктів підприємницької діяльності від ста до двохсот нмдг [80].

Як буде показано в цьому підрозділі надалі, у структурі складених протоколів стаття 188-40 Кодексу України про адміністративні правопорушення кількісно домінує над статтею 188-39 Кодексу України про адміністративні правопорушення, що свідчить про систематичну проблему саме на стадії взаємодії суб'єктів обробки персональних даних із контролюючим органом, а не лише на стадії власне обробки даних.

Аналіз наведених прикладів дає підстави стверджувати, що кримінальна відповідальність відіграє роль «верхнього порогу» в системі відповідальності за порушення законодавства про обробку персональних даних: вона застосовується тоді, коли діяння виходить за межі «недодержання порядку захисту персональних даних» (склад статті 188-39 Кодексу України про адміністративні правопорушення) і набуває ознак умисного, суспільно небезпечного посягання на конфіденційність інформації про особу.

Відповідно, існування цього «верхнього порогу» опосередковано підтверджує необхідність посилення інституту адміністративної відповідальності, оскільки за відсутності дієвого адміністративного реагування, більшість правопорушень, які за правовою кваліфікацією не підпадають під «кримінальні», залишатимуться без належної реакції з боку держави, а суб'єкти персональних даних – без захисту.

Уявляється обґрунтованим висновок про те, що ієрархія видів відповідальності у сфері обробки персональних даних в Україні є не нормативною, а функціональною: на вершині цієї ієрархії перебуває адміністративна відповідальність як єдиний вид, що реалізується через спеціалізований орган контролю (Уповноваженого Верховної Ради України з прав людини), має визначену процедуру (складення протоколу – розгляд судом) та підлягає статистичному обліку.

Саме тому подальший виклад зосереджується на адміністративній відповідальності, а кримінальна, дисциплінарна та цивільно-правова відповідальність розглядаються як додаткові (субсидіарні) механізми.

У межах цих повноважень Уповноважений здійснює перевірки володільців та розпорядників персональних даних, видає приписи про усунення порушень, обов'язкові для виконання, а в разі виявлення під час перевірки ознак адміністративного правопорушення, передбаченого статтею 188-39 або статтею 188-40 Кодексу України про адміністративні правопорушення, уповноважена особа Секретаріату Уповноваженого або представник Уповноваженого складає протокол про адміністративне правопорушення, який передається на розгляд місцевого суду загальної юрисдикції [80].

Таким чином, адміністративна відповідальність у досліджуваній сфері реалізується через триланкову процедуру: (1) виявлення порушення (за результатами перевірки, моніторингу відкритих джерел або звернення громадянина); (2) реагування у формі припису про усунення порушення або складення протоколу про адміністративне правопорушення; (3) розгляд

протоколу місцевим судом загальної юрисдикції з можливим накладенням адміністративного стягнення у вигляді штрафу.

Кожна з цих ланок має самостійне статистичне відображення (кількість перевірок, кількість приписів, кількість протоколів, кількість справ, що завершилися штрафом), що дає змогу побудувати наскрізний аналіз ефективності всього механізму – від виявлення порушення до застосування санкції.

Уявляється обґрунтованим висновок про те, що формулювання частини четвертої статті 188-39 Кодексу України про адміністративні правопорушення – «недодержання встановленого порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних» [80] є надмірно широким і водночас недостатньо визначеним: воно не містить переліку конкретних дій (бездіяльності), що утворюють «недодержання порядку», а пов`язує склад правопорушення з результатом, доведення якого на практиці є складним. Це спостереження надалі підтверджується аналізом судової практики, де саме недоведеність причинно-наслідкового зв'язку між діянням і результатом є однією з підстав закриття провадження через відсутність складу правопорушення.

Механізм складання уповноваженими особами Секретаріату Уповноваженого Верховної Ради України з прав людини протоколів про адміністративні правопорушення врегульовано Порядком оформлення матеріалів про адміністративні правопорушенн, затвердженим наказом Уповноваженого від 22.12.2025 [64].

Систематичний статистичний облік показників діяльності Уповноваженого у сфері захисту персональних даних у розрізі, придатному для дисертаційного аналізу (звернення, перевірки, приписи, протоколи), наявний у відкритому доступі переважно за 2022–2025 роки, період, що збігається з дією правового режиму воєнного стану.

За попередні роки (до 2022 року) Щорічні доповіді, як правило, не виокремлюють повною мірою усі показники у сфері захисту персональних

даних у вигляді порівнюваного набору індикаторів, що саме по собі є емпіричним фактом, який засвідчує недостатню прозорість статистичного обліку в цій сфері до 2022 року. У зв'язку з цим основний кількісний аналіз нижче побудовано на даних за 2022–2025 роки, з окремими застереженнями щодо доступності даних за інші роки досліджуваного періоду.

Зокрема, за 2022 рік до Уповноваженого надійшло 844 звернення з питань захисту персональних даних, за результатами розгляду яких відкрито 66 проваджень; працівниками Секретаріату проведено 85 перевірок дотримання законодавства про захист персональних даних, за результатами яких видано 75 приписів про усунення порушень [71]. У звітній доповіді за 2022 рік прямо зазначено, що кількість повідомлень порівняно з 2021 роком суттєво зменшилася.

За 2023 рік до Уповноваженого надійшло 1205 звернень (1336 повідомлень) щодо ймовірного порушення права на захист персональних даних, з яких 652 повідомлення стосувалися незаконної обробки персональних даних, 190 – порушення права на доступ до інформації про себе, 220 – питань організації обробки персональних даних; видано 92 приписи про усунення порушень [72].

Упродовж 2023 року за порушення права на інформацію, права на звернення та у сфері захисту персональних даних, а також невиконання законних вимог Уповноваженого складено 88 протоколів про адміністративні правопорушення, з яких 9 – за статтею 188-39 Кодексу України про адміністративні правопорушення, 29 – за статтею 188-40 Кодексу України про адміністративні правопорушення, 50 – за статтею 212-3 Кодексу України про адміністративні правопорушення.

За 2024 рік до Уповноваженого надійшло 857 звернень, які містили 1409 повідомлень у сфері захисту персональних даних; перевірено 103 підприємства, установи та організації, за результатами перевірок видано 85 приписів, обов'язкових для виконання [73]. Складено протоколів про адміністративні правопорушення, з яких 2 – за статтею 188-39, 4 – за статтею

188-40, 34 – за статтею 212-3 Кодексу України про адміністративні правопорушення.

Протягом 2025 року Уповноваженим отримано 15 217 звернень та 18 621 повідомлення про порушення, проведено 382 перевірками у сфері захисту персональних даних; відкрито 2 517 проваджень, поновлено 2 928 прав. Водночас подань Уповноваженого – лише 5, а приписів про усунення порушень безпосередньо у сфері персональних даних – 75, що менше трьох відсотків від загальної кількості контрольних заходів (таблиця 1).

Показник	**2022 рік**	**2023 рік**	**2024 рік**	**2025 рік**
Звернення/повідомлення щодо захисту персональних даних	844	1205 / 1336	857 / 1409	2109 / 2262
Відкриті провадження	66	н.д.	1334*	2 517*
Перевірки володільців/розпорядників ПД	85	н.д.	103	98
Приписи про усунення порушень	75	92	85	75
Протоколи за ст. 188-39 КУпАП	3	9	2	0
Протоколи за ст. 188-40 КУпАП	н.д.	29	4	16

**Показники за 2024 та 2025 роки наведені як загальна кількість проваджень у межах усього розділу «Інформаційні права» (включно з доступом до публічної інформації та правом на звернення), а не виключно у сфері захисту персональних даних.*

Таблиця 1. Основні показники діяльності Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних (2022–2025 рр.)

Крім того, за скерованими Секретаріатом Уповноваженого матеріалами до правоохоронних органів щодо порушень пов’язаних з неправомірною обробкою персональних даних, внесено відомості до Єдиного реєстру досудових розслідувань по 35 фактам.

Аналіз наведених у таблиці 1 показників дає підстави для важливого узагальнення: масштаб звернень громадян до Уповноваженого щодо захисту персональних даних демонструє стійку тенденцію до зростання – з 844 у 2022 році до 1336 повідомлень у 2023 році та 1409 повідомлень у 2024 році, тобто приріст за два роки склав близько 67 відсотків.

Водночас кількість приписів про усунення порушень залишається у вузькому діапазоні 75–92 за рік і не демонструє пропорційного зростання, а кількість протоколів за статтею 188-39 Кодексу України про адміністративні правопорушення – найбільш «матеріального» складу правопорушення у досліджуваній сфері – навіть скоротилася, попри зростання кількості звернень та перевірок (з 85 у 2022 році до 103 у 2024 році).

Аналіз наведених підходів дає підстави стверджувати, що між динамікою звернень (вхідний потік сигналів про можливі порушення) та динамікою протоколів за статтею 188-39 Кодексу України про адміністративні правопорушення (вихідний показник застосування адміністративної відповідальності) відсутня кореляція, яка очікувалася би за умови пропорційного реагування контролюючого органу. Вказане може свідчити про те, що «вузьким місцем» механізму адміністративної відповідальності є не виявлення порушень (цей етап, навпаки, демонструє позитивну динаміку – зростання кількості перевірок і приписів), а перехід від виявлення порушення до складення протоколу про адміністративне правопорушення за статтею 188-39 Кодексу України про адміністративні правопорушення.

Аналіз наведеної процедури дає підстави стверджувати, що адміністративна відповідальність за порушення законодавства про обробку персональних даних в Україні побудована за двоетапною моделлю «фіксація – судове провадження», яка принципово відрізняється від моделі, властивої

спеціалізованим органам захисту даних держав-членів ЄС, де наглядовий орган самостійно, в адміністративному порядку, накладає штраф без необхідності звернення до суду.

Згадана дволанкова модель реагування є додатковою процесуальною стадією, яка, як буде показано в надалі у цьому ж підрозділі, є основним джерелом неефективності всього механізму. Вказана теза знаходить своє підтвертдження і у результатах дослідження ГО «Платформа прав людини» «Аналіз практики розгляду судами справ про адміністративні правопорушення, передбачені статтями 188-39, 188-40, 212-3 Кодексу України про адміністративні правопорушення щодо протоколів, складених уповноваженими особами Секретаріату Уповноваженого Верховної Ради України з прав людини та представниками Уповноваженого Верховної Ради України з прав людини в 2022-2024 роках», де стверджується, що інструмент захисту інформаційних прав, як притягнення осіб до адміністративної відповідальності, є доволі неефективний [84].

Загалом забезпечено аналіз судової практики, а саме розміщених у Єдиному реєстрі судових рішень за резудьтатами розгляду судами перших інстанцій протягом 2022–2025 років протоколів про адміністративні правопорушення. А саме: 10 справ – за статтею 188-39 Кодексу України про адміністративні правопорушення (9 рішень – за частиною четвертою, 1 – за частиною першою) та 68 справ – за статтею 188-40 Кодексу України про адміністративні правопорушення.

Вказані статистичні показники свідчать про наявність суттєвого розриву між кількістю звернень та вжитими заходами реагування. Наведена вище інформація може свідчити про необхідність підвищення інституційної спроможності Офісу Омбудсмана або врегулювання питання щодо визначення окремого органу або посадової особи, до повноважень якої віднесено питання захисту персональних даних.

Результат розгляду	Ст. 188-39 (10 справ)	Ст. 188-40 (68 справ)
Накладено штраф	2 (20%)	17 (25%)
Закрито у зв'язку зі спливом строків (ст. 38 Кодексу України про адміністративні правопорушення)	4 (40%)	19 (28%)
Звільнення від відповідальності за малозначністю (ст. 22 Кодексу України про адміністративні правопорушення)	2 (20%)	5 (7,4%)
Закрито через відсутність складу/події правопорушення	1 (10%)	24 (35%)
Повернуто на доопрацювання	1 (10%)	3 (4,4%)

Таблиця 2. Результати розгляду судами першої інстанції справ за статтями 188-39 та 188-40 Кодексу України про адміністративні правопорушення (2022–2025 рр.)

Така диспропорція може свідчити як про обмежену ефективність існуючого механізму притягнення до відповідальності, так і частково бути обумовлена такими обставинами як невідповідності звернень громадян формальним вимогам, які визначені Законом України «Про звернення громадян» [77], а також фактичною відсутністю у діях суб’єктів, що здійснюють обробку персональних даних, складу адміністративного правопорушення.

Крім того, у Спеціальній доповіді щодо додержання конституційного права на інформацію в умовах дії правового режиму воєнного стану, Уповноважений пропонує спрощення процедури складання протоколу про адміністративне правопорушення, у разі відмови особи, яка притягається до

адміністративної відповідальності, від підписання протоколу, а також у разі відмови такої особи з'явитися до місця складання протоколу для його підписання [85].

Ще однією причиною значної диспропорції, наведеної вище, може бути специфіка правового статусу Уповноваженого Верховної Ради України з прав людини, який, будучи національною інституцією з прав людини, за своєю природою не наділений каральними функціями та повноваженням безпосередньо притягати винних осіб до відповідальності [20].

Українська модель, як випливає із наведеного, орієнтована лише на фіксацію порушень та подальше судове провадження. Аналіз, проведений у Звіті Директорату інформаційного суспільства, засвідчує недостатні повноваження, надані законом інституції Уповноваженого Верховної Ради України з прав людини для здійснення ефективного контролю та притягнення до адміністративної відповідальності [86, с. 106-107].

Вказаний порядок значно послаблює ефективність реалізації Уповноваженим як наглядовим органом власних повноважень, а також позбавляє можливості ефективно реагувати на порушення у сфері захисту персональних даних.

Суттєві недоліки такого підходу особливо проявляються за ситуації, коли суб'єкт, у діяльності якого виявили порушення законодавства про захист персональних даних, заперечує та не визнає обставин вчинення ним такого порушення, а тому відмовляється йти на співпрацю з Секретаріатом Уповноваженого та припиняти незаконну обробку персональних даних самостійно до визнання його провини у судовому порядку.

Це дає підстави для висновку про те, що низька результативність адміністративної відповідальності є структурною, а не ситуативною характеристикою досліджуваного інституту: вона спостерігається стабільно протягом усього періоду, щодо якого наявні зіставні дані, незалежно від коливань кількості звернень чи перевірок.

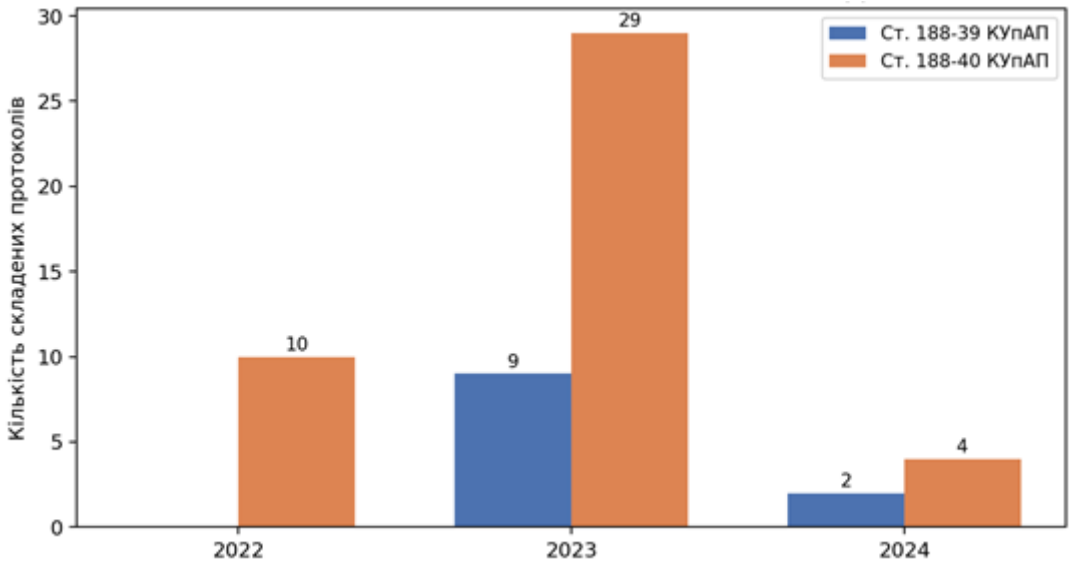

Рис. 3. Динаміка складення адміністративних протоколів

Аналіз судової практики за статтями 188-39 та 188-40 Кодексу України про адміністративні правопорушення доцільно здійснювати на основі трьох рівнів (рис. 3):

1) узагальнених статистичних показників результатів розгляду справ;

2) типових правових позицій судів, виявлених у конкретних рішеннях;

3) проблемних питань, що виникають при розгляді справ цієї категорії та потребують законодавчого врегулювання.

Перший рівень розглянуто нижче в цьому підрозділі на основі узагальнених даних дослідження, другий і третій – на основі конкретних судових рішень, внесених до Єдиного державного реєстру судових рішень.

Водночас слід наголосити на обставинах, які суттєво затягують процес притягнення до відповідальності, знижують невідворотність покарання, створюють додаткові підстави для спливу термінів притягнення до відповідальності. Для прикладу, стаття 38 Кодексу України про адміністративні правопорушення [80] встановлює строки притягнення до адміністративної відповідальності, які становлять три місяці з дня вчинення правопорушення або з дня його виявлення (табл. 2).

Відповідно до аналізу судових рішень у Єдиному державному реєстрі судових рішень, з 10 призначених протягом 2022-2025 років до розгляду справ за статтею 188-39 Кодексу України про адміністративні правопорушення, тільки 2 завершилися притягненням особи щодо якої будо складено протокол, до адміністративної відповідальності у вигляді накладення штрафу.

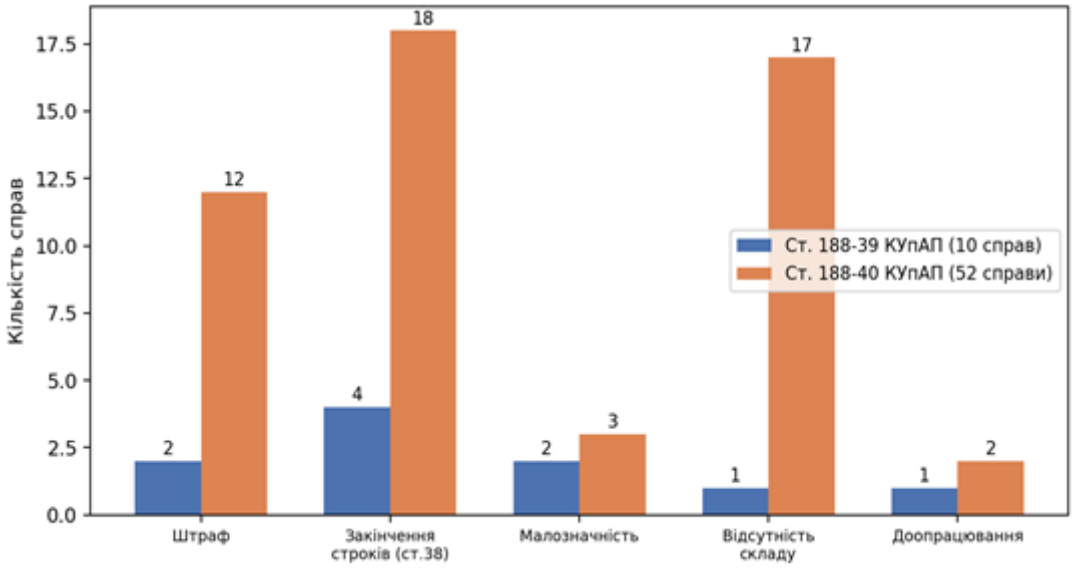

Рис. 4. Результати розгляду судами першої інстанції справ за статтями 188-39 та 188-40 КУпАП.

Аналіз наведених показників щодо розгляду відповідних справ протягом 2022–2025 років демонструє стійке зростання вхідного потоку звернень громадян щодо захисту персональних даних (з 844 до 1409) на фоні скорочення кількості складених протоколів за статтею 188-39 Кодексу України про адміністративні правопорушення (з 9 у 2023 році до 2 у 2024 році, а також до 0 у 2025 році) та незмінно низького рівня застосування реальних санкцій за результатами судового розгляду (рис. 4). Це дає підстави стверджувати, що проблема перебуває не на етапі виявлення порушень, а на етапах їх процесуального оформлення та судового розгляду.

Окремої уваги заслуговує проблема неможливості зміни кваліфікації правопорушення судом під час розгляду справи: чинний Кодекс України про

адміністративні правопорушення, на відміну від Кримінального процесуального кодексу України [87], не передбачає механізму, який дозволяв би суду перекваліфікувати діяння, якщо фактичні обставини справи відповідають іншому складу правопорушення, ніж зазначений у протоколі.

Узагальнюючи, можна виокремити п’ять самостійних, хоча й взаємопов’язаних, груп причин низької ефективності адміністративної відповідальності за порушення законодавства про обробку персональних даних в Україні.

По-перше, стаття 38 Кодексу України про адміністративні правопорушення встановлює, що адміністративне стягнення може бути накладено не пізніш як через три місяці з дня вчинення правопорушення, а при триваючому правопорушенні – не пізніш як через три місяці з дня його виявлення. Результатом розгляду 43,2 відсотка справ за статтями 188-39, 188-40 та 212-3 Кодексу України про адміністративні правопорушення за 2022–2024 роки стало закриття провадження без застосування санкцій саме через закінчення цього тримісячного строку, передбаченого пунктом 7 частини першої статті 247 Кодексу України про адміністративні правопорушення [84].

Для статті 188-39 Кодексу України про адміністративні правопорушення цей показник становить 40 відсотків – 4 справи з 10 (таблиця 2). Як зазначено у дослідженні, проведеному ГО «Платформа прав людини», у 27 з 37 проаналізованих випадків закриття справ за статтями 212-3, 188-39 та 188-40 Кодексу України про адміністративні правопорушення у зв’язку зі спливом строків (майже 73 відсотки) причиною були несвоєчасні процесуальні дії судів – призначення справи до розгляду через кілька місяців після надходження матеріалів [84].

Отже тримісячний строк притягнення до адміністративної відповідальності, встановлений статтею 38 Кодексу України про адміністративні правопорушення, є явно недостатнім. Сплив тримісячного строку є наслідком не одноразової, а кумулятивної затримки на щонайменше на наступних етапах: 1) між виявленням порушення та складенням протоколу;

2) між складенням протоколу та його переданням до суду; 3) між надходженням протоколу до суду та призначенням справи до розгляду; 4) розгляд справи по суті, ухвалення постанови. Дотого ж, відсутні законодавчі критерії віднесення правопорушення до триваючого, що також впливає на обчислення строків за статтею 38 Кодексу України про адміністративні правопорушення.

По-друге, організаційні причини. 10 відсотків матеріалів адміністративних справ за статтею 188-39 Кодексу України про адміністративні правопорушення протягом 2022–2025 років було повернуто судами Секретаріату Уповноваженого на доопрацювання у зв’язку з неналежним оформленням таких протоколів (таблиця 2). Кожне таке повернення фактично означає втрату процесуального часу в межах тримісячного строку, встановленого статтею 38 Кодексу України про адміністративні правопорушення, що в подальшому стає самостійною підставою закриття справи. Затвердження у лютому 2026 бланку протоколу [88], на думку автора, є спробою уніфікації підходів до складання протоколів про адміністративні правопорушення, а також припинення практики повернення судами протоколів про адміністративні правопорушення через формальні підстави (незазначення реквізитів тощо).

Третьою причиною є відсутність механізму зміни кваліфікації правопорушення судом, що, як показано в підрозділі 2.2. призводить до закриття справ через формальну невідповідність кваліфікації фактичним обставинам. Слід проаналізувати ситуації, коли діяння, що відповідало частині другій статті 212-3 Кодексу України про адміністративні правопорушення, було кваліфіковане за частиною дев’ятою цієї статті, унаслідок чого справу закрито через відсутність складу правопорушення [84]. Цей висновок має універсальне значення для всієї групи статей 188-39, 188-40, 212-3 Кодексу України про адміністративні правопорушення, оскільки відображає загальну прогалину процесуального регулювання провадження у справах про адміністративні правопорушення, яка з однаковою ймовірністю може

виникнути і за статтею 188-39 Кодексу України про адміністративні правопорушення – наприклад, у разі помилкової кваліфікації діяння посадовими особами Секретаріату Уповноваженого.

По-четверте, правозастосовні причини, пов’язані з відсутністю уніфікованих критеріїв оцінки суспільної шкоди, доцільно визнати окремою самостійною категорією. Так, стаття 22 Кодексу України про адміністративні правопорушення, що дозволяє звільняти особу від адміністративної відповідальності за малозначністю правопорушення, не містить критеріїв такої малозначності. Вказане залишає істотний простір для суб’єктивного тлумачення судами під час розгляду справ за статтею 188-39 Кодексу України про адміністративні правопорушення.

По-п’яте, ще однією проблемою, пов’язаною із застосуванням статті 38 Кодексу України про адміністративні правопорушення, є питання про необхідність встановлення вини особи при закритті провадження на підставі пункту 7 частини першої статті 247 Кодексу України про адміністративні правопорушення.

Як демонструє постанова Амур-Нижньодніпровського районного суду міста Дніпропетровська у справі № 199/840/24 (предметом якої було правопорушення за частиною другою статті 212-3 Кодексу України про адміністративні правопорушення, однак правова позиція суду має універсальне значення для всієї групи статей 188-39, 188-40, 212-3 Кодексу України про адміністративні правопорушення), суд визнав особу винною у вчиненні адміністративного правопорушення та водночас закрив провадження у зв’язку зі спливом строків притягнення до відповідальності, послідовно мотивувавши це тим, що «наслідком закриття провадження у справі про адміністративне правопорушення у зв’язку із закінченням строків накладення адміністративного стягнення є лише звільнення особи від накладення адміністративного стягнення», а не звільнення від встановлення вини [89].

Це рішення оскаржувалося в апеляційному порядку особою, яка притягалася до адміністративної відповідальності у зв’язку із тим, що, на

думку апелянта, суд першої інстанції неправильно застосував положення статті 38, пункту 7 частини 1 статті 247 Кодексу України про адміністративні правопорушення, закриваючи провадження у справі з вказаної підстави та одночасно визнаючи особу винуватим. Втім доводи апелянта не були визнані ґрунтовними, у зв'язку із чим оскаржена постанова суду першої інстанції була залишена без змін, а апеляційна скарга – без задоволення судом апеляційної інстанції [90].

Водночас висновок Науково-консультативної ради при Вищому адміністративному суді України від 7 листопада 2017 року свідчить про те, що поєднання закриття справи з одночасним визнанням вини особи є взаємовиключними рішеннями, оскільки пункт 7 частини першої статті 247 Кодексу України про адміністративні правопорушення не наділяє суд повноваженнями встановлювати вину особи при закритті провадження за цією підставою [91].

Загалом, судова практика щодо встановлення вини особи у випадку закриття справи через сплив строків притягнення до відповідальності є неоднорідною: дослідження виокремлює щонайменше три різні підходи судів – встановлення вини в резолютивній частині постанови, встановлення вини лише в мотивувальній частині та повну відмову від встановлення вини [84].

По-шосте, окремо слід визначити інституційні причини, пов'язані з правовою природою Уповноваженого Верховної Ради України з прав людини як національної інституції з прав людини, яка за своїм статусом не наділена каральними функціями і не може самостійно, в позасудовому порядку, застосовувати фінансові санкції.

По-сьоме, слід рознлянути пов'язані із співвідношенням розміру санкцій та практичної шкоди від порушень. Санкції за статтями 188-39 та 188-40 Кодексу України про адміністративні правопорушення, навіть у максимальному розмірі (до двох тисяч НМДГ за повторне порушення за статтею 188-39 Кодексу України про адміністративні правопорушення), є величинами фіксованими і не залежать від масштабу обробки персональних

даних, кількості постраждалих суб’єктів персональних даних чи тривалості порушення – на відміну, наприклад, від Європейського підходу, де розмір штрафу прямо корелює із систематичністю, повторюваністю та масштабом порушення.

Окремою, восьмою причиною неефективності санкційної системи є відсутність у наглядового органу, який склав протокол про адміністративне правопорушення (Секретаріату Уповноваженого), процесуального права на апеляційне оскарження постанови суду першої інстанції відповідно до статті 294 Кодексу України про адміністративні правопорушення, що унеможливлює виправлення помилкових рішень про закриття справ навіть у разі їх явної необґрунтованості.

Попри відсутність процесуального права, посадовими особами Секретаріату Уповноваженого здійснюються спроби в апеляційному порядку оскаржувати рішення судів перших інстанцій. Для прикладу, представником Уповноваженого в Харківській області було подано апеляційну скаргу із посиланням на наявність у нього нібито статусу потерпілого, а відповідно, і права на апеляційне оскарження постанови судді. Суд апеляційної інстанції визнав такі доводи безпідставним, з огляду на несумісність статусів потерпілого та представника Уповноваженого як посадової особи як таких, що є взаємовиключними у контексті можливості завдання моральної, фізичної або майнової шкоди у розумінні статті 269 Кодексу України про адміністративні правопорушення [83].

Натомість апеляційна практика 2025 року емпірично підтверджує асиметричність механізму перегляду судових рішень цієї категорії. Зокрема, скарги осіб, притягнутих до відповідальності, розглядаються по суті: постановою Черкаського апеляційного суду від 28 лютого 2025 року у справі №695/3489/24 постанову про притягнення особи до відповідальності скасовано, а провадження закрито через відсутність складу правопорушення.

Отже, низька ефективність адміністративної відповідальності за порушення законодавства про обробку персональних даних в Україні є

результатом не однієї, а кумулятивної дії зазначених груп причин, кожна з яких самостійно знижує ймовірність застосування санкції на відповідній стадії процедури.

Для прикладу, аналіз судових рішень за статтею 188-40 Кодексу України про адміністративні правопорушення свідчить, що без застосування адміністративного стягнення завершилося 56,25 відсотка проваджень (9 із 16 справ, закритих через відсутність складу чи події, сплив строків або повернутих на доопрацювання) у 2025 році.

З урахуванням двох випадків звільнення від відповідальності за малозначністю, питома вага справ, що не мали для порушника жодних майнових наслідків, сягає 68,75 відсотка.

З цього випливає методологічно важливий наслідок: пропозиції щодо вдосконалення законодавства мають бути комплексними, тобто впливати на кожну зі стадій процедури, оскільки усунення лише однієї причини (наприклад, виключно збільшення строків за статтею 38 Кодексу України про адміністративні правопорушення) не здатне забезпечити істотне підвищення ефективності за наявності інших, не усунутих причин.

Таким чином, сучасна модель захисту персональних даних в Україні ґрунтується на поєднанні конституційних гарантій, міжнародних стандартів та національних інституційних механізмів. Водночас її ефективність обмежується відсутністю у наглядового органу повноважень щодо безпосереднього застосування санкцій.

У зв’язку з цим актуальним є питання модернізації системи захисту персональних даних України, зокрема шляхом удосконалення механізмів притягнення до відповідальності, а також підвищення інституційної спроможності наглядового органу у сфері захисту персональних даних.

Узагальнюючи, можна констатувати, що проблема статті 38 Кодексу України про адміністративні правопорушення має не одновимірний, а тривимірний характер: 1) матеріально-правовий вимір – тримісячний строк є об’єктивно недостатнім з огляду на реальну тривалість процедури взаємодії

«Секретаріат Уповноваженого – суд»; 2) процесуальний вимір – закриття справи за спливом строків позбавляє орган, який склав протокол, можливості апеляційного оскарження (стаття 294 Кодексу України про адміністративні правопорушення), оскільки особа, щодо якої закрито справу, як правило, не оскаржує сприятливе для неї рішення; 3) доктринальний вимір – відсутність законодавчо визначеного підходу до питання встановлення вини при закритті справи за спливом строків породжує суперечливу судову практику, яка підриває принцип правової визначеності.

Водночас усунення всіх законодавчих та організаційних недоліків, розглянутих вище, потребує усвідомлення, що інституційна архітектура контролю сьогодня залишається дволанковою («орган контролю – суд»). Вказане, саме по собі, є повільнішою та більш ресурсомісткою порівняно з одноланковою моделлю прямого застосування санкцій наглядовим органом.

Відтак, незважаючи на формальне закріплення у статті 28 Закону України «Про захист персональних даних» чотирьох видів юридичної відповідальності, реальним механізмом реагування на порушення законодавства про обробку персональних даних в Україні є виключно адміністративна відповідальність за статтями 188-39 та 188-40 Кодексу України про адміністративні правопорушення. Дисциплінарна та цивільно-правова відповідальність існують на рівні нормативної декларації, не підтвердженої емпіричним матеріалом, а кримінальна відповідальність виконує субсидіарну функцію «верхнього порогу», що застосовується у випадках, які виходять за межі складу статті 188-39 Кодексу України про адміністративні правопорушення за критерієм суспільної небезпечності.

При цьому, у структурі адміністративної відповідальності стаття 188-40 Кодексу України про адміністративні правопорушення (невиконання законних вимог Уповноваженого) кількісно домінує над статтею 188-39 Кодексу України про адміністративні правопорушення (власне порушення режиму обробки персональних даних). Вказане свідчить про те, що системною проблемою є не лише саме порушення режиму обробки персональних даних,

але й неналежна взаємодія володільців і розпорядників персональних даних із наглядовим органом.

Висновки до розділу II

1. Досліджено багатоманітність доктринальних підходів до розуміння контролю за обробкою персональних даних та сформульовано авторське визначення цього поняття як здійснюваної на систематичній основі або за зверненням діяльності уповноважених суб'єктів, спрямованої на встановлення відповідності обробки персональних даних вимогам законодавства та захист прав суб'єктів персональних даних із застосуванням засобів впливу, – яке, на відміну від наявних у доктрині визначень, що зводять контроль до повноважень єдиного наглядового органу, фіксує його багатосуб'єктну природу як системну ознаку.

Обґрунтовано сферозалежний (секторальний) характер контролю: доведено, що конфігурація контрольного механізму – коло суб'єктів, обсяг повноважень, застосовні форми – визначається природою суспільних відносин, у межах яких здійснюється обробка, унаслідок чого уніфікована модель контролю є помилковою по суті предмета регулювання, а не лише практично недосконалою.

На цій основі запропоновано п'ятирівневу типологію суб'єктів контролю за критерієм природи суб'єкта та юридичної сили його рішень (загальний регулятор; секторальні державні регулятори; органи професійного самоврядування; етичні органи саморегулювання; внутрішній самоконтроль володільця), доповнену виокремленням громадського контролю як самостійного наскрізного квазіконтрольного елемента, підтверджену емпірично на медійному кейсі, у якому одночасно реалізуються чотири з п'яти рівнів типології.

2. Досліджено суб'єктний склад системи контролю за обробкою персональних даних в Україні, включно з інституційною позицією судів у цій системі, та доведено доктринальну некоректність віднесення судів до

суб’єктів контролю за статтею 22 Закону: встановлено, що судова діяльність структурно протилежна адміністративному контролю за критеріями систематичності, ініціативності, превентивності та можливості прямого владного втручання, унаслідок чого запропоновано термінологічну корекцію законодавства – заміну щодо судів категорії «суб’єкт контролю» на категорію «суб’єкт судового захисту прав у сфері обробки персональних даних». Класифіковано повноваження Уповноваженого Верховної Ради України з прав людини за функціональним призначенням та стадією контрольного циклу (превентивна, розслідувальна, коригувальна, постконтрольна), що дало змогу встановити структурну асиметрію: у розслідувальному та дорадчому вимірах структура повноважень відповідає універсальному стандарту статті 58 GDPR, однак демонструє системне ослаблення в коригувально-санкційному вимірі – відсутність права самостійного накладення штрафу – за одночасного непропорційного розширення в нормотворчому вимірі, що не має прямого аналога в жодній із порівнюваних юрисдикцій. Виявлено, що ця асиметрія є інституційним джерелом розриву між законодавчою активністю Уповноваженого та статистично підтвердженою слабкістю фактичного правозастосування.

Обґрунтовано, що для переходу до ризик-орієнтованої моделі контролю визначальним є саме коригувально-санкційний вимір повноважень, оскільки лише він перетворює виявлення порушення на реальний превентивний стимул для суб’єктів обробки, – що є прямим структурним елементом авторської концепції ефективного контролю, операціоналізованої надалі через індекс SEI.

3. Досліджено статистичну динаміку та судову практику застосування адміністративної відповідальності за 2022–2025 роки та встановлено емпірично підтверджену диспропорцію: зростання кількості звернень громадян (на 67 відсотків) супроводжується суттєвим скороченням кількості протоколів за статтею 188-39 Кодексу України про адміністративні правопорушення, що доводить структурний, а не ситуативний характер неефективності механізму відповідальності і є прямим емпіричним

підтвердженням центральної гіпотези дисертації на рівні правозастосування. Доведено функціональне співвідношення статей 188-39 і 188-40 Кодексу України про адміністративні правопорушення як «матеріальної» та похідної «процесуальної» санкцій; кількісне домінування статті 188-40 над статтею 188-39 дало змогу встановити, що первинною системною проблемою є не сама неправомірна обробка персональних даних, а неналежна взаємодія володільців і розпорядників персональних даних із наглядовим органом під час здійснення контрольних заходів. Виявлено п’ять груп причин неефективності інституту адміністративної відповідальності – законодавчі, організаційні, правозастосовні, інституційні та системні; зокрема встановлено, що об’єктивно недостатній тримісячний строк притягнення до відповідальності за статтею 38 Кодексу України про адміністративні правопорушення зумовлює закриття 43,2 відсотка справ без застосування санкцій. Обґрунтовано, що прийняття проєктів Закону України від 25.10.2022 року № 8153 та Закону України від 18.10.2021 № 6177 є необхідною, але недостатньою умовою підвищення ефективностівідповідальності.

Доведено, що оптимальна стратегія реформування передбачає трирівневу синхронізацію: (1) на рівні матеріального права – диференціація санкцій залежно від масштабу й тривалості порушення та запровадження обов’язкового статусу виконавчого документа для приписів Уповноваженого; (2) на рівні процесуального права – продовження строків за статтею 38 Кодексу України про адміністративні правопорушення до шести (дванадцяти для триваючих правопорушень) місяців, надання органу, який склав протокол, права на апеляційне оскарження, та законодавче визначення критеріїв малозначності й триваючого правопорушення; (3) на рівні інституційної архітектури – створення Національної комісії з питань захисту персональних даних та доступу до публічної інформації як спеціалізованого наглядового органу відповідно до проєкту Закону України від 18.10.2021 № 6177 [52] з одночасним перенесенням до нього функцій контролю, передбачених наразі для Уповноваженого, але без повторення дволанкової моделі «орган контролю

– суд» у її нинішньому вигляді стосовно фінансових санкцій помірного розміру. Лише одночасна реалізація цих трьох рівнів реформи здатна перетворити інститут адміністративної відповідальності за порушення законодавства про обробку персональних даних в Україні з переважно декларативного на реально діючий механізм захисту прав суб'єктів персональних даних.

Розділ ІІІ. Напрями забезпечення ефективності здійснення контролю за обробкою персональних даних

3.1. Міжнародні стандарти контролю за обробкою персональних даних: практика ЄСПЛ, Суду ЄС та досвід європейських наглядових органів

Стаття 8 Конвенції про захист прав людини і основоположних свобод, що гарантує право на повагу до приватного і сімейного життя, становить ту конституційну матрицю, з якої Європейський суд з прав людини послідовно виводив усе ширше коло гарантій для особи в умовах зростання державних і приватних практик збирання та обробки інформації.

Принципово важливо, що цей процес не був лінійним: він відображав глибше концептуальне питання про те, чи є обробка персональних даних лише одним із можливих видів втручання у приватне життя, чи, натомість, є самостійним феноменом, що потребує власного нормативного каркасу.

Питання суттєве не тільки з доктринальних міркувань. Якщо захист даних є лише аспектом приватності, то стандарти виправданості втручання визначаються в кожному конкретному випадку через призму статті 8 (2) Конвенції про захист прав людини і основоположних свобод [19].

Значення цього руху для органів контролю за обробкою персональних даних є прямим і практичним. Рішення Європейського суду з прав людини (далі – ЄСПЛ) формують мінімальний конвенційний стандарт, відступ від якого є підставою для встановлення порушення зобов’язань держави. Водночас ці рішення слугують джерелом доктринального обґрунтування вимог до незалежності наглядових органів, обсягу їхніх повноважень, стандартів пропорційності при обмеженні прав суб’єктів даних та меж допустимого державного спостереження. Ігнорування практики ЄСПЛ при розробці та застосуванні законодавства про захист персональних даних означає ризик відтворення структурних порушень, вже кваліфікованих Судом як несумісні з Конвенцією.

Еволюція підходів ЄСПЛ охоплює кілька виразних фаз. У першій фазі – 1970–1990-ті роки – ЄСПЛ зосереджувався на таємному стеженні та захисті кореспонденції, розуміючи приватність переважно як негативне право невтручання (Klass and Others v. Germany [92]; Malone v. United Kingdom [99]; Leander v. Sweden [93]).

Другий період (1990-2000-ні роки) ознаменований трансформацією, згідно із якою ЄСПЛ почав визнавати, що само лише збирання й зберігання інформації державою про особу, навіть якщо ці дані не використовуються активно, є втручанням у право на приватність (Rotaru v. Romania [94]; Amann v. Switzerland [95]; S. and Marper v. United Kingdom [96]).

Третій період характеризується виходом на проблематику масового цифрового спостереження, алгоритмічної обробки та розробкою стандартів, прямо застосовних до технологій штучного інтелекту і великих даних (Roman Zakharov v. Russia [97]; Big Brother Watch and Others v. United Kingdom [98]). Кожна з цих фаз залишила доктринальний слід, що є обов'язковим для аналізу будь-яким органом, відповідальним за контроль у сфері обробки персональних даних.

Визначальним для розуміння підходу ЄСПЛ до захисту персональних даних є питання про те, яка саме інформація підпадає під захист статті 8 Конвенції про захист прав людини і основоположних свобод [19]. Суд формував широке, функціональне розуміння персональних даних через аналіз конкретних обставин справ.

У вище згаданій справі Amann v. Switzerland (заява № 27798/95, рішення від 16 лютого 2000 року) [95] Суд дослідив обставини, за яких швейцарська федеральна поліція перехопила телефонний дзвінок заявника і внесла зібрані відомості до картотеки. Принциповий внесок цього рішення полягає у двох взаємопов'язаних положеннях. По-перше, Суд констатував, що зберігання даних про особу само по собі є втручанням у право на приватне життя, навіть якщо зібрана інформація є, на перший погляд, нейтральною або мінімальною за обсягом. По-друге, Суд встановив, що поняття «приватне життя» охоплює

всю сукупність відомостей, що стосуються ідентифікованої або такої, що може бути ідентифікована, особи, – формулювання, безпосередньо відтворювальне зі статті 2 Конвенції № 108. Це зближення конвенційного і спеціалізованого стандарту захисту даних у рамках одного рішення не є випадковим: воно відображає свідоме використання Судом acquis у сфері захисту даних для наповнення змістом розмитої категорії «приватне життя».

Справа Rotaru v. Romania [94] стала ще радикальнішим кроком. Суд встановив, що Румунська служба безпеки зберігала інформацію про заявника, частина якої виявилася недостовірною, ще з часів комуністичного режиму.

ЄСПЛ визнав порушення статті 8 Конвенції про захист прав людини і основоположних свобод [19] і сформулював тезу, що надалі стала наріжним каменем доктрини: навіть публічна інформація може підпадати під захист статті 8, якщо вона систематично збирається і зберігається у файлах органів влади. Суд підкреслив, що відсутність у законодавстві чітких меж щодо категорій інформації, яку може збирати спецслужба, строків зберігання та умов знищення даних, унеможливлює будь-яку ефективну оцінку пропорційності – а значить, саме за такого нормативного вакууму збирання даних є незаконним апріорі.

Аналіз рішення у справі Rotaru [94] дозволяє виокремити його концептуальне значення, яке виходить за межі конкретних обставин справи. По суті, Суд запровадив презумпцію проти відкритих баз даних без належної нормативної рамки: держава, що зберігає персональні дані без чіткого, доступного і передбачуваного правового регулювання, діє незаконно навіть тоді, коли конкретне використання цих даних не спричинило видимої шкоди. Ця логіка безпосередньо проєктується на вимоги до сучасних наглядових органів: перевірка законності обробки даних не може обмежуватися аналізом наслідків – вона повинна охоплювати оцінку правової бази як такої.

Найбільш розгорнуту концепцію захисту даних у практиці ЄСПЛ сформовано у справі S. and Marper v. United Kingdom [96]. Суд дослідив британську практику безстрокового зберігання зразків ДНК, клітинних

профілів і відбитків пальців осіб, виправданих або щодо яких провадження закрито. Рішення є знаковим у кількох відношеннях. По-перше, Суд чітко встановив, що ДНК-профілі є особливо чутливою категорією персональних даних, оскільки містять унікальну генетичну ідентифікаційну інформацію про особу і її родичів.

По-друге, Суд застосував принцип мінімізації даних ще до того, як він був кодифікований у GDPR: зберігання даних осіб, що не засуджені, не може вважатися необхідним у демократичному суспільстві, оскільки воно непропорційно переважує публічний інтерес над правом на приватність. По-третє, Суд підкреслив значення стигматизаційного ефекту: включення до бази даних осіб, чия вина не встановлена, прирівнює їх у реєстраційному значенні до засуджених злочинців, порушуючи принцип презумпції невинуватості в контексті захисту даних.

Доктринальний висновок, що випливає з аналізу цих трьох справ у сукупності, полягає в наступному. ЄСПЛ сформував широке, функціональне поняття персональних даних, що не залежить від категорії чутливості чи формального правового статусу інформації.

Будь-яка ідентифікуюча або ідентифікаційна інформація про особу, що є предметом систематичного державного збирання, зберігання або обробки, входить до сфери захисту статті 8 Конвенції про захист прав людини і основоположних свобод [19].

Само це «входження» вже є втручанням, що потребує виправдання. Органи контролю за обробкою персональних даних мають враховувати цю логіку при оцінці законності будь-якого реєстру, системи спостереження або бази даних, незалежно від їхнього офіційного призначення.

Одним із найбільш детально розроблених напрямів практики ЄСПЛ у сфері захисту персональних даних є питання стандартів законності втручання. Стаття 8 (2) Конвенції про захист прав людини і основоположних свобод [19], щоб будь-яке обмеження права на приватність здійснювалося «відповідно до

закону», переслідувало «законну мету» та було «необхідним у демократичному суспільстві».

Перша з цих вимог – законність – зазнала найбільш розгорнутого тлумачення, еволюціонувавши від формального критерію наявності правової підстави до змістовного стандарту якості закону.

Справа Malone v. United Kingdom [99] заклала підвалини доктрини «якості закону». Суд встановив, що англійське право, яке регулювало перехоплення комунікацій, не відповідало вимогам доступності (accessibility) та передбачуваності (foreseeability): воно не визначало з достатньою точністю ні підстав для застосування прослуховування, ні умов його здійснення, ні гарантій проти зловживань.

Формального існування правового регулювання виявилося недостатньо – Суд вимагав, щоб закон давав громадянинові можливість передбачити наслідки своїх дій і з достатньою впевненістю оцінити ризик стати об’єктом спостереження. Принцип передбачуваності (foreseeability) в його конвенційному значенні є суворішим за буквальний зміст цього терміна: він вимагає, щоб особа могла – за потреби з юридичною консультацією – передбачити, за яких умов державний орган матиме право отримати або використати її персональні дані.

Справа Liberty and Others v. United Kingdom [100] застосувала ці стандарти до масового перехоплення зовнішніх комунікацій.

Суд встановив, що британське законодавство, хоч і містило відповідні повноваження, не визначало чітких критеріїв відбору перехоплених даних, умов їх обробки та передачі, а також меж строків зберігання. Особливо принциповим є такий висновок Суду : відсутність у законодавстві «адекватних гарантій проти зловживань» є самостійною підставою для констатації порушення статті 8 Конвенції про захист прав людини і основоположних свобод, навіть якщо сам факт перехоплення формально допустимий. Поняття «адекватних гарантій» охоплює як матеріальні (чіткі критерії допустимості), так і процесуальні (незалежний контроль) елементи [100].

Найбільш повне і системне викладення вимог до законодавчого регулювання таємного спостереження міститься у справі Roman Zakharov v. Russia.

Суд дослідив систему СОРМ – технічний засіб, що зобов'язував операторів зв'язку надавати ФСБ прямий доступ до всіх телекомунікацій без попереднього судового дозволу.

ЄСПЛ розробив структурований перелік критеріїв оцінки систем таємного спостереження, що включає: (1) характер правопорушень, які можуть виправдати спостереження; (2) визначення категорій осіб, які можуть стати його об'єктом; (3) тривалість спостереження; (4) процедуру аналізу, використання і зберігання перехоплених даних; (5) запобіжні заходи щодо їх передачі третім особам; (6) умови і порядок знищення даних; (7) незалежний та ефективний нагляд за системою в цілому. Відсутність будь-якого з цих елементів у правовій базі є порушенням вимоги законності.

Рішення у справі Big Brother Watch and Others v. United Kingdom (заяви №58170/13, 62322/14 і 24960/15) [98] є найбільш актуальним для сучасного розуміння допустимого обсягу цифрового спостереження.

Суд дослідив три режими: масове перехоплення комунікацій, отримання даних від іноземних розвідок та отримання комунікаційних даних від постачальників послуг. У частині масового перехоплення Суд підтвердив, що такі системи не є несумісними з положеннями Конвенції, однак встановив ряд структурних вимог до їх правового регулювання. Принциповим є такий висновок: ризик масового спостереження для демократії залежить не тільки від використання отриманих даних, а й від самої архітектури системи – зокрема від того, чи існують ефективні механізми відбору, мінімізації та незалежного контролю вже на етапі перехоплення.

Ці рішення у сукупності мають пряме значення для регулювання сучасних технологій аналізу даних на основі алгоритмів і штучного інтелекту, у тому числі в контексті Акта про штучний інтелект ЄС [101]. Коли державний або приватний суб'єкт використовує систему профілювання або навчання

моделей, ці системи часто здійснюють масову автоматизовану обробку персональних даних без індивідуалізованого рішення для кожного випадку. Стандарти, розроблені ЄСПЛ для оцінки законності масового перехоплення, застосовні до таких систем: передбачуваність правової бази, адекватні гарантії проти зловживань та незалежний нагляд є вимогами, що не залежать від технічного способу здійснення обробки. Органи контролю за обробкою персональних даних мають враховувати ці критерії при оцінці законності систем обробки великих масивів даних та інструментів штучного інтелекту, що використовуються у публічному секторі.

Якщо стандарти законності регулюють питання наявності та якості правової підстави для обробки даних, то принцип пропорційності визначає межі допустимого обсягу такої обробки. У практиці ЄСПЛ принцип пропорційності в контексті захисту персональних даних набув трьох взаємопов'язаних вимірів: відповідності засобів легітимній меті, необхідності – у значенні відсутності менш обмежувальних альтернатив – та пропорційності у вузькому значенні, що передбачає справедливе балансування конкуруючих інтересів. Саме в цьому вимірі практика ЄСПЛ конвертує принцип пропорційності в операційні стандарти строків зберігання, обсягу зібраних даних і умов доступу до них.

Знаковим прикладом імплементації стандартів ЄСПЛ у практику контролю за обробкою персональних даних є результати перевірок підрозділів органів внутрішніх справ щодо ведення дактилоскопічного обліку, проведених Уповноваженим Верховної Ради України з прав людини у 2014 році.

Так, за результатами таких перевірок виявлено понад тисячу осіб (1004), у яких незаконно було відібрано відбитки пальців, причому жодного факту вилучення та знищення дактилокарт виправданих осіб зафіксовано не було [180]. Уповноважений прямо послався на практику ЄСПЛ у справах «S. and Marper v. the United Kingdom» [96] та «M.K. v. France» [103], відповідно до якої зберігання правоохоронними органами відбитків пальців осіб, щодо яких

кримінальне провадження закрито або які виправдані судом, становить надмірне втручання у права, гарантовані статтею 8 Конвенції про захист прав людини і основоположних свобод [19]. Цей випадок є ілюстрацією того, як стандарти ЄСПЛ виступають безпосереднім нормативним орієнтиром для оцінки правомірності обробки персональних даних не лише у правоохоронній сфері, але й діяльності наглядових органів.

Справа S. and Marper [96], яку вже розглянуто в контексті концепції персональних даних, містить і центральний для принципу пропорційності висновок: безстрокове зберігання даних осіб, щодо яких кримінальне переслідування не завершилося засудженням, є непропорційним навіть тоді, коли запровадження відповідного реєстру переслідує законну мету боротьби зі злочинністю.

Суд виявив, що англійський підхід не розрізняє осіб відповідно до характеру обвинувачень, ймовірності повторних правопорушень або часу, що минув після випадків, які спричинили внесення до бази. Ця індиференційованість є сама по собі ознакою диспропорційності: пропорційна система захисту даних повинна передбачати диференційований підхід залежно від індивідуальних обставин. Вказана проблематика також фіксується у Щорічних доповідях Омбудсмана України [102].

Справа M.K. v. France [103] розвинула цю логіку стосовно реєстру відбитків пальців.

Суд встановив, що французьке законодавство, яке передбачало зберігання відбитків пальців осіб, підозрюваних у вчиненні злочинів, протягом 25 років без урахування індивідуальних обставин справи і за відсутності ефективного механізму вилучення даних, є непропорційним. Принципово значущою є теза Суду про те, що відсутність реальної можливості домогтися вилучення даних є самостійним порушенням статті 8 Конвенції про захист прав людини і основоположних свобод [19]: право на захист персональних даних включає не тільки право на те, щоб зібрані дані не використовувалися протиправно, а й право вимагати їх знищення за

відсутності легітимних підстав для подальшого зберігання. Це положення безпосередньо відповідає праву на забуття, кодифікованому у статті 17 GDPR.

Рішення у справі Gaughran v. United Kingdom (заява № 45245/15, рішення від 13 лютого 2020 року) [104] підтвердило і систематизувало ці стандарти. Суд констатував порушення статті 8 Конвенції про захист прав людини і основоположних свобод [19] у зв'язку з тим, що Північна Ірландія зберігала відбитки пальців, фотографію і профіль ДНК заявника – засудженого за правопорушення середньої тяжкості – безстроково і беззастережно. Виходячи з принципу мінімізації, Суд вимагав, щоб строки і умови зберігання кримінальних ідентифікаційних даних визначалися відповідно до характеру правопорушення і ступеня ризику рецидиву, а не застосовувалися автоматично до всіх засуджених за будь-які злочини.

Доктринальне значення наведених рішень для порівняльного аналізу з GDPR полягає в тому, що Суд фактично сформулював принцип мінімізації даних (data minimisation) як елемент конвенційного права ще до його кодифікації у Регламенті.

Стаття 5(1)(c) GDPR закріплює, що персональні дані мають бути «адекватними, відповідними та обмеженими тим, що необхідно для цілей, з якими вони обробляються». Практика ЄСПЛ демонструє, що цей принцип є не просто нормативним приписом галузевого законодавства, а вимогою конвенційного рівня, чия порушення є порушенням основоположного права. Це означає, що наглядові органи у сфері захисту даних, оцінюючи відповідність практики оператора стандарту мінімізації, спираються не тільки на GDPR, а й на конвенційні зобов'язання держав. Порушення принципу мінімізації, відповідно, може утворювати підстави і для адміністративних санкцій у рамках GDPR, і для констатації порушення ЄКПЛ – два паралельних механізми відповідальності, що мають взаємопідсилюючий ефект.

Для практики органів контролю наведений аналіз означає таке: при проведенні перевірок реєстрів, баз даних або систем обробки персональних даних оцінка законності не може обмежуватися перевіркою наявності правової

підстави. Обов'язковим є аналіз строків зберігання, умов вилучення даних і наявності диференційованого підходу залежно від обставин конкретної особи. Відсутність таких механізмів є ознакою структурної невідповідності вимогам як GDPR, так і конвенційного права.

Сучасна фаза практики ЄСПЛ у сфері захисту персональних даних безпосередньо пов'язана з питаннями масового цифрового спостереження, аналізу великих масивів даних і автоматизованої обробки. Ці питання, що кілька десятиліть тому видавалися технічно спекулятивними, набули центрального значення у двох великопалатних рішеннях 2021 року.

Справа Big Brother Watch and Others v. United Kingdom та паралельна справа Centrum för Rättvisa v. Sweden (заява № 35252/08, рішення Великої палати від 25 травня 2021 року) [105] становлять комплементарний юрисдикційний аналіз систем масового перехоплення сигнальних комунікацій у двох державах-членах Ради Європи.

У першій справі Велика палата дійшла висновку, що британський режим масового перехоплення та режим отримання даних від іноземних розвідок порушували статтю 8 Конвенції про захист прав людини і основоположних свобод [19] через недостатність надійних і незалежних механізмів наглядового контролю. У справі Centrum for Rättvisa шведський режим сигнальної розвідки визнаний сумісним з Конвенцією, хоча і з мінімальним переважуванням на користь держави.

Теоретично найбільш значущим аспектом цих рішень є визнання того, що масовий збір даних є за своєю природою якісно відмінним від цільового спостереження. Коли держава здійснює масове перехоплення, вона апріорі не знає, які дані матимуть оперативну цінність: вся сукупність перехоплених комунікацій стає предметом подальшого аналізу.

Суд визнав, що само проведення масового перехоплення є втручанням у права кожної особи, чиї комунікації потрапляють до цієї системи, – незалежно від того, чи були конкретні дані в подальшому доступні аналітикам. Це принципово розширює суб'єктивну сферу захисту: порушення прав особи

може мати місце вже на стадії збирання даних, ще до будь-якого їх аналізу або використання.

Ця логіка застосовна до алгоритмічних систем і штучного інтелекту в повному обсязі. Системи навчання машинного інтелекту на основі великих масивів даних відтворюють логіку масового перехоплення: вони збирають і обробляють персональні дані всіх осіб, дані яких входять до навчальної вибірки, – без індивідуалізованої мети стосовно кожної з них.

Стандарти, розроблені ЄСПЛ для оцінки масового перехоплення, потребують трансляції у сферу систем штучного інтелекту: наявність правової підстави, чіткі критерії відбору даних, мінімізація обробки, незалежний нагляд і ефективні засоби правового захисту для осіб, чиї дані обробляються. Водночас ці стандарти поки що не отримали спеціалізованого тлумачення у практиці ЄСПЛ стосовно систем штучного інтелекту, що частково намагається компенсувати Конвенція про штучний інтелект – що є системним пробілом, який потребує практичного вирішення на рівні наглядових органів, окремі тенденції застосування якої досліджено надалі у дисертації (підрозділ 3.2.).

Системний аналіз практики ЄСПЛ у сфері захисту персональних даних виявляє стійку вимогу до наявності ефективного та незалежного органу нагляду – вимогу, що не є спеціально кодифікованою у тексті Конвенції про захист прав людини і основоположних свобод [19], проте послідовно виводиться Судом з сукупності процесуальних зобов’язань держав і принципу ефективності прав.

У справі Rotaru v. Romania [94], яка вже згадувалась, Суд констатував, що відсутність незалежного наглядового органу, наділеного правом здійснювати ефективний контроль за реєстром спецслужби, є самостійним конвенційним порушенням. Логіка є такою: якщо право на захист персональних даних підпадає під гарантії статті 8 Конвенції про захист прав людини і основоположних свобод [19], а виправданість обмеження цього права вимагає наявності «адекватних гарантій проти зловживань», то ці гарантії мають бути не лише декларовані, а й реально забезпечені. Реальне

забезпечення, у розумінні Суду, передбачає наявність органу, незалежного від виконавчої влади, що має повноваження доступу до реєстру, оцінки законності зберігання даних і ухвалення зобов'язальних рішень.

Справа Roman Zakharov v. Russia деталізує ці вимоги стосовно систем таємного спостереження. Суд встановив, що наглядові органи в Російській Федерації – зокрема суди та органи прокуратури, що формально уповноважені контролювати застосування СОРМ, – не мали реального доступу до перехоплених даних і не могли ефективно перевіряти обґрунтованість рішень ФСБ. Формальне існування наглядового механізму без фактичної можливості здійснювати незалежну перевірку є конвенційно недостатнім. Суд вимагав, щоб наглядовий орган мав необхідну технічну компетентність, незалежний від спецслужб доступ до відповідних систем і правовий інструментарій для ухвалення зобов'язальних приписів щодо припинення незаконної обробки або знищення незаконно зібраних даних.

Рішення у справі Big Brother Watch наводить найбільш системний перелік елементів ефективного нагляду: 1) незалежність від виконавчої влади та від суб'єктів, що здійснюють обробку; 2) наявність широких повноважень доступу до систем і документації; 3) компетентність у технічних питаннях відповідних технологій; 4) право ухвалення зобов'язальних рішень щодо припинення порушень; 5) прозорість діяльності та підзвітність відповідно до визначених законом процедур; 6) доступність для осіб, чиї права можуть бути порушені.

Ці вимоги мають пряме значення для оцінки існуючих і потенційних моделей наглядових органів у сфері захисту персональних даних. Орган, що формально є незалежним за назвою, але залежить від органів виконавчої влади в питаннях фінансування, призначення керівників або встановлення пріоритетів перевірок, не відповідає конвенційному стандарту незалежності. Так само недостатнє ресурсне забезпечення, що унеможливлює технічну перевірку складних цифрових систем обробки, є конструктивним дефіцитом, що підриває саму функцію нагляду. Відповідно, правовий режим діяльності

наглядового органу у сфері захисту персональних даних повинен забезпечувати не тільки інституційну незалежність, а й операційну спроможність – кадрову, технічну та фінансову.

Стаття 51 GDPR вимагає незалежності наглядових органів і надає їм широкий перелік коригуючих повноважень. Однак практика ЄСПЛ додає до цих нормативних вимог вимір правового захисту, відсутній у GDPR: порушення вимог до ефективності наглядового органу може бути предметом індивідуальної скарги до ЄСПЛ, а не тільки підставою для розгляду в процедурах Комісара з питань захисту даних.

Це означає, що держави несуть конвенційну відповідальність не тільки за неправомірні конкретні дії з обробки даних, а й за системні дефіцити у механізмах нагляду.

Аналіз практики ЄСПЛ щодо України у сфері захисту персональних даних виявляє стійку кореляцію між системними вадами вітчизняного правового регулювання і конкретними порушеннями Конвенції, зафіксованими Судом. Ця кореляція має діагностичне значення: вона дозволяє ідентифікувати пріоритетні напрями реформування з опорою на конвенційний стандарт, а не лише на критерії гармонізації з GDPR.

Справа Garnaga v. Ukraine (заява № 20390/07, рішення від 16 травня 2013 року) [106] порушила питання, що на перший погляд видається далеким від захисту персональних даних у технічному значенні: законодавчу заборону змінювати по батькові. Проте ЄСПЛ кваліфікував законодавче закріплення по батькові – ідентифікаційного компонента імені особи – як частину персональних даних у значенні статті 8 Конвенції про захист прав людини і основоположних свобод [19]. Відмова держави надати особі право визначати цей компонент своєї ідентичності становила непропорційне втручання, позбавлене достатнього законодавчого обґрунтування.

Виконання цього рішення спричинило зміни до Цивільного та Сімейного кодексів України, що вперше гарантували право вибору по

батькові. Ця справа ілюструє, як вимоги ЄСПЛ мають прямий нормотворчий вплив на законодавство держав-відповідачів.

Справа Zaichenko v. Ukraine [107] виявила системну прогалину: відсутність спеціального законодавчого врегулювання порядку збирання психіатричних даних у рамках адміністративного провадження. Суд встановив, що дії органів внутрішніх справ, які зібрали дані про стан психічного здоров'я заявника без відповідних правових підстав, порушують статтю 8 Конвенції про захист прав людини і основоположних свобод [19].

Характерно, що Суд не кваліфікував це як порушення загальних принципів захисту даних, а констатував відсутність конкретної нормативної процедури – тобто порушення вимоги передбачуваності закону. На виконання рішення Міністерство юстиції розробило відповідний законопроєкт, що залишається на стадії опрацювання. Ця незавершеність виконання є прикладом інституційної неспроможності, що сама по собі є предметом критики в контексті вимог ЄСПЛ до ефективного виконання судових рішень.

Справа Surikov v. Ukraine (заява № 42788/06, рішення від 26 січня 2017 року) [108] поставила питання про законність збирання і використання чутливих психіатричних даних роботодавцем. Суд встановив, що тлумачення і застосування судами України норм про захист медичних даних дозволяло зберігати і використовувати застарілі чутливі дані за межами мети, для якої вони збиралися, – що є порушенням принципів мінімізації та обмеження мети обробки. Це рішення ставить системне питання про відповідність практики національних судів конвенційним стандартам: недостатньо мати формально адекватне законодавство, якщо його застосування систематично відхиляється від вимог статті 8 Конвенції про захист прав людини і основоположних свобод [19].

Для аналізу перспектив імплементації стандартів ЄСПЛ у новому законі про захист персональних даних принципово важливими є такі спостереження.

По-перше, практика ЄСПЛ стосовно України демонструє, що порушення Конвенції у сфері захисту даних не є наслідком тільки відсутності

відповідного законодавства: вони виникають також через недостатню деталізацію процедур (Zaichenko), через неправильне застосування наявних норм (Surikov) і через незадовільне функціонування наглядових механізмів.

По-друге, нинішня модель покладення повноважень наглядового органу на Уповноваженого Верховної Ради України з прав людини є системно неоптимальною: поєднання широкого правозахисного мандату з технічно складними завданнями нагляду за обробкою персональних даних унеможливлює досягнення операційної спроможності, яку вимагає ЄСПЛ.

По-третє, майбутній закон про захист персональних даних повинен відтворювати не тільки норми GDPR, а й конвенційні стандарти – зокрема, чіткі критерії строків зберігання, механізми вилучення і знищення даних, а також ефективні процедури оскарження рішень про відмову у задоволенні запитів суб'єктів даних.

Розвиток законодавства України у сфері захисту персональних даних також не може ігнорувати актуальні проблеми, пов'язані з обробкою персональних даних в умовах воєнного стану. Проєкт Закону України від 25.10.2022 року № 8153, що перебуває на розгляді Верховної Ради, містить ряд позитивних кроків у напрямі гармонізації з GDPR, однак не вирішує в повному обсязі питання механізму незалежного нагляду та повноважень відповідного органу. Відповідно, реформа законодавства про захист персональних даних, щоб відповідати конвенційному стандарту, повинна включати і реформу інституційної архітектури контролю.

ЄСПЛ сформував у практиці тлумачення статті 8 Конвенції про захист прав людини і основоположних свобод [19] автономну систему стандартів захисту персональних даних, що хронологічно передує системі GDPR і Конвенції № 108+ та слугує їх конституційно-правовою основою. Ця система є обов'язковою для держав-учасниць Конвенції незалежно від ступеня їхньої гармонізації з правом ЄС, що надає їй особливе значення для держав, що не є членами ЄС, але прагнуть відповідності конвенційним стандартам.

Принцип широкого тлумачення персональних даних, розроблений ЄСПЛ у справах Amann, Rotaru [94] та S. and Marper [96], встановлює, що будь-яка ідентифікуюча або ідентифікаційна інформація про особу, що є предметом систематичної державної або приватної обробки, підпадає під захист статті 8 Конвенції про захист прав людини і основоположних свобод [19]. Збирання і зберігання таких даних є втручанням, що вимагає виправдання. Цей підхід є суворішим за визначення персональних даних у GDPR з точки зору підстав для захисту: він не залежить від формального статусу інформації або технічного способу її обробки.

Принцип якості закону, що вимагає доступності, передбачуваності та наявності адекватних гарантій проти зловживань, є конвенційним еквівалентом принципу законності обробки GDPR, але з більш широким інституційним виміром: він охоплює не тільки підстави для обробки, а й процедуру нагляду і засоби правового захисту. Законність правового регулювання у цьому значенні є необхідною, але недостатньою умовою відповідності Конвенції – обов’язковим є також наявність ефективних механізмів забезпечення.

Принцип мінімізації даних як конвенційна вимога, виведена ЄСПЛ у справах S. and Marper, M.K. v. France і Gaughran [103], є нормативно обов’язковою ще до GDPR і незалежно від нього. Відсутність диференційованих строків зберігання, механізмів перегляду необхідності зберігання і реальних процедур вилучення даних є конвенційним порушенням.

Наглядові органи у сфері захисту даних мають оцінювати ці параметри як критерії законності обробки, а не тільки як рекомендовані найкращі практики.

Вимоги ЄСПЛ до ефективного і незалежного органу нагляду (Rotaru, Roman Zakharov, Big Brother Watch) [94; 97; 98] є конвенційними зобов’язаннями держав, порушення яких тягне відповідальність за статтею 8 Конвенції про захист прав людини і основоположних свобод [19].

Незалежність органу нагляду у конвенційному значенні включає не тільки формальну інституційну відокремленість, а й операційну спроможність – кадрову, технічну і фінансову. Модель, за якою функції наглядового органу поєднуються з широкою правозахисною мандатурою без виділення спеціальних ресурсів і компетенцій, є структурно неадекватною вимогам Конвенції.

Практика ЄСПЛ стосовно України виявляє стійкий патерн: порушення статті 8 Конвенції про захист прав людини і основоположних свобод [19] у сфері захисту персональних даних зумовлені не тільки відсутністю законодавчого регулювання, а й недостатньою деталізацією процедур (Zaichenko [107]), неправильним застосуванням наявних норм судами (Surikov [108]) і системними дефіцитами наглядових механізмів.

Реформування законодавства про захист персональних даних в Україні повинне адресувати всі три виміри, а не обмежуватися формальною гармонізацією з GDPR.

Порівняльний аналіз практики ЄСПЛ, Конвенції № 108+ і GDPR виявляє конвергенцію матеріальних стандартів захисту даних при збереженні відмінностей у механізмах виконання. GDPR і Конвенція № 108+ є галузевими інструментами, що деталізують конвенційні вимоги. ЄСПЛ, застосовуючи статтю 8, забезпечує конституційний мінімальний поріг, нижче якого жодне галузеве регулювання не може опускатися. Розуміння цієї ієрархії є ключовим для органів контролю: при конкуренції інтерпретацій між нормами GDPR і конвенційними вимогами останні мають пріоритет.

Ризик автоматизованої обробки даних і алгоритмічного профілювання ставить перед правом захисту персональних даних виклики, що виходять за межі наявних нормативних категорій. Здатність алгоритмів виводити чутливу інформацію з нечутливих вихідних даних не охоплена в повному обсязі ні чинним конвенційним правом, ні GDPR, ні Конвенцією про штучний інтелект [147]. Органи контролю мають враховувати цей пробіл при оцінці систем

штучного інтелекту і розробляти адаптивні підходи до застосування принципу мінімізації та вимог про оцінку впливу на захист даних.

Практика ЄСПЛ у сфері захисту персональних даних є динамічним нормативним ресурсом, що реагує на технологічний розвиток через послідовне застосування принципів до нових контекстів. Органи контролю, законодавці і суди повинні відстежувати еволюцію цієї практики як обов'язкову складову нормативно-правової бази у сфері захисту даних – не тільки у частині конкретних рішень щодо своїх держав, а й у частині загальних доктринальних розробок, що формують конвенційні стандарти для всіх держав-учасниць Ради Європи.

Якщо практика Європейського суду з прав людини формує конвенційний мінімум захисту персональних даних, виводячи його зі змісту статті 8 Конвенції про захист прав людини і основоположних свобод, то Суд ЄС діє у іншій правовій парадигмі. Тлумачачи право на захист персональних даних як автономне фундаментальне право Європейського Союзу, закріплене статтею 8 Хартії основних прав Європейського Союзу [109], Суд ЄС визначає операційний зміст і межі Загального регламенту про захист даних (GDPR).

Для України як держави-кандидата на членство в Європейському Союзі, що взяла на себе зобов'язання гармонізації національного законодавства з acquis communautaire, ця практика має не порівняльно-ілюстративне, а нормативно-орієнтуюче значення.

Принципова відмінність між підходами Європейського суду з прав людини і Суду ЄС є не лише технічною, але й доктринально значущою. Європейський суд з прав людини розглядає захист персональних даних як складову права на повагу до приватного життя і застосовує трискладовий тест виправданості втручання, що охоплює вимоги законності, наявності легітимної мети та необхідності у демократичному суспільстві.

Суд ЄС, натомість, трактує статтю 8 Хартії як самостійне право, обмеження якого підпорядковується власному тесту пропорційності відповідно до статті 52 Хартії основних прав Європейського Союзу [109].

Нижче проаналізовано шість рішень Суду ЄС, що є визначальними для розуміння цього стандарту та його значення для реформування української системи контролю за обробкою персональних даних.

У справі Google *Spain* SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González Суд ЄС розглянув питання про те, чи зобов'язаний оператор пошукової системи на вимогу фізичної особи вилучати зі списку результатів пошуку посилання на веб-сторінки з персональними даними цієї особи навіть у тому разі, коли публікація на самих сторінках є законною [110]. Позивач вимагав видалення посилань на оголошення про примусовий продаж його майна, здійснений багато років тому, оскільки відповідна інформація втратила актуальність.

Суд визнав оператора пошукової системи «контролером» у розумінні статті 2(d) Директиви 95/46/ЄС, обґрунтувавши це тим, що пошукова система самостійно визначає мету і засоби обробки персональних даних, здійснюючи їх збирання, індексування, зберігання і надання користувачам. Суд встановив, що суб'єкт даних має право вимагати видалення посилань, якщо відображення відповідної інформації у результатах пошуку є неадекватним, таким, що не відповідає меті обробки, неактуальним або надмірним з огляду на час, що минув. Доктринальне значення цього рішення полягає в тому, що так зване «право на забуття» було кваліфіковане не як окремий аспект приватності, а як конкретизація права на захист персональних даних у його автономному розумінні. Із рішення випливає, що це право охоплює позитивний обов'язок контролера забезпечувати актуальність і пропорційність обробки протягом усього її строку.

Для української правової системи значення справи є подвійним. З одного боку, чинний Закон України «Про захист персональних даних» формально закріплює право особи вимагати знищення своїх даних, однак не встановлює дієвого механізму реалізації права на забуття. З іншого боку, положення проєкту Закону України від 25.10.2022 року № 8153 [178] лише частково усувають цю прогалину, оскільки не дають відповіді на питання про

обсяг відповідальності платформ, що агрегують персональні дані з відкритих джерел.

Дві послідовні справи за позовами австрійського активіста Максиміліана Шремса сформували стандарт незалежності наглядового органу і законності транскордонної передачі персональних даних. У першій справі Суд ЄС розглянув скаргу щодо передачі даних користувача компанією Facebook до Сполучених Штатів Америки на підставі механізму Safe Harbour і визнав відповідне рішення Європейської Комісії про адекватність захисту недійсним [111].

У другій справі, що стала продовженням першої після заміни Safe Harbour механізмом Privacy Shield, Суд ЄС визнав недійсним і цей механізм, встановивши, що законодавство Сполучених Штатів Америки у сфері національної безпеки не забезпечує рівня захисту, рівноцінного гарантованому правом Європейського Союзу [112]. Ключова правова позиція, спільна для обох рішень, полягає в тому, що наглядові органи із захисту персональних даних зобов'язані діяти незалежно і не можуть бути беззастережно зв'язані рішенням Європейської Комісії про адекватність, якщо таке рішення суперечить Хартії [109]. Показово, що вказані рішення у подальшому матимуть вплив на EU-US Data Privacy Framework (Рішення Європейської Комісії (ЄС) 2023/1795) й зачіпатимуться у практиці Верховного Суду США [113].

Суд ЄС кваліфікував незалежність наглядового органу не як інституційну перевагу чи організаційну характеристику, а як конституційну вимогу, що зобов'язує орган діяти навіть усупереч позиції виконавчої влади.

Для України ці рішення мають безпосереднє значення при оцінці конституційного статусу майбутнього спеціалізованого органу захисту персональних даних – Національної комісії з питань захисту персональних даних та доступу до публічної інформації [52].

Обґрунтовано, що якщо такий орган буде підпорядкований виконавчій владі або його мандат не включатиме права діяти всупереч позиції уряду, він

не відповідатиме стандарту незалежності, сформульованому Судом ЄС, а отже, і вимогам статті 51 GDPR.

У справі Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV Суд ЄС розглянув правові наслідки розміщення онлайн-рітейлером на своєму веб-сайті стороннього плагіна соціальної мережі Facebook (кнопки «Подобається»), унаслідок чого персональні дані відвідувачів сайту передавалися компанії Facebook без їхнього відома і незалежно від того, чи були вони користувачами цієї мережі [114].

Суд встановив, що власник сайту є спільним контролером разом із оператором соціальної мережі щодо стадії збирання і передачі персональних даних, навіть попри те, що він не має доступу до самих даних і не визначає мету їх подальшої обробки. Із рішення випливає принцип, згідно з яким поняття «контролер» і «спільний контролер» підлягають широкому функціональному тлумаченню: інтеграція стороннього програмного коду, що ініціює збирання даних, є достатньою підставою для кваліфікації особи як спільного контролера з відповідним обсягом обов'язків. Значення цього висновку для української правової системи полягає у виявленні суттєвої прогалини: чинне законодавство не закріплює інституту спільного контролю в явному вигляді, що є критичним з огляду на масштабне використання вітчизняними веб-сайтами і застосунками сторонніх трекерів, піксельних кодів і аналітичних інструментів.

У справі Meta Platforms Inc. and Others v. Bundeskartellamt Суд ЄС розглянув ситуацію, за якої Федеральне антимонопольне відомство Німеччини встановило, що компанія Facebook зловживає домінуючим становищем на ринку, збираючи персональні дані користувачів із позамережевих джерел без належної правової підстави [115]. Особливість справи полягала в перетині двох правових режимів – конкурентного права і права захисту персональних даних.

Суд ЄС підтвердив, що законний інтерес як підстава обробки, передбачена статтею 6(1)(f) GDPR, не може виправдовувати систематичну

обробку особливо чутливих даних у комерційних цілях, а також роз'яснив взаємозв'язок між правом конкуренції і правом захисту даних.

Із рішення випливає, що обробка на підставі законного інтересу підлягає суворому тесту необхідності і балансування, а домінуюче становище платформи фактично виключає вільний вибір користувача і ставить під сумнів дійсність будь-якої наданої ним згоди. Для України висновки цієї справи є актуальними при оцінці практики великих цифрових платформ, що діють на національному ринку: обґрунтовано, що вітчизняне законодавство не розмежовує підстав обробки для звичайних і домінуючих суб'єктів, не містить концепції «вимушеної згоди» і не пов'язує антимонопольне регулювання з режимом захисту персональних даних.

У справі Rīgas satiksme Суд ЄС розглянув ситуацію, за якої латвійський оператор громадського транспорту відмовив особі, потерпілій унаслідок дорожньо-транспортної пригоди, у наданні персональних даних винуватця пригоди, обґрунтовуючи відмову необхідністю захисту персональних даних останнього [116].

Суд ЄС встановив, що законний інтерес третьої особи може слугувати належною підставою для передачі персональних даних за умови, що він переважує інтереси суб'єкта даних. Із рішення випливає, що тест балансування інтересів є обов'язковим елементом оцінки правомірності і не може бути замінений абсолютною забороною передачі; захист персональних даних не може бути підставою для відмови у захисті інших законних прав. Для української правозастосовної практики значення справи полягає у протидії інструменталізації захисту персональних даних як універсального приводу для відмови у наданні інформації.

Показовими прикладами такої інструменталізації є відмови у доступі до відомостей про власника транспортного засобу після дорожньо-транспортної пригоди або відмови суб'єктів господарювання надати дані контрагента на запит потерпілої особи.

Проаналізовані рішення у сукупності формують доктринальний стандарт, що виходить за межі буквального тексту GDPR і має враховуватися при реформуванні національної системи контролю. По-перше, практика Суду ЄС розширює поняття контролера і запроваджує інститут спільного контролю (Google Spain, Fashion ID), що потребує прямого закріплення у національному законодавстві. По-друге, вона встановлює операційний, а не декларативний стандарт незалежності наглядового органу (Schrems I і II), який є визначальним орієнтиром для формування статусу Національної комісії. По-третє, вона обмежує застосування законного інтересу і згоди суворим тестом балансування (Meta Platforms, Rīgas satiksme), унеможливлюючи як зловживання підставами обробки, так і інструменталізацію захисту даних для обмеження інших прав. Обґрунтовано, що для України як держави-кандидата саме стандарт Суду ЄС, а не лише конвенційний мінімум Європейського суду з прав людини, є юридично орієнтуючим при розробленні та застосуванні законодавства у сфері захисту персональних даних.

Захист персональних даних є ширшою категорією, що охоплює матеріально-правові норми (визначення, принципи, права суб'єктів), тоді як механізм контролю є системою процесуально-організаційних інструментів, що забезпечують практичну реалізацію та примусове виконання матеріальних норм. Саме механізми контролю – суб'єкти, повноваження, процедури, санкції – становлять предмет цього підрозділу.

У доктрині адміністративного права механізм контролю традиційно розуміється як сукупність взаємопов'язаних елементів: 1) суб'єктів контролю та їх правового статусу; 2) об'єктів і предмету контрольної діяльності; 3) підстав та форм контролю; 4) процедур здійснення контрольних заходів; 5) процедур розгляду скарг; 6) механізмів застосування примусових заходів; 7) інструментів транскордонного контролю. Аналіз кожної юрисдикції здійснюватиметься саме через призму цих елементів.

Порівняльно-правове дослідження охоплює три принципово відмінні моделі, що сформувалися у провідних юрисдикціях: правозахисну модель

Європейського Союзу, Сполучених Штатів Америки та Китайської Народної Республіки. Вибір цих юрисдикцій зумовлений не лише їх практичним значенням для регулювання глобальних цифрових платформ, що оперують на ринку України, але й тим, що кожна з них втілює самостійну і внутрішньо послідовну концепцію співвідношення державного контролю і прав особи у цифровому просторі.

Авторська гіпотеза дослідження полягає в такому: ефективність механізму контролю за обробкою персональних даних знаходиться у прямій залежності від трьох чинників – інституційної незалежності наглядового органу, повноти та визначеності його контрольних повноважень, а також наявності пропорційного і здійснюваного санкційного механізму. Перевірка цієї гіпотези є наскрізним завданням усього підрозділу.

Механізм контролю за обробкою персональних даних в Європейському Союзі представлений багаторівневою системою. Перший рівень утворюють національні органи захисту даних (Data Protection Authorities, DPA) – незалежні публічні органи держав-членів, що діють на підставі статей і національного законодавства [16].

У країнах Європейського Союзу функціонування наглядових органів базується на положеннях Загального регламенту про захист даних (51–59 GDPR), який передбачає широкі повноваження національних органів із захисту даних.

Другий рівень – Європейська рада із захисту даних (EDPB), заснована статтею 68 GDPR як орган координації та видачі обов’язкових рішень у транскордонних справах.

Третій рівень – судовий: Суд справедливості ЄС (CJEU) здійснює правову інтерпретацію GDPR і формує обов’язкові прецеденти, а Загальний суд (General Court) розглядає скарги на рішення Європейської ради із захисту даних.

Правовий статус DPA за статтею 51 GDPR визначається трьома ключовими характеристиками: (а) публічний характер органу – DPA є

частиною системи публічного управління, наділеною державно-владними повноваженнями; (б) незалежність – DPA здійснює свої повноваження «з повною незалежністю» (ст. 52(1)); (в) спеціальна компетенція – DPA є єдиним органом, наділеним повноваженнями нагляду за GDPR на національному рівні.

Зазначений правовий статус відрізняється від статусу Омбудсмана (контроль за дотриманням прав і свобод людини і громадянина з боку державних органів), суду (процесуальна незалежність і нейтралітет), статусу виконавчого органу (підпорядкованість уряду) і є самостійним видом суб'єкта публічного управління – регуляторним органом.

Європейська рада із захисту даних є органом Союзу і має правосуб'єктність. ЇЇ рішення, прийняті в порядку статей 65–66 GDPR (механізм вирішення спорів та механізм термінового провадження), є юридично обов'язковими для всіх DPA держав-членів – унікальна риса, що відрізняє ЄС-систему від будь-яких інших міжнародних моделей координації у сфері захисту даних.

Гарантії незалежності DPA за GDPR є комплексними і закріплені на рівні первинного законодавства ЄС. Стаття 52 GDPR передбачає: функціональну незалежність (відсутність зовнішніх інструкцій); фінансову незалежність (власний бюджет); кадрову незалежність (особи, що очолюють DPA, не можуть бути звільнені під час строку повноважень, крім як за грубе порушення закону); заборону несумісності (члени DPA не можуть провадити будь-яку несумісну оплачувану або неоплачувану діяльність) [16]. Стаття 54(1)(e) додатково вимагає, щоб строк повноважень членів DPA та умови їх дострокового припинення були встановлені законом.

Важливим аспектом, який часто лишається поза увагою, є те, що незалежність DPA неодноразово ставала предметом розгляду CJEU.

Принципове значення для утвердження незалежності наглядових органів має рішення Суду ЄС від 9 березня 2010 року у справі C-518/07 (Комісія проти Німеччини). Суд констатував, що Німеччина, підпорядкувавши

адміністративній опіці держави наглядові органи земель, компетентні контролювати обробку персональних даних у недержавному секторі, помилково імплементувала вимогу статті 28 Директиви 95/46/ЄС щодо виконання цими органами своїх завдань «у повній незалежності», і тим самим не виконала своїх зобов'язань за Директивою. Сформульований Судом стандарт, що виключає будь-які форми впливу виконавчої влади на наглядові органи, згодом було закріплено у статті 52 GDPR. Таким чином, незалежність DPA є не лише нормативною вимогою, але й об'єктом судового захисту на рівні ЄС.

Відтак, на думку автора, система гарантій незалежності DPA в ЄС є найбільш розвиненою серед усіх досліджених юрисдикцій і може слугувати еталоном при розробці відповідного законодавства в Україні. Ключовими елементами, що мають бути відтворені, є: (а) заборона зовнішніх інструкцій; (б) окремий бюджет, затверджений парламентом; (в) строковий мандат з обмеженими підставами дострокового припинення; (г) процедура звітності перед парламентом, а не урядом.

Стаття 58 GDPR закріплює три категорії контрольних повноважень DPA, що в сукупності формують повний цикл контрольної діяльності [16].

Розслідувальні повноваження (ст. 58 (1)) включають: доступ до всіх персональних даних, що обробляються, та до будь-якої інформації, необхідної для виконання завдань DPA; доступ до приміщень контролера і обробника даних, включно з обладнанням; сповіщення контролера або обробника про передбачувані порушення.

Коригувальні повноваження (ст. 58(2)) є найбільш практично значущими і охоплюють: видання попереджень і доган; наказ про задоволення запитів суб'єкта даних; наказ про приведення обробки у відповідність до GDPR або про знищення даних; тимчасову або постійну заборону обробки; розпорядження про сповіщення суб'єктів даних про порушення; анулювання сертифікації; накладення адміністративних штрафів. Зокрема, у Німеччині федеральні та земельні органи із захисту даних (Data Protection Authorities)

також мають право проводити перевірки без попередження, видавати обов'язкові приписи. Водночас до компетенції органу віднесено право накладати адміністративні штрафи без звернення до суду. Практика показує, що такі штрафи можуть бути значними. Наприклад, у 2020 році німецький регулятор оштрафував компанію H&M на понад 35 млн євро за незаконне збирання даних працівників [117].

Національна комісія з питань інформатики і свобод Французької Республіки (CNIL – Commission nationale de l'informatique et des libertés) як незалежний орган у Французькій Республіці, також має повноваження самостійно накладати санкції. Відомим є рішення Національної комісії з питань інформатики і свобод Французької Республіки (CNIL)щодо компанії Google, на яку було накладено штраф у розмірі 50 млн євро за порушення принципів прозорості обробки персональних даних [118]. Однак важливо підкреслити, що стягнення штрафу є лише одним із інструментів коригувального впливу – і не завжди найбільш ефективним. У справі Amazon France Logistique CNIL комплексно застосувала аналіз пропорційності та наказ про виправлення порушень разом із накладенням штрафу, що свідчить про стратегічний та комплексний підхід до вибору заходів впливу.

Процедура здійснення перевірок залежить від виду контролю. Плановий аудит (ex officio) ініціюється на підставі аналізу ризиків, скарг або публічної інформації про можливі порушення. Розслідування за скаргою (ст. 77 GDPR) є обов'язковим: DPA зобов'язаний повідомити скаржника про хід розгляду і результат провадження [16].

В контексті зазначеного важливо наголосити і на системі розгляду скарг. Стаття 77 GDPR гарантує суб'єкту даних право подати скаргу до DPA будь-якої держави-члена ЄС – незалежно від того, де знаходиться контролер. Це право є необмеженим і безумовним: DPA не може відмовити у прийнятті скарги до розгляду з формальних підстав.

Також стаття 78 GDPR забезпечує право на ефективний судовий захист проти рішень DPA, а стаття 79 – право на судовий захист проти контролера або обробника незалежно від провадження у DPA.

Таким чином, суб'єкт даних має паралельні можливості адміністративного та судового захисту, що є важливою гарантією ефективності системи.

Строки розгляду скарг GDPR не встановлює, передбачаючи лише зобов'язання повідомити скаржника «в розумні строки» [16]. Практика DPA свідчить, що справи можуть тривати роками – що є суттєвим недоліком системи. Для прикладу, у справі CNIL проти Amazon France Logistique тривалість провадження становила понад чотири роки (з листопада 2019 по грудень 2023), що охоплювало: п'ять інспекцій на місцях, тривале листування, призначення рапортера, заслуховування сторін і прийняття рішення.

Такий строк свідчить про ретельність, але водночас – про недостатню оперативність реагування як системний недолік. Справа Комісії із захисту персональних даних Ірландії (DPC) проти Meta щодо персональних даних дітей перебувала на розгляді понад два роки, а тиск Європейської ради із захисту даних через механізм статті 65 GDPR виявився необхідним для прийняття остаточного рішення.

У більшості європейських юрисдикцій наглядові органи поєднують правозахисну функцію з ефективними інструментами примусу та санкцій, що забезпечує реальний вплив на суб'єктів обробки персональних даних.

Санкційний механізм GDPR є дворівневим. Перший рівень (ст. 83(4)): штрафи до €10 млн або 2% глобального обороту – за порушення технічних вимог (процедура оцінки впливу на захист даних, записи обробки, призначення DPO тощо). Другий рівень (ст. 83(5)): штрафи до €20 млн або 4% глобального обороту – за порушення базових принципів обробки, прав суб'єктів даних, передачі даних до третіх країн.

Практика застосування санкцій демонструє значну диференціацію між DPA. Найбільші штрафи зафіксовано в Ірландії (Meta: €1,2 млрд у 2023 р. за

порушення ст. 44 GDPR при передачі даних до США, та LinkedIn: на 310 мільйонів євро за те, що вона не повідомила користувачам, як їхні дані використовуються для поведінкового аналізу та цільової реклами), Люксембурзі (Amazon: €746 млн у 2021 р.) та Франції (Google €150 млн у 2022 р. за порушення законодавства про cookies, Amazon France Logistique €32 млн у 2023 р. за незаконне стеження за працівниками) [119, С. 195-198].

Разом із тим, ряд наглядових орагнів застосовують штрафи, що не перевищують кількох тисяч євро навіть за системні порушення, – що породжує проблему нерівномірності правозастосування («forum shopping»).

Справа Національної комісії з питань інформатики і свобод Французької Республіки (CNIL) проти Amazon France Logistique є особливо показовою для аналізу санкційного механізму. Національна комісія з питань інформатики і свобод Французької Республіки (CNIL) встановила, що система збору і обробки даних про продуктивність і «неактивний час» кожного працівника була системно надмірною: зокрема, індикатор «Stow Machine Gun», що відстежував швидкість дій сканера з точністю до 1,25 секунди, та показники перерв тривалістю менше 10 хвилин були визнані незаконними як такі, що порушують принцип мінімізації даних (ст. 5(1)(c) GDPR) та вимоги законної підстави (ст. 6 GDPR).

Показово, що орган застосував не лише штраф, але й публічне оголошення рішення, яке збережеться в ідентифікованій формі протягом двох років – що саме по собі є потужним інструментом репутаційного тиску.

Механізм транскордонного контролю, у випадку транскордонної обробки даних, запроваджує принцип «єдиного вікна» (One-Stop-Shop) відповідно до статей 56–60 GDPR, що є найбільш інноваційним елементом ЄС-моделі контролю.

За таким принципом, повноваження здійснює орган держави місцезнаходження контролера або оператора. Відтак, наглядовий орган держави-члена, де знаходиться головне представництво контролера (Lead Supervisory Authority, LSA), виступає провідним органом для всього

транскордонного провадження, а наглядові органи держав-членів, яких стосується обробка даних (Concerned Supervisory Authorities, CSA), мають право надавати обґрунтовані заперечення проти проєкту рішення LSA. Якщо ж LSA не погоджується із запереченнями, спір передається до Європейської ради із захисту даних, рішення якого є обов'язковим (ст. 65 GDPR).

Передбачається, що за відсутності у організації головного представництва в ЄС, вона продовжуватиме працювати з DPA кожної держави-члена, у якій вона працює, та не матиме права на роботу за принципом «єдиного вікна».

Ключовим прецедентом щодо транскордонного виміру контролю є рішення CJEU у справі Google LLC v. CNIL (C-507/17, 2019). Суд встановив, що GDPR не зобов'язує оператора пошукової системи застосовувати право на забуття до всіх своїх глобальних доменів, проте суд не виключив можливості застосування ширших, включно з глобальними, заходів дереференсування на підставі національного права держав-членів та за умови дотримання принципу пропорційності та належного балансу основоположних прав. У науковій спільноті [120] прецедент кваліфікується як «пост-Сноуденська жорстка позиція CJEU», що допускає варіативність національного рівня в межах загальної рамки GDPR. Важливо акцентувати: рішення підтверджує, що DPA може ухвалювати рішення, що мають екстериторіальний ефект, якщо правова підстава для цього достатньо обґрунтована у внутрішньому праві. Це принципово відрізняє ЄС-підхід від усіх інших моделей.

Втім наведений вище принцип виявляє наступні лакуни у правозастосуванні. Для прикладу, понад третина урядових вебсайтів ЄС розміщена на серверах, кінцевий бенефіціарний власник яких перебуває поза юрисдикцією Європейського Союзу [121], а понад половина урядових поштових доменів покладається на непов'язаних із Європейським Союзом операторів – факт, що має пряме значення для оцінки реальної (а не формальної) ефективності контрольного механізму. Отже залежність країн Європейського Союзу від позаєвропейських постачальників обчислювальних

потужностей, хмарних рішень та напівпровідникових компонентів є проблемою юрисдикційного контролю в розумінні права захисту даних, оскільки дані, що обробляються на інфраструктурі під позаєвропейською юрисдикцією, потенційно підпадають під дію екстериторіальних режимів доступу.

Показово, що саме цю проблему юрисдикційної залежності від позаєвропейської хмарної інфраструктури Європейська Комісія визнала предметом окремого регулювання. 3 червня 2026 року оприлюднено проєкт Регламенту про розвиток хмарних технологій та штучного інтелекту (Cloud and AI Development Act, COM(2026) 502) [195], який запроваджує систему рівнів довіри для хмарних провайдерів державного сектору саме з метою зменшення залежності від позаєвропейських постачальників та пов’язаних із цим ризиків екстериторіального доступу до даних. Утім, предметом цього регламенту є інфраструктурний вимір проблеми, що не встановлює нових повноважень органів захисту персональних даних та перебуває поза межами цього дослідження.

Попри очевидні переваги, така модель має системні вади та лакуни у правозастосуванні, що потребують осмислення. По-перше, принцип «єдиного вікна» (One-Stop-Shop) породжує структурний конфлікт інтересів: наглядові органи країн із найбільшою концентрацією штаб-квартир технологічних компаній (передусім Ірландія) стає de facto провідним органом для більшості великих платформ, що може зумовлювати регуляторну м’якість. По-друге, тривалість складних провадження суперечить вимозі ефективного захисту та «розумним термінам». По-третє, Європейська рада із захисту даних як орган координації діє за принципом консенсусу, що уповільнює прийняття рішень.

Водночас незважаючи на ці недоліки, ЄС-модель залишається найбільш ефективною за сукупністю наведених вище критеріїв і є референтним стандартом для України.

Механізм контролю за обробкою персональних даних у Сполучених Штатах Америки проаналізовано окремо. Визначальною рисою американської

системи є відсутність єдиного федерального органу із загальною компетенцією у сфері захисту персональних даних – на відміну від ЄС-моделі. Натомість функції контролю розподілені між декількома органами залежно від сектору обробки даних. Федеральна торгова комісія (Federal Trade Commission, FTC) є де-факто основним федеральним регулятором у сфері приватності даних, хоча її мандат визначений широко: «несправедливі або оманливі дії» у торгівлі (Section 5 FTC Act). Федеральна торгова комісія є незалежним квазісудовим агентством, очолюваним п’ятьма комісарами, що призначаються Президентом за погодженням Сенату на строк 7 років – із обмеженням: не більш ніж три комісари з однієї партії одночасно.

Щодо раніше окресленого стандарту незалежності наглядового органу (Schrems I і II), а також його контекстного порівняння із системою США, важливо проаналізувати наступний судовий прецедент, сформований безпосередньо під час підготовки цього дослідження. 29 червня 2026 р. Верховний суд США в рішенні Trump v. Slaughter визнав неконституційним захист членів Федеральної торгової комісії (FTC) від звільнення президентом без причини, оскільки орган, що здійснює виконавчу владу, повинен підпорядковуватися президентському контролю [113].

Показово, що EU-US Data Privacy Framework (Рішення Європейської Комісії (ЄС) 2023/1795) неодноразово посилається на незалежність FTC як підставу висновку про «істотно еквівалентний» захист даних у США на виконання статті статті 8 Хартії основоположних прав ЄС. Автор припускає, що наслідком набутих у рішенні Верховного суду США змін процедурної незалежності наглядового органу США, Рамкова угода може бути переглянута або взагалі скасована, визнана недійсниою Судом СЄ.

Галузеві регулятори є другим ключовим суб’єктом контролю. Бюро охорони здоров’я та соціальних служб (HHS/OCR) здійснює нагляд за виконанням HIPAA у сфері медичних даних. Бюро фінансового захисту споживачів (CFPB) контролює захист фінансових даних. Федеральна комісія зі зв’язку (FCC) – телекомунікаційні дані. Це галузеве розпорошення є

системним недоліком: суб’єкт даних, права якого порушила платформа, що обробляє одночасно медичні, фінансові і поведінкові дані, не має єдиного органу для захисту.

Принципово важливою новацією, що частково усуває цей недолік, є створення Каліфорнійське агентство із захисту приватності (California Privacy Protection Agency, CPPA) у 2020 році [122]. Каліфорнійське агентство із захисту приватності розпочало регуляторну діяльність у 2023 році і є першим спеціалізованим незалежним органом захисту даних у США. Його правовий статус (незалежне агентство штату Каліфорнія з бюджетним фінансуванням і п’ятирічними строками повноважень членів) є значно ближчим до моделі наглядового органу GDPR у ЄС, ніж статус Федеральної торгової комісії.

Контрольні повноваження Федеральної торгової комісії ґрунтуються на двох засадах: (а) адміністративне провадження із прийняттям наказів про припинення і утримання від порушень (cease-and-desist orders); (б) федеральний судовий позов для отримання заборонного наказу та стягнення цивільних штрафів. Федеральна торгова комісія не має права безпосередньо накладати адміністративні штрафи за первинні порушення приватності – лише за невиконання вже прийнятих актів. Це суттєво обмежує каральну функцію органу порівняно з наглядовими органами в ЄС.

Так, штраф у розмірі $5 млрд, накладений на Facebook у 2019 році, формально є штрафом за невиконання наказу, а не за порушення законодавства про приватність як таке [123].

Каліфорнійське агентство із захисту приватності наділене більш широкими і прямими повноваженнями: право на проведення аудитів, розслідувань за скаргами тощо; видання адміністративних наказів; накладення цивільних штрафів до $7,500 за навмисне порушення і $2,500 за ненавмисне. Примітно, що Каліфорнійське агентство із захисту приватності має право вимагати проведення регуляторного аудиту від компаній, що обробляють персональні дані з високим ризиком, або щодо 100 000 або більше осіб, – що наближає її до розслідувальних повноважень.

Особливим виміром, що детально проаналізований Луценко О.Є., є механізм захисту приватності працівників: закон про недискримінацію на підставі генетичної інформації (Genetic Information Nondiscrimination Act – GINA), закони штатів про доступ до соціальних мереж, заборони вимагати паролі облікових записів. Цей напрямок є практично не розробленим в українському законодавстві, що робить американський досвід особливо цінним для формування відповідних норм трудового права [124, с. 254]. Водночас критично важливо зазначити: механізм правозастосування у сфері трудової приватності США ґрунтується переважно на судових позовах, а не на контролі спеціалізованого органу – що зумовлює нижчу ефективність порівняно з моделлю наглядового органу системи GDPR.

Американська модель поєднує високий рівень розвитку права приватності у найбільш прогресивних штатах (насамперед Каліфорнія), однак характеризується недостатнім рівнем розбудови федерального рівня регулювання. До ключових недоліків системи можна віднести відсутність уніфікованого федерального закону про захист персональних даних; відсутність єдиного федерального органу із загальною компетенцією; опціональність санкційного механізму за первинні порушення тощо.

Разом із тим, для України американська модель не може бути запозичена в цілому через три принципові відмінності правової системи: (а) Україна є унітарною державою з чіткою вертикаллю виконавчої влади, що виключає штатний федералізм як основу регулювання; (б) рівень розвитку судової системи в Україні є недостатнім для того, щоб покладатися на судовий позов як основний механізм захисту; (в) ресурсна база для підтримки множини галузевих регуляторів є обмеженою.

Водночас досвід Каліфорнійського агентства із захисту приватності як незалежного органу із прямими контрольними повноваженнями системи США та GINA-підхід [125] до захисту специфічних категорій чутливих даних мають конкретний потенціал імплементації.

Механізм контролю за обробкою персональних даних у Китайській Народній Республіці є кардинально відмінним від іноземних підходів, зазначених вище.

Система контролю за обробкою персональних даних у КНР є централізованою і ієрархічною. Головним суб'єктом контролю є Адміністрація кіберпростору Китаю (Cyberspace Administration of China, CAC), заснована 2014 року як урядовий орган, безпосередньо підпорядкований Центральній комісії з кібербезпеки та інформатизації (CCCI) – постійному органу ЦК КПК.

CAC координує діяльність галузевих регуляторів: Міністерства промисловості та інформаційних технологій (MIIT) – у сфері телекомунікацій, Державного управління ринкового регулювання (SAMR) – у сфері антимонопольного регулювання платформ, Міністерства громадської безпеки (MPS) – у правоохоронному вимірі захисту даних.

Ма А. точно характеризує цю структуру: CAC «функціонує як регулятор sui generis, що засвідчує повернення Партії на перший план», – однак для цілей юридичного аналізу важливо підкреслити: CAC є органом виконавчої влади, а не незалежним регуляторним органом у правовому значенні цього поняття.

Правовий статус CAC принципово відрізняється від DPA в ЄС за чотирма параметрами: (а) відсутність незалежності – CAC підпорядкована уряду та Партії без будь-яких законодавчих гарантій незалежності; (б) подвійна функція – CAC одночасно є органом контролю за приватними суб'єктами та інструментом державного нагляду за громадянами; (в) відсутність судового контролю – рішення CAC практично не оскаржуються в суді; (г) класифікована частина повноважень – ряд функцій CAC у сфері нагляду за «безпекою» є непублічними.

Закон Китайської Народної Республіки «Про захист персональної інформації» [126] частково імплементує концептуальні рішення GDPR, що відображає свідоме запозичення нормативних рішень. Подібно до GDPR, законодавство КНР закріплює принципи мінімізації даних і цільової

визначеності; встановлює правові підстави обробки (аналог ст. 6 GDPR); надає суб'єктам даних права доступу, виправлення і видалення; передбачає штрафи до 50 млн юанів або 5% річного обороту.

Водночас PIPL не відтворює модель незалежного регуляторного нагляду, характерну для ЄС, а покладає функції координації та контролю на Адміністрацію кіберпростору Китаю у межах адміністративної системи державного управління.

У науковій літературі зазначається подібність визначення персональних даних у PIPL та GDPR, однак не завжди проводиться критичне розмежування між нормативною подібністю текстів і фактичною відмінністю механізмів правозастосування, що має принципове значення для оцінки ефективності моделі захисту даних [127].

При цьому жодного механізму подачі скарг, аналогічного ст. 77 GDPR, і жодних процедурних гарантій для суб'єкта даних у провадженні проти великого технологічного гравця PIPL не містить.

Екстериторіальний ефект PIPL є технічно ширшим за GDPR: він поширюється на обробку даних китайських громадян за кордоном для будь-яких цілей, включно з «аналізом і оцінкою поведінки осіб на території КНР». Однак реальний механізм правозастосування екстериторіального ефекту є значно слабшим за ЄС-модель через відсутність міжнародних угод про взаємне виконання рішень і брак дипломатичного авторитету для примусового застосування поза межами КНР.

Таким чином, Китайська модель є принципово неприйнятною як зразок для запозичення Україною як демократичною правовою державою, що прагне до членства в ЄС. Причини є системними, а не випадковими.

По-перше, відсутність незалежності наглядового органу означає, що «захист» персональних даних є умовним і функціонально підпорядкованим державному нагляду за громадянами.

По-друге, подвійна природа CAC як органу захисту даних і одночасно – інструменту цифрового авторитаризму робить саму концепцію «захисту»

даних у КНР принципово відмінною від розуміння, закладеного у GDPR чи навіть у американській конституційній традиції.

По-третє, відсутність судового контролю за рішеннями регулятора унеможливлює реальний захист прав суб'єктів даних навіть у межах існуючого законодавства.

Щодо можливості запозичити практику, важливо зауважити на наступному. Першочерговим і безумовно необхідним є відтворення в Україні інституційної моделі незалежного спеціалізованого органу захисту даних – аналога наглядового органу згідно GDPR.

Р.А. Пристай переконливо доводить, що «ключовими відмінностями, які відрізняють держави, в яких існують відповідні органи, є: нижчий рівень порушень приватності; реальна можливість ефективного захисту прав» [128, с. 246]. Ці відмінності є прямим і вимірюваним наслідком наявності/відсутності ефективного наглядового органу, а не лише кореляційною залежністю.

Нормативні елементи, що підлягають імплементації: (а) закріплення гарантій незалежності наглядового органу на рівні закону (заборона інструкцій, бюджетна самостійність, строкові мандати, обмежені підстави дострокового припинення); (б) закріплення триланцюгової системи контрольних повноважень – розслідувальних, коригувальних і дорадчих; (в) введення обов'язкового розгляду скарг суб'єктів даних з правом на ефективний судовий захист проти рішень органу; (г) закріплення санкційного механізму, прив'язаного до обороту порушника; (д) інституту процедури оцінки впливу на захист даних як обов'язкового інструменту попереднього контролю ризиків; (е) норми про захист специфічних категорій чутливих даних – за моделлю GINA і каліфорнійських законів про соцмережі.

Американська модель галузевого регулювання (множина секторальних регуляторів) не є придатною для України з двох причин: (а) обмеженість інституційних ресурсів робить підтримку множини спеціалізованих органів нереалістичною; (б) горизонтальний характер GDPR, на адаптацію до якого

орієнтована Україна, вимагає єдиного органу із загальною компетенцією. Водночас секторальні повноваження (наприклад, спеціальні вимоги у сфері фінансових і медичних даних) можуть бути надані єдиному органу у вигляді спеціальних процедур, а не окремих регуляторів.

Китайська модель не підлягає запозиченню ні в цілому, ні в її інституційній частині (відсутність незалежності). Технічні норми PIPL щодо локалізації критично важливих даних можуть бути використані як орієнтир для спеціального секторального регулювання (наприклад, щодо державних інформаційних систем), але лише із збереженням принципу незалежного нагляду.

Таким чином, ефективність механізму контролю перебуває у прямій і підтвердженій правозастосовною практикою залежності від трьох факторів: інституційної незалежності наглядового органу; повноти і визначеності його контрольних повноважень; наявності пропорційного і реально здійснюваного санкційного механізму. ЄС-модель є єдиною із досліджених, де всі три фактори присутні системно.

На думку автора, для України безумовно придатна для адаптації правозахисна модель ЄС у частині: інституційних гарантій незалежності органу; триланцюгової системи контрольних повноважень; санкційного механізму; інституту процедури оцінки впливу на захист даних; механізмів транскордонної кооперації. Окремі елементи американської моделі (GINA, захист від доступу роботодавців до соцмереж) мають обмежений, але цілком конкретний потенціал імплементації у трудове законодавство. Китайська модель є неприйнятною в інституційному вимірі.

Повноваження щодо розгляду звернень згідно статті 23 Закону України «Про захист персональних даних» [10], формально відповідає ст. 77 GDPR, яка гарантує суб’єкту даних безумовне право подати скаргу до наглядового органу. Проте принципова відмінність полягає в процесуальних гарантіях: GDPR зобов’язує DPA повідомити скаржника про результат провадження «в

розумні строки», а ст. 78 надає право на ефективний судовий захист проти рішень наглядового органу.

Закон України «Про захист персональних даних» не містить аналогічних гарантій строків розгляду скарги та механізму оскарження рішення Уповноваженого в частині захисту персональних даних у стандартизованому процесуальному порядку.

Надалі пропонується аналіз попередньо окреслених моделей контролю у порівнянні з українською системою, зокрема як структуроване порівняння за окремими функціональними групами повноважень, попередньо визначеними у підрозділі 2.2 на підставі статті 23 Закону України «Про захист персональних даних».

Порівняння здійснюється, у тому числі за трьома осями: відповідність еталонному стандарту Європейського наглядового органу (ст. 58 GDPR), відмінності від американської секторально-ліберальної моделі та від державно-суверенної моделі КНР.

Найсуттєвіша структурна асиметрія між українською та еталонною моделями зосереджена у владно-розпорядчих повноваженнях. Стаття 58(2) GDPR налічує десять конкретизованих і градуйованих за тяжкістю коригувальних інструментів, тоді як п. 5 Закон України «Про захист персональних даних» у обмежується узагальненою формулою «обов’язкові вимоги (приписи)» без диференціації заходів відповідно до принципу пропорційності [10].

Принципово відрізняє українську модель від ЄС-стандарту відсутність права самостійного накладення фінансової санкції: національним законодавством передбачено лише складання протоколу та направлення до суду, що перетворює санкційний механізм із одноступеневого адміністративного акта (як у Національної комісії з питань інформатики і свобод Французької Республіки (CNIL). Порівняно з наглядовим органом КНР коригувальний потенціал Уповноваженого є суттєво слабшим: наглядовий орган КНР може накладати заходи примусового характеру безпосередньо, у

тому числі блокувати обробку і призупиняти діяльність платформ без судового рішення.

Принципова відмінність повноважень щодо розгляду звернень (п. 1 ст. 23 Закону України «Про захист персональних даних»), хоча формально відповідає ст. 77 GDPR, однак полягає в процесуальних гарантіях. Так, GDPR зобов'язує наглядовий орган повідомити скаржника про результат провадження «в розумні строки», а стаття 78 надає право на ефективний судовий захист проти рішень такого органу.

Законодавство України передбачає, що Уповноважений [78] розглядає усі звернення, що надходять до нього в порядку, передбаченому Законом України «Про звернення громадян», положеннями якого визначено, що звернення розглядаються у визначені законом строки: до одного місяця з дня їх надходження.

При цьому звернення, що не потребують додаткового опрацювання, розглядаються невідкладно, але не пізніше 15 днів. У разі необхідності строк може бути продовжено керівником відповідного органу, про що обов'язково повідомляється заявник. Загальний строк вирішення питань не може перевищувати 45 днів [77].

Вказаним нормативно-правовим актом визначено не лише терміни розгляду, але й обов'язок органу, що здійснює розгляд звернення – повідомляти особу про прийняте рішення, що умовно відповідає зобов'язанням наглядового органу GDPR [16].

Водночас Положення про порядок здійснення провадження Уповноваженого Верховної Ради України з прав людини у справах про порушення прав і свобод людини і громадянина, затвердженого наказом Уповноваженого від 10.03.2023 № 30.15/23 визначає порядок провадження Уповноваженого у разі підтвердження інформації зі звернення щодо порушення прав і свобод людини і громадянина, а також регулює питання контролю за здійсненням такого провадження у розумних строках. Відтак, вказаним Положенням передбачена фактична можливість Уповноваженого

протягом терміну, визначеного у статті 20 Законом України «Про звернення громадян», приймати рішення про відкриття провадження Уповноваженого у справі про порушення прав і свобод людини і громадянина. Надалі – провадження Уповноваженого не має конкретно визначених термінів [129].

При цьому, слід зауважити, що терміни «провадження Уповноваженого у справі про порушення прав і свобод людини і громадянина» та «перевірка володільців або розпорядників персональних даних» не є тотожними, мають різну правову природу, обсяг та зміст заходів.

Змістовний аналіз згаданих документів визначає, що перевірка володільців або розпорядників персональних даних може здійснюватися як самостійний захід парламентського контролю Уповноваженого незалежно від наявності відкритого Уповноваженим провадження у справі про порушення прав і свобод людини і громадянина.

Натомість для забезпечення розгляду скарги, яка в установленому законом порядку надходить до Уповноваженого, фактично відкриття провадження не є обов’язковим. Вказаний висновок наглядно ілюструють статистичні показники щодо співвідношення кількості скарг суб’єктів персональних даних у зв’язку із порушенням їхніх прав, а також кількість відкритих Уповноваженим проваджень, що більш детально визначено та проаналізовано у підрозділі 2.2.

Отже на практиці може виникати ситуація, за якої працівники Секретаріату Уповноваженого, що здійснюватимуть розгляд скарги щодо порушення права на доступ до персональних даних можуть вживати заходів у межах відкритого провадження, однак які за своєю суттю не вважатимуться перевіркою володільця або розпорядника персональних даних у розумінні статті 23 Закону України «Про захист персональних даних» та Порядком здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних, затвердженого наказом Уповноваженого Верховної Ради України з прав людини 08.01.2014 №1/02-14 [60].

Таким чином, порівняно із розглянутою раніше Європейською моделлю подачі та розгляду скарг, законодавство, що регулює діяльність Уповноваженого, хоча є максимально наближеним, однак не містить аналогічних гарантій строків розгляду скарги та прийняття рішення по суті.

Надалі представлена модель оцінки ефективності наглядового органу (Supervisory Effectiveness Index – SEI) для операціоналізації гіпотези про залежність ефективності контролю від структурних характеристик наглядового органу розроблено Supervisory Effectiveness Index (SEI). SEI складається з п’яти субіндексів, кожен з яких оцінюється за шкалою від 0 до 10 (додаток Б).

3.2. Технології штучного інтелекту як новий виклик для контролю за обробкою персональних даних

Штучний інтелект у політиці сучасних держав перестав бути об’єктом вузькоспеціалізованого регулювання і перетворився на наскрізний вимір усієї цифрової архітектури – від обчислювальної інфраструктури до кібербезпеки.

Стрімке поширення технологій штучного інтелекту у різних сферах суспільного життя – охорони здоров’я, фінансового сектору, публічного управління та правоохоронної діяльності. Вказане створює якісно нові випробування для системи контролю за обробкою персональних даних, що історично формувалася навколо інших технологічних реалій.

Проблематика захисту персональних даних у контексті штучного інтелекту привертає дедалі більшу увагу правознавців. Серед вітчизняних дослідників питання штучного інтелекту та його співвідношення з інформаційним законодавством, у тому числі під час обробки персональних даних, досліджували В. М. Фурашев, С. О. Дорогих, Ю. В. Деркаченко, Б. Д. Леонов, Д. В. Швець, Л. В. Куцак., А. О. Гачкевич, Н. А. Загребельна, І.М. Берназюк.

Окремим напрямком у науковій літературі є впровадження штучного інтелекту у діяльність вже усталених процесів функціонування державних органів. К.А Машненков та Ю.В Деркаченко розглядають цифровізацію публічного адміністрування, включно із застосуванням технологій штучного інтелекту, як дієвий інструмент превентивного управління соціальними конфліктами та зміцнення економічної стійкості [130]. О.М. Гумін та А.О. Гачкевич, досліджуючи питання застосування сучасних технологій для модернізації системи кримінальної юстиції приходять до висновку, що такий технологічний прогрес здатний значним чином розширити можливості правоохоронних органів [131]. Натомість І.В. Басиста, Ж.В. Удовенко та М.А Кулинич наголошують, що системи штучного інтелекту у правничій та правоохоронній сферах вважаються «підвищеними ризиками» [132, с. 33].

Б.Д. Леонов, розглядаючи питання впровадження технологій штучного інтелекту під час здійснення парламентського контролю, також приходить до висновку, що запровадження таких інновацій може не лише посилити існуючі процедури, але й забезпечить можливість реагувати на сучасні виклики та покращити якість державного управління [133, с. 57].

Водночас наявні дослідження залишаються переважно фрагментарними щодо центрального для цієї дисертації питання – як саме технології штучного інтелекту трансформують механізм контролю за обробкою персональних даних та які зміни потребує українська наглядова модель для забезпечення своєї ефективності. Недослідженим залишається питання контролю за обробкою персональних даних системами штучного інтелекту як єдиного об’єкту, що потребує одночасного оновлення нормативного інструментарію, технічної спроможності наглядового органу та методології нагляду саме в українських правових умовах з урахуванням європейських стандартів.

Відтак традиційний індивідуалізований підхід до перевірки правових підстав обробки (таких як перевірка наявності згоди та її оцінки) стосовно кожного конкретного суб’єкта даних – стає технічно нездійсненним за такого масштабу, що ставить перед наглядовими органами завдання розробки нових,

агрегованих методологій оцінки законності обробки даних на популяційному, а не індивідуальному рівні.

Узагальнюючи, технології штучного інтелекту трансформують не окремі параметри обробки, а саму природу об’єкта контролю. Якщо в класичній моделі наглядовий орган перевіряв правомірність дискретних операцій, то в середовищі штучного інтелекту він має оцінювати правомірність динамічної архітектури, яка безперервно змінюється внаслідок самонавчання.

Водночас навіть формально бездоганний нормативний документ не здатний забезпечити реальний контроль, якщо національний наглядовий орган не має технічної спроможності для незалежного тестування моделі, аудиту навчальних даних чи проведення оцінки відповідності. Відтак ефективність контролю за системами штучного інтелекту дедалі більше залежить не лише від якості нормативного тексту, а від матеріальної здатності держав та наглядових органів, а також можливостей володільців персональних даних ці положення реалізувати.

Нормативна база ЄС у сфері штучного інтелекту є фрагментованою – її формують не один десяток частково перехресних актів, систему яких буде детально проаналізовано надалі. Так, архітектура нормативно-правових актів включає обов’язкові інструменти, на яких тримається вся конструкція. Такими документами є GDPR [16], Акт ЄС про штучний інтелект, модернізована Конвенція 108+ та Конвенція про штучний інтелект [147]. Вказана ланка фактично включає документи, які функціонують щодо м’якого правового корпусу як зовнішній твердий каркас.

Над рівнем обов’язкових актів розташовується рівень міжнародних квазістандартів – принципові набори міжнародних конференцій органів захисту даних та стандарти міжнародних організацій зі стандартизації, на які орієнтуються регулятори.

Нижче розташовується рівень міжурядового м’якого права – резолюції Генеральної Асамблеї ООН та заяви органів захисту даних провідних демократій. Ще нижче – рівень політичних декларацій держав та об’єднань.

Реконструкція генези цієї архітектури дозволяє виявити її внутрішню логіку, що полягає в послідовному розширенні об’єкта контролю: від окремих персональних даних – до бази даних, далі до алгоритму, потім до автоматизованого рішення, моделі, системи штучного інтелекту, її життєвого циклу і, нарешті, до екосистеми та ланцюга постачання моделей.

Кожен етап відповідає черговому розширенню об’єкта, а нормативні концепції, що з’являються на кожному етапі, є реакцією на нездатність попередніх конструкцій охопити новий, ширший об’єкт. Формування цієї архітектури стало одним із етапів формування сучасної парадигми відповідального штучного інтелекту, інтелектуальне підґрунтя якої закладалося ще наприкінці 2010-х років, у тому числі зокрема ініціативою Інституту інженерів електротехніки й електроніки «Ethically Aligned Design» 2016 року [134] та Монреальською декларацією відповідального розвитку штучного інтелекту 2017 року [135], що артикулювали засади людиноцентричності, прозорості й підзвітності задовго до їх кодифікації в міжурядових інструментах. Водночас положення цих актів мали переважно академічно-дорадчий характер і не дістали інституційного оформлення.

Важливим кроком стали документи Ради Європи щодо великих даних, ухвалені у 2017–2019 роках, які встановили зв’язок між режимом Конвенції 108+ і практиками масової обробки даних.

Зокрема, Декларація про етику та захист даних у штучному інтелекті стала одним із перших міжнародних документів, який поєднав традиційні принципи захисту персональних даних із ширшим етичним виміром регулювання штучного інтелекту, стала одним із етапів формування сучасної парадигми: вона концептуально розширила принцип *privacy by design* і перенесла фокус зі шкоди індивідові на колективну шкоду від алгоритмічних систем [136].

Декларація 2018 року не залишилася ізольованим актом саме тому, що вона заснувала постійну робочу групу з питань етики та захисту даних у штучному інтелекті [137]. Ця інституційна новела виявилася вирішальною для подальшої генези: робоча група перетворилася на постійне джерело нормотворення, що забезпечило безперервність та кумулятивність розвитку.

Рекомендація Організації економічного співробітництва та розвитку щодо штучного інтелекту, ухвалена у 2019 році та суттєво оновлена у 2024 році, є першим міжурядовим документом, що визначив узагальнені принципи людиноцентричного штучного інтелекту для держав-членів OECD та партнерів.

Документ закріплює п’ять принципів: інклюзивний ріст і сталий розвиток; ціннісно-орієнтоване ставлення до прав людини; прозорість і підзвітність; надійність і безпека; пояснюваність [138]. Рекомендація OECD справила вирішальний вплив на подальше нормотворення у сфері штучного інтелекту, ставши основою для документів G7 з питань штучного інтелекту та структурно відобразившись у тексті відповідних резолюцій Генеральної Асамблеї ООН. Прикметно, що ці принципи були прямо інкорпоровані в українську Концепцію розвитку штучного інтелекту [139], основні засади якої, як зазначають дослідники, відповідають саме Принципам Організації економічного співробітництва та розвитку [140, с. 14].

Поряд із Рекомендаціями OECD, Етичні настанови щодо надійного штучного інтелекту, підготовлені Незалежною експертною групою високого рівня з питань штучного інтелекту, створеною Європейською Комісією у 2019 році, сформували базові принципи сучасної моделі AI Governance, закріпивши орієнтацію на людиноцентричність, прозорість, людський контроль та підзвітність [141].

Натомість Рекомендація ООН з питань освіти, науки і культури щодо етики штучного інтелекту, ухвалена у листопаді 2021 року, є першим глобальним формуючим стандарти інструментом у сфері етики штучного інтелекту, схваленим усіма державами-членами організації [142]. Як держава-

член UNESCO, Україна взяла на себе політичне зобов'язання керуватись цими принципами.

Хоча за своїм статусом Рекомендація належить до м'якого права: вона не породжує юридично обов'язкових зобов'язань, проте її універсальне ухвалення надає їй виняткової легітимаційної ваги як глобального еталона належної поведінки. Значення документа полягає в тому, що він закріпив на універсальному рівні цінності, які до того формулювалися переважно в експертних інструментах.

Вона закріплює десять принципів, серед яких для теми захисту персональних даних особливе значення мають: принцип пропорційності та ненанесення шкоди (вимога забезпечення безпеки та конфіденційності даних); принцип захисту конфіденційності та даних (вимога системного захисту особистих даних протягом усього життєвого циклу штучного інтелекту); принцип нагляду і підзвітності (вимога можливості ефективного нагляду, включаючи мінімальний рівень управління людини, особливо для систем, що впливають на права людини); принцип прозорості та пояснюваності.

В контексті забезпечення контролю за обробкою персональних даних, ключовими є чотири засадничі принципи. Наприклад, *принцип прозорості та пояснюваності* вимагає, щоб особи, на яких впливають системи штучного інтелекту, могли отримувати своєчасну та зрозумілу інформацію про використання їхньої особистої інформації, – позиція, яку Спеціальна доповідачка ООН з права на приватність прямо назвала ключовою структурною частиною кожної національної правової системи [143]. *Принцип підзвітності* покладає відповідальність за роботу та наслідки систем штучного інтелекту на людських акторів, виключаючи можливість перекладення відповідальності на «автономну» технологію. *Принцип людського контролю (нагляду)* вимагає збереження за людиною спроможності втручатися у функціонування системи. *Принцип захисту приватності* закріплює право на захист персональних даних як засадниче для всього життєвого циклу системи штучного інтелекту.

Заява раунд-столу органів захисту даних G7 про генеративний штучний інтелект, ухвалена в червні 2023 року та згадана у подальших інструментах корпусу, першою серед авторитетних регуляторних структур привернула увагу до специфічних ризиків генеративних систем для приватності та підтвердила, що чинне право захисту даних застосовується до розробки й використання генеративних продуктів навіть за відсутності спеціального законодавства [144].

Рада Європи зробила принципово важливі за юридичною силою внески в архітектуру контролю за обробкою персональних даних із використанням штучного інтелекту. Рекомендація Комітету Міністрів CM/Rec(2020)1 державам-членам щодо впливу алгоритмічних систем на права людини, ухвалена 8 квітня 2020 року [145]. Хоча Рекомендація Комітету Міністрів CM/Rec(2020)1 належить до м’якого права, однак за своєю суттю має істотне доктринальне значення як документ, що системно поставив питання впливу алгоритмічних систем не лише на окремого суб’єкта, а й на права людини загалом, та сформулював вимоги до держав щодо забезпечення прозорості, підзвітності й засобів правового захисту в контексті автоматизованого оброблення даних. Рекомендація заклала концептуальну основу для подальшого переходу від індивідуалістичної моделі захисту персональних даних до сприйняття персональних даних як категорії, що має водночас приватний і суспільний вимір.

Визначним актом ЄС став Регламент (ЄС) 2024/1689 Європейського Парламенту і Ради від 13.06.2024 р., що встановлює гармонізовані правила щодо штучного інтелекту, який визначив фундаментальні правила функціонування внутрішнього цифрового простору ЄС (далі – Акт про штучний інтелект), ухвалений 13 червня 2024 року запровадив ризик-орієнтовану модель регулювання, що диференціює застосування систем штучного інтелекту за рівнями ризику: неприйнятний ризик (заборонений рівень – маніпуляції поведінкою, соціальний скоринг), високий ризик

(системи, що підлягають суворим вимогам відповідності та нагляду), обмежений ризик (вимоги прозорості) та мінімальний ризик.

Акт виокремлює неприйнятний рівень ризику для практик, що суттєво впливають на людську поведінку, підривають автономію особи або використовують маніпулятивні методи, та встановлює щодо них заборону [146, с. 339–340]. Серед заборонених практик – нецільове збирання зображень облич з інтернету або записів відеоспостереження для створення баз розпізнавання, розпізнавання емоцій на робочому місці та в навчальних закладах (за винятком медичних і безпекових підстав), а також біометрична категоризація за чутливими ознаками [163, с. 129].

Найбільш вагомим за юридичним статусом документом є Рамкова конвенція Ради Європи про штучний інтелект та права людини, демократію і верховенство права (CETS No. 225) [147], відкрита для підписання у Вільнюсі 5 вересня 2024 року. Співвідносячи положення Конвенції про ШІ та Регламенту ЄС слід наголосити, що в цьому питанні визначальним є аспект юридичної обов’язковості, оскільки регламенти ЄС мають пряму дію у правопорядках держав-членів у той час, як Конвенція потребує ратифікації та імплементації [148, с. 24].

Таким чином, на відміну від раніше згаданих інструментів, Конвенція про штучний інтелект є революційним документом – першим юридично обов’язковим міжнародним договором у сфері регулювання штучного інтелекту. Її значення для предмета цього дослідження посилюється тим, що Україна приєдналася до Конвенції про штучний інтелект, зобов’язавшись дотримуватися закріплених у ній принципів при формуванні законодавства та використанні штучного інтелекту в публічному секторі.

Особливе значення для системи контролю за обробкою персональних даних має положення статті 11, відповідно до якого держави повинні забезпечити захист приватності та персональних даних протягом усього життєвого циклу систем штучного інтелекту. Крім того, положення статей 8, 9 та 16 формують основу ризик-орієнтованої моделі контролю, що передбачає

прозорість, документування, оцінювання впливу та моніторинг потенційних негативних наслідків використання штучного інтелекту.

Поміж іншого, Конвенція про штучний інтелект встановлює механізм подальшого контролю – Конференцію Сторін, що складається з офіційних представників Сторін Конвенції про штучний інтелект, для визначення ступеня виконання її положень. Їхні висновки та рекомендації допомагають забезпечити дотримання державами Конвенції про штучний інтелект та гарантувати її довгострокову ефективність. Конференція Сторін також сприяє співпраці з відповідними зацікавленими сторонами, зокрема шляхом проведення публічних слухань щодо відповідних аспектів виконання Конвенції про штучний інтелект.

Зокрема, у розділі VII «Механізм подальших дій та співпраця» Рамкової конвенції Ради Європи про штучний інтелект, права людини, демократію та верховенство права визначено процедурні аспекти створення національних наглядових механізмів. Так, стаття 26 Конвенції передбачає обов’язок держав створити або визначити ефективні механізми нагляду за дотриманням встановлених вимог, які повинні діяти незалежно та неупереджено і мати достатні повноваження, експертні можливості та ресурси для здійснення контролю [148]. Такий підхід відповідає сучасній тенденції розвитку моделі врядування у сфері штучного інтелекту, де незалежні регуляторні органи виступають гарантами дотримання прав людини та законності обробки персональних даних у процесі використання систем штучного інтелекту.

Заява Європейської ради із захисту даних (3/2024), присвячена ролі органів захисту даних у межах інституційної структури, що запроваджується Актом про штучний інтелект [149], обстоює доцільність призначення органів захисту даних наглядовими органами щодо систем штучного інтелекту високого ризику, які стосуються захисту персональних даних, зокрема систем біометричної ідентифікації, правоохоронної діяльності, міграційного контролю та здійснення правосуддя. Для решти високоризикових систем,

пов’язаних з обробкою персональних даних, Європейська рада із захисту даних лише рекомендує таке призначення.

У межах права ЄС ключове значення має стаття 10 Акта про штучний інтелект ЄС, що встановлює вимоги до системи управління даними для високоризикових систем: якість, релевантність, репрезентативність навчальних, валідаційних і тестових наборів даних, а також перевірку на наявність упереджень, здатних вплинути на права осіб.

Аргумент на користь такого розподілу компетенції полягає в тому, що органи захисту даних уже мають незалежність, експертизу й досвід оцінки впливу на основоположні права, тоді як зосередження нагляду дозволяє уникнути фрагментації правозастосування між органом захисту даних, Офісом ЄС зі штучного інтелекту (компетентним щодо моделей загального призначення) та секторальними регуляторами.

Координація правозастосування забезпечується також спеціальними механізмами Європейської ради із захисту даних. Показовим є створення під егідою Ради спеціальної робочої групи з питань ChatGPT, що опублікувала у травні 2024 року звіт, який запровадив більш-менш однаковий підхід до нагляду та сформулював три правила правомірності обробки: визначення правової підстави на всіх етапах функціонування системи (стаття 6), неможливість звільнення контролера від зобов’язань Регламенту через застереження про невідповідальність за безпеку даних (стаття 51) та диференціацію обов’язку інформування залежно від способу збору даних – через вебскрейпінг чи в процесі взаємодії з системою. Ці механізми демонструють, що ефективний контроль за транснаціональними розробниками систем штучного інтелекту неможливий силами окремого національного органу та потребує координації.

Коло повноважень та особливості діяльності наглядових органів детально було проаналізовано у підрозділі 2.2. дисертації. Практична операціоналізація цих повноважень щодо генеративної системи штучного інтелекту найповніше виявилася в кейсі «Garante Італії проти OpenAI».

Італійський наглядовий орган із захисту персональних даних (Garante per la Protezione dei Dati Personali) у межах розслідування щодо OpenAI застосував комплекс коригувальних заходів, включаючи тимчасове обмеження обробки персональних даних та вимоги щодо забезпечення прозорості, реалізації прав суб'єктів даних і впровадження механізмів перевірки віку. У подальшому орган ухвалив рішення про накладення адміністративного штрафу у розмірі 15 млн євро за порушення положень GDPR, пов'язаних із відсутністю належної правової підстави для обробки даних при навчанні моделі та порушенням принципу прозорості, а також зобов'язав компанію провести інформаційну кампанію [150]. У подальшому, це рішення стало предметом судового перегляду.

Звіт Digital Decade засвідчує саме ці матеріальні передумови: національні наглядові органи (на момент звіту призначені лише в 10 державах-членах) потребують технічної, фінансової та кадрової бази.

Відтак реконструкція ґенези виявляє приховану закономірність: міжнародне регулювання розвивалося двома паралельними треками, що походять із різних епістемічних спільнот і послуговуються різними нормативними мовами. Перший трек – регуляторний – представлений спільнотою органів захисту даних, що оперують мовою приватності та основоположних прав і виробляють найдетальніші щодо персональних даних принципи. Другий трек – політичний – постав із саммітової дипломатії держав і оперує мовою «безпеки», «стійкості» та «надійності», запозиченою з інженерії безпеки та сфери національної безпеки.

Регуляторний трек є найдетальнішим щодо персональних даних, але найслабшим за політичною вагою; політичний трек є найвагомішим за легітимністю, але найзагальнішим за змістом. Інструментом їхнього зближення стала спільна формула «безпечний, надійний і довірений штучний інтелект» (safe, secure and trustworthy AI), що повторюється в актах обох треків. Проте важливо наголосити, що це зближення є риторичним, а не

інституційним: треки не злилися в єдину структуру, а лише виробили спільний словник, який маскує глибинне напруження між мовою прав і мовою безпеки.

Із наведеного випливає висновок, що має далекосяжні теоретичні наслідки для оцінки ефективності контролю. Міжнародний режим контролю за обробкою персональних даних у штучному інтелекті у його теперішньому вигляді є режимом, що сформований у м'якому праві та знаходить свою реалізацію GDPR, Акту про штучний інтелект, Конвенції 108+ та Конвенції про штучний інтелект.

Резолюція Глобальної асамблеї з питань приватності [151] лише розгорнула та деталізувала цю тезу, перетворивши її з твердження на систему принципів. Теза технологічної неперервності має й глибший наслідок: вона визначила саме органи захисту даних як первинних регуляторів штучного інтелекту, обґрунтувавши це тим, що персональні дані вже перебувають у сфері їхньої компетенції, а штучний інтелект є передусім технологією обробки персональних даних.

Другий трек, політичний, постав майже одночасно. Блетчлійська декларація [152], ухвалена на саміті з безпеки штучного інтелекту у листопаді 2023 року, перенесла регістр обговорення з персональних даних на системний і навіть катастрофічний ризик «межових» моделей загального призначення.

Принципово, що Блетчлійська декларація послуговується словником «безпеки» (safety), «стійкості» (robustness) та «надійності» (security), запозиченим не з інформаційного права, а сфери національної безпеки. Тут вперше у корпусі проявляється напруження між двома нормативними генеалогіями: правозахисною, що походить від традиції захисту даних, і безпековою, що походить від технічної та державної безпеки.

Політичний трек, започаткований у Блетчлі, розвивався за власною логікою послідовних самітів. Блетчлійський саміт започаткував тенденції, подовжені Сеульським самітом та Паризьким самітом. Відтак зміщувалися акценти від виключно безпекової проблематики до ширшого порядку денного, включаючи інклюзивність.

Паралельно розгортався універсальний трек ООН, інституційним джерелом якого став Пакт заради майбутнього та його додаток – Глобальний цифровий договір. Саме рішення, ухвалені в межах цього Пакту, передбачили створення Незалежної міжнародної наукової панелі та започаткування Глобального діалогу, що згодом були операціоналізовані окремою резолюцією.

Прикметно, що навіть державоцентричний План глобального управління штучним інтелектом Китайської Народної Республіки та Паризька заява апелюють до Глобального цифрового договору та до ООН як до каналу глобального управління, що засвідчує консолідуючу роль універсального треку навіть для акторів, які в інших аспектах розходяться між собою.

Таким чином, два паралельні треки поступово визнали інституційну архітектуру ООН як спільну точку відсилання. Зокрема, Резолюція Генеральної Асамблеї ООН 78/265 [153] перенесла проблематику на універсальний міжурядовий рівень і здійснила вирішальний кодифікаційний крок: вона визначила життєвий цикл системи штучного інтелекту як послідовність стадій від попереднього проєктування через розробку, оцінювання, тестування, розгортання, використання, продаж і експлуатацію до виведення з експлуатації, та вимагала забезпечення прав людини впродовж усього цього циклу.

Резолюція Генеральної Асамблеї ООН 78/311 [154] додала розвитковий вимір, наголосивши на потребі подолання цифрового розриву та забезпечення рівних можливостей держав у сфері штучного інтелекту.

Того ж року Заява «Statement on the Role of Data Protection Authorities in Fostering Trustworthy AI», ухвалена під час 4-го раунд-столу органів захисту даних держав G7 [155] стала одним із перших міжнародних документів, що комплексно окреслив інституційну роль органів захисту даних у забезпеченні надійного штучного інтелекту, проголосивши, що вони виходять із пріоритетності захисту фундаментальних прав людини, приватності та мають людиноцентричний підхід за замовчуванням. Задекларовано, що оскільки

значна частина сучасних систем штучного інтелекту функціонує шляхом обробки персональних даних, органи захисту даних здійснюють нагляд за одним із ключових компонентів їх функціонування як на стадії розробки технології, так і на стадії її розгортання, тобто «у джерелі проблеми», а їхня незалежність є передумовою неупередженого управління.

Ця Заява артикулює модель інституційної взаємодії, за якої орган захисту даних виступає сполучною ланкою між режимом захисту персональних даних та режимом регулювання штучного інтелекту. Документ не наділяє органи захисту даних статусом універсального регулятора штучного інтелекту, а визначає їх як спеціалізованих суб'єктів контролю в тих випадках, коли функціонування систем штучного інтелекту пов'язане з обробкою персональних даних.

Завершальний етап 2025 року позначений двома взаємопов'язаними процесами: інституціоналізацією політичного треку та кульмінацією контролю за персональними даними в регуляторному треку.

Інституціоналізація відбулася через резолюцію Генеральної Асамблеї ООН A/RES/79/325 [156], якою створено Незалежну міжнародну наукову панель з питань штучного інтелекту у складі сорока членів та започатковано Глобальний діалог щодо управління штучним інтелектом, сформувавши постійний міжнародний консультативний механізм у системі ООН.

Завершальний етап формування нормативної бази настав через Резолюцію про збирання, використання та розкриття персональних даних для попереднього навчання, навчання та доналаштування моделей [157], яка перенесла нормативний контроль безпосередньо на стадію формування моделі та сформулювала вісім принципів обробки навчальних даних.

У подальшому, Резолюція про змістовний людський нагляд за рішеннями, що приймаються із використанням систем штучного інтелекту (*Resolution on meaningful human oversight of decisions involving AI systems*) [158] визначила критерії ефективного людського нагляду, наголосивши, що участь людини має бути реальною, своєчасною та здатною впливати на результат

автоматизованого прийняття рішень, а Спільна заява про довірене управління даними [159] спробувала примирити потребу в інноваціях із захистом прав через концепцію довірених рамок управління даними.

Таким чином, Резолюції Генеральної Асамблеї ООН 78/265 та 78/311 закріпили глобальний консенсус щодо того, що штучний інтелект має бути безпечним, надійним і довіреним та слугувати сталому розвитку, тоді як Резолюція Генеральної Асамблеї ООН A/RES/79/325 заклала інституційну інфраструктуру управління штучним інтелектом. Вказана резолюція надала регулюванню штучного інтелекту найбільшого рівня універсальної легітимності, оскільки лише ООН об'єднує майже всі держави світу. Водночас саме ця універсальність зумовлює головні обмеження діяльності ООН, що полягають у необхідності досягнення консенсусу між державами з різними політичними, економічними та правовими підходами. Вказане спричиняє ухвалення документів, які переважно формулюють загальні принципи та орієнтири, залишаючи питання їх практичної конкретизації на рівні інших міжнародних і національних механізмів.

Таким чином, модель ЄС є найбільш зрілою та найбільш правозахисною. Її головною метою є захист основоположних прав, закріплених у Хартії основоположних прав Європейського Союзу, зокрема права на повагу до приватного життя та права на захист персональних даних. Персональні дані в цій моделі розглядаються як предмет основоположного права, а не як економічний ресурс.

Китайська модель, представлена в корпусі Планом глобального управління штучним інтелектом [160], є державоцентричною. Її головною метою є державний суверенітет, контрольованість штучного інтелекту та розвиток, підпорядкований концепції «штучного інтелекту для блага», а персональні дані розглядаються переважно як елемент безпеки даних та державно керованих потоків. План наголошує на захисті персональної інформації та безпеці даних, але вписує їх у рамку вільного потоку даних та державного управління. Ставлення до інновацій є пріоритетним, але інновації

здійснюються під державною координацією. Підхід до ризиків є категоризованим і безпекоцентричним, з акцентом на системах простежуваності та запобіганні зловживанням. Механізми відповідальності орієнтовані передусім на державу та політичні цілі, а не на захист індивідуальних прав.

Прикметно, що китайська модель апелює до ООН як до головного каналу глобального управління та до Глобального цифрового договору. Подвійність китайської моделі заслуговує на окреме теоретичне осмислення, оскільки вона руйнує спрощене протиставлення національного суверенізму та глобального мультилатералізму.

Апелюючи до ООН як до головного каналу та наголошуючи на потребах Глобального Півдня, китайська модель прагне закріпити в універсальних інструментах ті засади – повагу до суверенітету, розвитковий пріоритет, неупередженість до внутрішніх регуляторних виборів держав, – що відповідають її власному підходу.

Модель групи провідних демократій, представлена Заявою про роль органів захисту даних [161], орієнтована на довіру та інтероперабельність серед однодумців. Її головною метою є забезпечення вільного потоку даних із довірою та координація правозастосування. Таким чином, принципова відмінність між моделями полягає у модальності контролю. ЄС покладає контроль на незалежний наглядовий орган, в той час як КНР – на державу, Глобальна асамблея з питань приватності та група провідних демократій – на мережу регуляторів, а ООН – на міжурядовий консенсус.

Врядування у сфері штучного інтелекту (так зване «AI Governance») функціонує не як автономний регуляторний трек, а як інтегрований елемент політики технологічного суверенітету. Традиційна модель контролю за обробкою персональних даних, що відображена у Законі України «Про захист персональних даних» та відтворює підходи Конвенції 108+, побудована навколо дискретних операцій з ідентифікованими даними: збирання

конкретних відомостей про особу для визначеної мети, за наявності правової підстави, із забезпеченням доступу суб'єкта до власних даних.

Однак класичні механізми нагляду, що використовуються для перевірки дискретних операцій з персональними даними (збирання, зберігання, передача конкретному отримувачу), виявляються недостатньо адаптованими до середовища, в якому обробка персональних даних є безперервним, динамічним і непрозорим процесом, вбудованим у логіку самонавчання алгоритмічних систем.

Принциповою особливістю обробки персональних даних системами штучного інтелекту є її двоетапність: дані використовуються як на етапі навчання моделі (тренувальні дані), так і на етапі її подальшого функціонування (операційні дані, що надходять від користувачів у режимі реального часу). На кожному з цих етапів виникають специфічні правові ризики. О. Посикалюк слушно виокремлює щонайменше три життєві цикли моделі: збір значних масивів даних як навчальних; власне навчання моделі з утворенням сконфігурованої моделі; застосування моделі до конкретних випадків або осіб [162, с. 127]. Кожен із згаданих циклів (етапів) породжує самостійні ризики для захисту персональних даних, причому ризики етапу навчання якісно відрізняються від ризиків етапу експлуатації. Водночас як зазначає автор, ефективність моделі перебуває у нелінійній залежності від обсягу даних, які обробляються. Отже, за таким принципом, чим більший масив персональних даних обробляє модель, тим вищою стає її якість [163]. Відтак проблема пропорційності масштабу обробки постає дедалі гостріше.

На стадії навчання системи загального призначення та великі мовні моделі обробляють масиви даних, що вимірюються мільярдами одиниць інформації, зібраних із загальнодоступних джерел. На стадії функціонування модель здатна генерувати, реконструювати та виводити дані про осіб, яких не ідентифікував жоден оператор свідомо.

Викладене зумовлює низку фундаментальних ризиків для контролю за обробкою персональних даних, кожна з яких має пряму прив'язку до конкретних положень GDPR як еталонного європейського стандарту.

Перший ризик обумовлений неможливістю застосування індивідуалізованої перевірки правових підстав обробки. Стаття 6 Загального регламенту вимагає, щоб будь-яка обробка персональних даних ґрунтувалася на одній із шести правових підстав. Традиційний індивідуалізований підхід – оцінка згоди, законного інтересу чи виконання договору стосовно кожного конкретного суб'єкта даних – стає технічно нездійсненним за масштабу обробки, властивого моделям загального призначення.

Аналогічні вимоги передбачає стаття 11 Закону України «Про захист персональних даних». За умов масового використання даних у навчальних корпусах мовних моделей такий підхід є технічно нездійсненним: ані контролюючий орган, ані оператор не можуть ідентифікувати кожного суб'єкта, чиї дані потрапили до навчального масиву.

Це вимагає розробки агрегованих методологій оцінки законності обробки на системному рівні, а не індивідуальному. Вказане також ставить перед наглядовими органами завдання розробки нових, агрегованих методологій оцінки законності обробки на популяційному, а не на індивідуальному рівні. Практика наглядових органів дедалі частіше визнає законний інтерес (стаття 6(1)(f)) допустимою підставою для навчання моделей за умови проходження трискладової перевірки, що охоплює визначення законного інтересу, тест на необхідність та тест на балансування [163, с. 131].

Другим ризиком є порушення принципу обмеження мети обробки. Стаття 6 Закону України «Про захист персональних даних» і стаття 5 GDPR вимагають, щоб мета обробки була визначена заздалегідь і дані не використовувалися повторно в несумісний спосіб. Системи штучного інтелекту за своєю природою є системами вторинного використання даних: дані, зібрані для однієї мети, стають навчальним матеріалом, що визначає поведінку системи в принципово відмінних контекстах. Ризик «вторинного

використання» зумовлений особливістю функціонування технологій штучного інтелекту, а отже є системним, а не ситуативним.

Третій ризик пов’язаний із непрозорістю алгоритмічних рішень і труднощі реалізації прав суб’єктів. Право на доступ до власних персональних даних (стаття 8 Закону України «Про захист персональних даних», стаття 15 GDPR), право на виправлення (стаття 16 GDPR) і право на заперечення проти автоматизованого рішення (стаття 22 GDPR) базуються на припущенні, що оператор здатен надати суб’єкту конкретну ідентифіковану інформацію про нього. У контексті великих мовних моделей і систем профілювання ця передумова може бути відсутньою: «знання» системи про особу дифузно розподілені серед параметрів моделі і не можуть бути ізольовані та пред’явлені. Багато сучасних моделей, особливо побудованих на глибоких нейронних мережах, функціонують як «чорні скриньки»: навіть їхнім розробникам складно або неможливо точно пояснити, чому модель ухвалила те чи інше рішення [163, с. 125].

Підрозділ 3.1 дисертації констатує, що стандарти ЄСПЛ щодо оцінки законності масового автоматизованого оброблення – зокрема висновок у справі Big Brother Watch and Others v. United Kingdom (2021) про те, що ризик масового збирання даних залежить не лише від подальшого використання даних, а й від самої архітектури системи [98].

Четвертий ризик – неможливість повноцінного застосування принципу мінімізації даних. Стаття 5(1)(c) GDPR і відповідні положення національного законодавства вимагають, щоб збір даних обмежувався необхідним мінімумом. Ефективне навчання сучасних моделей потребує масивних наборів різноманітних даних – що концептуально суперечить мінімізації. Принцип «захисту даних вже на стадії проєктування та за замовчуванням» (*privacy by design* and by default, стаття 25 GDPR) потребує переосмислення застосовно до систем, для яких «мінімальна» кількість даних є питанням технічної архітектури, а не організаційного вибору.

П’ятим є ризик реалізації права доступу. Так, стаття 15 GDPR закріплює право суб’єкта даних на доступ до інформації про обробку його даних, зміст якого деталізовано в Настановах Європейської ради із захисту даних 01/2022 [164]. У середовищі штучного інтелекту реалізація цього права наражається на технічну перешкоду: суб’єкт даних здебільшого не може отримати повних пояснень про те, яка саме інформація про нього та в який спосіб використовується системою, що позначається в доктрині як ситуація «сірої зони» [163, с. 123].

Ще один, шостий ризик, що стосується права на видалення даних, зумовлений чи не найскладнішою технічною перешкодою. Надання персональних даних системі штучного інтелекту та її інкорпорація в параметри навченої моделі, у подальшому унеможливлює її видалення, що ставить під сумнів реалізацію права на стирання та права на виправлення.

Для прикладу, навіть якщо дані в первісному наборі будуть виправленими, це не змінить кінцевого результату, що добре помітно в контексті генерування контенту [163, с. 133].

Так, Посикалюк О. наводить як приклад застереження політики приватності одного з провідних розробників про те, що «з огляду на технічну складність роботи моделей, виправлення неточності в кожному випадку може бути неможливим». [162, с. 133].

Окремої уваги слід надати сьомому ризику, який стосується деанонімізації та виведення чутливої інформації про особу з нечутливих вихідних даних. Зокрема, ризик алгоритмічної обробки виявляє і специфічний вимір, не охоплений традиційними стандартами захисту даних. Системи штучного інтелекту суттєво підвищують ризик повторної ідентифікації осіб у наборах даних, що вважалися анонімними, оскільки алгоритми виявляють складні кореляції, які дозволяють поєднувати знеособлені дані із загальнодоступними джерелами [164]. Таким чином, профілювання на основі великих масивів даних дозволяє з достатнім ступенем точності встановлювати расову або етнічну приналежність, релігійні чи політичні погляди, стан

здоров’я або сексуальну орієнтацію особи – без доступу до відповідних прямих категорій чутливих даних. Це актуалізує вимоги статей 25 (захист даних за задумом та за замовчуванням) і 35 (оцінка впливу на захист даних) Загального регламенту, оскільки лише вбудовування технічних запобіжників на стадії проєктування та попередня оцінка ризиків здатні мінімізувати ймовірність вивідного профілювання. Спираючись на практику ЄСПЛ щодо оцінки такого «вивідного профілювання» важливо проаналізувати принцип ефективності захисту (effective protection), який вимагає, щоб гарантії захисту поширювалися на весь комплекс ризиків, пов’язаних з обробкою, – в тому числі на ризики ідентифікації чутливих атрибутів через непряму обробку.

Принципово, що це не новий за юридичною природою, а технологічно новий за формою прояв ризику. Ще у справі Rotaru v. Romania (2000) [94], проаналізованій у підрозділі 3.1 цієї дисертації, ЄСПЛ встановив, що навіть публічна або на перший погляд нейтральна інформація підпадає під захист статті 8 Конвенції про захист прав людини і основоположних свобод [19], якщо вона систематично збирається і зіставляється органами влади: втручання породжує саме систематичне зіставлення окремих, самих по собі невинних відомостей, а не їхня індивідуальна чутливість. Вивідне профілювання відтворює цю логіку інструментально: система штучного інтелекту виконує операцію систематичного зіставлення в масштабі й зі швидкістю, недосяжними для методів, які Суд оцінював у 2000 році, але юридична природа втручання залишається тією самою.

Виявлені проблеми не є суто технічними – вони є правовими в тому сенсі, що чинна нормативна база контролю за обробкою персональних даних в Україні не дає відповіді на питання про те, як здійснювати перевірку відповідності системи, яка за своєю природою є непрозорою. Це підтверджує центральну тезу дисертації про необхідність переходу від реактивної моделі контролю до ризик-орієнтованої моделі.

Станом на час дослідження в Україні відсутній правовий акт, який комплексно регулював би питання штучного інтелекту. Базовим інструментом

залишається Закон України «Про захист персональних даних» 2010 року [10], доповнений Концепцією розвитку штучного інтелекту, схваленою розпорядженням Кабінету Міністрів України у 2020 році [141], яка визначила дев'ять пріоритетних сфер та закріпила базові принципи розвитку штучного інтелекту, що відповідають Принципам Організації економічного співробітництва та розвитку [142, с. 14].

Як зазначає А. Гачкевич, питання застосування штучного інтелекту в Україні наразі лише частково врегульоване Законом «Про захист персональних даних» та Концепцією 2020 року, що зумовлює необхідність посилення механізмів контролю [163]. Концепція, проте, є рамковим політичним документом, який не створює операційного контрольного інструментарію.

Приєднання України до Рамкової конвенції Ради Європи про штучний інтелект [165] створює прямі міжнародно-правові зобов'язання щодо забезпечення відповідності життєвого циклу систем штучного інтелекту правам людини та верховенству права. Виконання цих зобов'язань вимагає не лише декларативного приєднання, а й гармонізації національного законодавства з ризик-орієнтованою моделлю Акта Європейського Союзу про штучний інтелект.

Йдеться насамперед про запровадження диференціації систем за рівнями ризику, встановлення вимог прозорості та людського нагляду, а також про чітке розмежування компетенції майбутнього наглядового органу із захисту даних та органів, що здійснюватимуть нагляд за іншими аспектами систем штучного інтелекту. При цьому, з огляду на висновки цього підрозділу, орган захисту даних має бути визначений ключовим суб'єктом контролю саме в частині систем штучного інтелекту, які обробляють персональні дані [101].

Узагальнення дозволяє сформулювати напрями розвитку українського контрольного механізму, що випливають із проведеного аналізу. При цьому запозичення окремих норм зарубіжного права не є запорукою ефективних змін, оскільки переосмислення природи контролю та його систем: оцінювання

ризиків на початкових стадіях, на етапі формування моделі, що в свою чергу, призведе до розбудови інституційної спроможності [166, с. 278].

По-перше, наглядові органи мають розвивати технічну спроможність аудиту алгоритмічних систем, що включає не лише перевірку документації оператора, а й здатність здійснювати незалежне тестування моделі на предмет вивідного профілювання чутливих категорій даних та оцінювати адекватність застосованих технік мінімізації даних, таких як псевдонімізація, диференційна приватність чи федеративне навчання.

Окремого нормативного забезпечення потребує здатність наглядового органу встановлювати факт вчинення практик, віднесених статтею 5 Акта про штучний інтелект до неприйнятного рівня ризику, – маніпуляції поведінкою та соціального скорингу, – оскільки елементи складу цих порушень (ефект істотного викривлення поведінки, відчутне погіршення здатності ухвалити поінформоване рішення, використання оцінки поза контекстом її формування) є емпіричними, а не суто юридичними категоріями і не можуть бути встановлені виключно шляхом аналізу правових підстав обробки. У зв’язку з цим у діяльності новоствореного наглядового органу з питань захисту персональних даних важливо запровадити механізм залучення фахівців та експертів, технічних аудиторів – за аналогією з моделлю міждисциплінарних команд, рекомендованою [161], а також доповнити передбачений процесуальним законодавством перелік видів експертиз самостійним видом експертиз.

Важливість урегулювання системи ризиків підкреслює й те, що ризик-орієнтована модель регулювання та категорія заборонених практик, визначених у Акті про штучний інтелект, для ЄС залишилася незмінним пріоритетом, в той час як застосування інших вимог до автономних високоризикових систем, а також систем, інтегрованих у продукцію було відтерміновано на 2027 та 2028 роки відповідно [167].

По-друге, необхідним є перегляд індивідуалізованої моделі контролю на користь системного аудиту: оцінка законності обробки персональних даних

системою штучного інтелекту повинна охоплювати архітектуру системи в цілому – джерела навчальних даних, механізми відбору і мінімізації, наявність гарантій проти запам’ятовування й реконструкції даних, – а не обмежуватися перевіркою окремих операцій. Ця вимога прямо продовжує стандарт операційної незалежності наглядового органу, сформульований Судом ЄС у справах Schrems I і Schrems II (проаналізованих у підрозділі 3.1 дисертації), де незалежність визнана конституційною, а не декларативною вимогою, яка передбачає спроможність органу діяти всупереч зовнішньому впливу [111; 112].

У контексті систем штучного інтелекту ця вимога набуває технічного виміру – орган, позбавлений власної спроможності перевірити модель, залишається функціонально залежним від її розробника навіть за повної інституційної незалежності.

По-третє, наглядові органи повинні брати активну участь у формуванні законодавчих ініціатив на етапі їх розробки, аби забезпечити, що раціоналізація регуляторного навантаження на бізнес не здійснюється за рахунок применшення повноважень самих наглядові органів або скорочення обсягу прав суб’єктів персональних даних.

Таким чином, технології штучного інтелекту не лише породжують нові матеріально-правові ризики обробки персональних даних, а й трансформують саму конфігурацію контрольного механізму, висуваючи вимоги одночасного оновлення нормативного інструментарію, інституційної архітектури, технічної спроможності та методології нагляду.

Для України, що перебуває на ранньому етапі формування національної політики у сфері штучного інтелекту, ці вимоги означають необхідність побудови – а не лише вдосконалення – дієвої моделі контролю, заснованої на створенні незалежного спеціалізованого органу, наділеного слідчими, коригувальними та консультативно-дозвільними повноваженнями, гармонізації законодавства з європейськими ризик-орієнтованими

стандартами та формуванні технічної спроможності системного аудиту алгоритмічних систем.

Лише за умови одночасної реалізації цих напрямів український механізм контролю за обробкою персональних даних зможе зберегти ефективність в умовах поширення технологій штучного інтелекту.

3.3. Організаційні та нормативно-правові напрями забезпечення ефективності здійснення контролю за обробкою персональних даних в Україні

Відхід Української системи від функціонування наглядового органу за обробкою персональних даних у вигляді урядового компоненту, здійснений у 2014 році через ліквідацію Державної служби з питань захисту даних як підконтрольного Уряду України органу, що не мав інституційної, кадрової, процедурної та фінансової автономії, як про те вже зазначалося у підрозділі 2.2. цієї дисертації, започаткував період установлення та розбудови незалежної системи контролю за обробкою та захисту персональних даних.

При цьому покладання таких функцій безпосередньо на Омбудсмана України здійснювалося як складова доповнення його вже існуючого мандату парламентського контролю.

Варто зауважити, що наділення Уповноваженого Верховної Ради України з прав людини функціями, є вже усталеною практикою в Українській державі. Так, Уповноважений Верховної Ради України з прав людини наділений повноваженнями незалежного органу запобігання та протидії дискримінації відповідно до вимог Законів України «Про забезпечення рівних прав та можливостей жінок і чоловіків» [168] та «Про засади запобігання та протидії дискримінації в Україні» [169], контролюючого органу щодо розгляду звернень громадян та доступу до публічної інформації [170], а також виконує функції національного превентивного механізму відповідно до Факультативного протоколу до Конвенції проти катувань та інших жорстоких,

нелюдських або таких, що принижують гідність, видів поводження та покарання [171].

Вказане обумовлено тим, що за своїм унікальним конституційним статусом, Уповноважений Верховної Ради України з прав людини є чи не єдиною посадовою особою щодо якої законодавчо закріплені гарантії незалежності та автономії, а коло об'єктів, на яких поширюються контролюючі повноваження Уповноваженого, є надзвичайно широким та охоплює всі без виключення органи державної влади та місцевого самоврядування, навіть в умовах запровадження правого режиму воєнного стану. Як одну із позитивних складових діяльності омбудсманів, А.П. Лелеченко згідно європейських та міжнародних стандартів визначає їхню незалежність згідно із стандартами Ради Європи, ООН та Європейської комісії «За демократію через право» (Венеціанська комісія), включаючи Паризькі принципи, Принципи Венеційської комісії щодо захисту інституту Омбудсмана та Рекомендації Комітету Міністрів Ради Європи [172].

Оцінюючи цю тезу в контексті попередньо визначених особливостей здійснення Уповноваженим парламентського контролю за захистом персональних даних, можна дійти до висновку, що саме період виконання вказаних функцій безпосередньо Офісом Омбудсмана, характеризується створенням сталої системи та розбудови генези захисту персонального даних в Україні. Особливо це демонструється у порівнянні із інституційним досвідом інших державних органів, які здійснювали захист приватності громадян в Україні лише декларативно.

Відтак, попри наявність законодавчих ініціатив та закріплення відповідних зобов'язань у євроінтеграційних дорожніх картах, Уповноважений Верховної Ради України з прав людини вже тривалий період залишається ключовим суб'єктом у системі контролю за дотриманням законодавства про обробку персональних даних та зберігає функції наглядового органу із захисту персональних даних.

Для виконання відповідних функцій, в структурі Секретаріату Уповноваженого [173] функціонує самостійний структурний підрозділ – Департамент моніторингу додержання інформаційних прав.

У структурі згаданого Департаменту є відділ розгляду звернень та взаємодії з суб'єктами обробки персональних даних та відділ нормативно-правової роботи та моніторингу міжнародних стандартів у сфері захисту персональних даних, працівники якого з метою здійснення контролю та згідно з підпунктами 2, 3 частини першої статті 23 Закону України «Про захист персональних даних» реалізують відповідні контрольні функції. Також Уповноваженим Верховної Ради України з прав людини, відпоідно до штатної структури, призначено свого представника (заступника) з інформацінйних прав, до сфери відповідальності якого фактично віднесено діяльність Офісу Омбудсмана України щодо контролю за захистом персональних даних.

Щонайперше слід зауважити, що штатна чисельність згаданих відділів складає 11 посад (5 та 6 у кожному відділі відповідно), що становить 42,3% від чисельності працівників Департаменту моніторингу додержання інформаційних прав та 2,4 % від загальної кількості працівників Офісу Омбудсмана України [172]. Незначний кадровий резерв, з якого було б можливе залучення до роботи додаткового висококваліфікованого та досвідченого персоналу, велике навантаження, а також обмежений розвиток спроможності персоналу у Звіті щодо оцінювання спроможності Уповноваженого Верховної Ради України з прав людини [174, с. 29] визначені найбільшими викликами в умовах воєнного стану.

Втім, пов'язані з воєнним станом виклики, істотно трансформують не лише ризики у сфері захисту персональних даних, але й у свою чергу, зумовлюють необхідність трансформації діяльності наглядового органу. Так, В.А. Світличний [175, с. 226-228], розглядає несанкціоноване поширення інформації про військовослужбовців, кібератаки на державні ресурси, а також маніпуляції з персональними даними у контексті інформаційної війни як типові порушення.

Очевидно, що вказане ускладнює здійснення контролю за обробкою персональних даних та розширює коло суб'єктів, змінює специфіку їхньої роботи. Для прикладу, у грудні 2024 держава зазнала наймасштабнішої зовнішньої кібератаки на державні реєстри [176]. Атака була здійснена з боку держави-агресора, щоб порушити роботу критично важливої інфраструктури України. Внаслідок зазначеного було зупинено діяльність державних реєстрів, які адмініструються Міністерством юстиції України, таких як Державний реєстр актів цивільного стану громадян, Єдиний державний реєстр юридичних осіб та фізичних осіб підприємців, Державний реєстр прав на нерухоме майно та їх обтяжень. Однак у вказаній ситуації, як спосіб реагування, Уповноважений звернувся до Міністерства юстиції України, Національної поліції України та Служби безпеки України. Остання повідомила, що за фактом здійснення росіянами кібератаки на державні реєстри розпочато досудове розслідування у кримінальному провадженні [73].

Вказане засвідчує, що у цих умовах забезпечення належного рівня захисту даних набуває не лише правового, але й безпекового значення, що потребує міждисциплінарного підходу із залученням фахівців у сфері кібербезпеки та інформаційних систем, залучення яких не передбачено у межах здійснення відповідних перевірок Секретаріатом Уповноваженого.

Окремим викликом в умовах триваючої війни є фактичне здійснення недержавними українськими та міжнародними організаціями функцій із забезпечення допомоги постраждалим від війни або документування воєнних злочинів. Через недостатню спроможність державних механізмів, недержавний сектор забезпечує здійснення надзвичайно важливого в умовах війни пласту роботи. Одночасно із зазначеним, така діяльність недержавних організацій супроводжується обробкою значної кількості персональних даних осіб, у тому числі чутливих (зокрема про вчинення сексуального насильства [177]). За загальним правилом, чутливі персональні дані не можуть поширюватися поза межами таких організацій за відсутності згоди, наданої суб'єктом персональних даних [178, с. 175-176]. Однак національне

законодавство сьогодні не містить спеціального комплексного регулювання особливостей збору, зберігання, передачі та використання таких даних. Водночас уразливий психологічний стан таких осіб, що є суб'єктами персональних даних, може істотно впливати на їх здатність усвідомлено оцінювати наслідки передачі персональних даних. У таких умовах особа не завжди має можливість повною мірою розуміти, кому саме вона надає свої дані, з якою метою вони будуть використовуватися, де та протягом якого строку зберігатимуться, кому можуть бути передані та які механізми захисту від їх неправомірного використання існують.

Відсутність спеціальних процедур обробки персональних даних осіб, які пережили особливо травматичні події, створює ризики надмірного збору інформації, її неконтрольованого поширення, повторного використання з іншою метою, а також порушення принципів законності, пропорційності та мінімізації даних, що є фундаментальними стандартами сучасного права захисту персональних даних. Ще одним викликом, пов'язаним із порушенням правового режиму захисту персональних даних, за наведених вище обставин є можлива їх транскордонна передача, зумовлена використанням такими організаціями іноземних серверів та хмарних сховищ.

Зважаючи на назначені та інші ризики, а також системні проблеми, які призводять до неефективності здійснюваного контролю та аналіз яких здійснено у попередніх підрозділах цієї дисертації, у цьому підрозділі виокремлено організаційні та нормативно-правові напрями, які потребують системного вдосконалення з метою забезпечення ефективності здійснення контролю, у тому числі розроблено авторські пропозиції змін до законодавства України.

Суміщення двох мандатів має свої наслідки та недоліки, а практика поєднання Уповноваженим функцій парламентського контролю та мандату наглядового органу за GDPR потребує перегляду та якнайшвидшого вирішення ряду проблемних питань, що були наведені у тексті дисертації раніше, як-от виконання невластивої каральної функції під час складання

протоколів про адміністративну відповідальність (підрозділ 2.3.), так і інших системних недоліків, які унеможливлюють здійснення Омбудсманом України ефективного та дієвого контролю за додержанням персональних даних.

Проведений аналіз дає підстави для виваженої позиції: прийняття законопроєктів «Про захист персональних даних» [179] та «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації» [52], підтримане Уповноваженим у щорічних доповідях за 2022–2024 роки та таке, що пройшло перше читання у Верховній Раді України 20 листопада 2024 року, є необхідною, але не достатньою умовою гармонізації українського законодавства з європейськими стандартами.

Відтак, інституційна реформа (створення нового органу) та процесуальна реформа (зміни до Кодексу України про адміністративні правопорушення) мають здійснюватися синхронно, інакше новий орган, наділений широкими матеріально-правовими повноваженнями, успадкує ті самі процесуальні дефекти, які наразі знижують ефективність діяльності Уповноваженого.

Є очевидним, що створення нового спеціалізованого наглядового органу саме по собі не вирішить проблем, виявлених у підрозділі 2.3, таких як збільшення строків для притягнення особи до відповідальності за статтею 38 Кодексу України про адміністративні правопорушення або визначення поняття триваючого правопорушення, якщо одночасно не будуть внесені відповідні зміни до Кодексу України про адміністративні правопорушення.

Натомість частина сутнісних недоліків, виявлених у підрозділі 2.3 цієї дисертації, можуть бути вирішеними шляхом надання відповідних повноважень наглядовому органу самостійно притягувати до відповідальності осіб, які порушили законодавство про захист персональних даних. Зокрема, вказане одночасно усувало неузгодженість у статусі наглядового органу із вимогами GDPR, усувало питання затягування судами термінів розгляду справ з причин, що не залежать від наглядового органу. За таких умов також втрачає актуальність питання надання права оскаржувати в апеляційній інстанції

рішення судів, які здійснювали розгляд складених протоколів про адміністративні правопорушення.

Окремо слід наголосити на випадках, коли внаслідок необґрунтованих зволікань або низької юридичної техніки, новоствореним контролюючим органам не забезпечують правових гарантій протидії перешкоджанню їхній діяльності, що суттєво обмежує інституційну спроможність таких органів. Показовим є випадок закріплення у профільному законі про Військового омбудсмана норми, яка передбачає «встановлену законом відповідальність» за невиконання законних вимог Військового омбудсмана [180], однак відсутності у будь-якому іншому нормативно-правовому акті (у тому числі Кодексі України про адміністративну відповідальність) конкретного виду та змісту юридичної відповідальності. Відтак важливим аспектом дієвості новоствореного наглядового органу із захисту персональних даних, є не лише формальне закріплення обов’язку забезпечення сприяння та заборони перешкоджання, але й реальних механізмів притягнення таких суб’єктів до відповідальності у разі порушення таких зобов’язань та відмови від співпраці.

В сьогоднішніх умовах, які передують створенню спеціалізованого незалежного наглядового органу та змістовного обсягу його повноважень як наглядового органу [52] та введення у законодавство новел у сфері захисту персональних даних, виникає декілька викликів. Насамперед, мова йде про запровадження у проєкті нового Цивільного кодексу України [53], прийнятого Верховною Радою України в першому читанні 28 квітня 2026 року, права на забуття як самостійної особистої немайнової гарантії.

Вказане законодавче рішення подається як таке, що узгоджується з континентальною традицією визнання особистих немайнових прав елементом цивільно-правового статусу особи і структурно відтворює логіку статті 17 Регламенту (ЄС) 2016/679. Водночас редакція запропонованої статті 328 містить прогалину, що має пряме значення для ефективності контролю за обробкою персональних даних. Так, підставою застосування права на забуття є визнання інформації «такою, що втратила суспільний інтерес, а її подальша

обробка завдає шкоди особистим правам такої особи»[53]. У запропонованій редакції законопроєкту, норма щодо «втрати суспільного інтересу» сформульована як самостійна альтернатива поряд із недостовірністю, неповнотою та протиправністю обробки даних. Вказане вириваєтся з контексту, у якому близький за змістом критерій – «неактуальність з огляду на час, що минув» застосовується у судовій практиці [110] як один із факторів обов'язкового багатофакторного зважування проти суспільного інтересу в доступі до інформації, а не як самостійна та достатня підстава.

Поряд із законодавчим врегулюванням поняття «права на забуття», важливо забезпечити їх процедурне узгодження із повноваженнями наглядового органу. Наприклад, здійснення Уповноваженим повноваження щодо видалення чи знищення даних, передбаченого пунктом 5 статті 23 Закону, має спиратися на аналогічну методологію оцінки, запроваджену у законодавстві, а не лише на формальну констатацію протиправності обробки. Отже додатково потребує визначення співвідношення цивільно-правового механізму реалізації права з компетенцією Уповноваженого за Законом «Про захист персональних даних», з метою уникнення паралельної юрисдикції та збереження превентивної функції нагляду.

Окрім процесуального питання притягнення до відповідальності осіб, що допустили порушення законодавства про захист персональних даних, авторська концепція цього дослідження обстоює тезу необхідності зміни концепції контролю за обробкою персональних даних від формально-адміністративної до ризик-орієнтованої моделі гарантування цифрових прав.

Надалі пропонується розглянути ознаки ризик-орієнтованої моделі гарантування цифрових прав, запровадження якої обґрунтовується, та корелюється із нормативною реалізацією цього принципу у статті 35 GDPR як процедурою оцінки ризиків при обробці персональних даних.

Перша ознака: превентивна орієнтація. На відміну від класичної моделі нагляду, де контроль є реакцією на порушення, що вже відбулося або відбувається, захист персональних даних вимагає попередньої оцінки ризиків,

яка має здійснюватися ще до початку обробки персональних даних. Це не є методологічною перевагою – це структурна необхідність, зумовлена непоправністю шкоди.

Друга ознака: технічна компетентність як умова ефективності. Орган контролю повинен мати не лише правові, але й технічні повноваження і спроможність – здатність незалежно тестувати системи обробки, алгоритми і проводити технічну оцінку відповідності. Ця ознака відрізняє процедуру оцінки ризиків при обробці персональних даних від класичного контролю.

Третя ознака: класичний адміністративний нагляд перевіряє відповідність нормі (правилу). Контроль за обробкою персональних даних має перевіряти відповідність правам суб'єктів – тобто оцінювати не лише «чи дотримані процедури», але й «чи забезпечені гарантії цифрової автономії особи». Це близьке до концепції Х. Хейманса про захист даних як конституційного мандата [6], але автор обстоює більш конкретну тезу: right-based логіка повинна визначати не лише мету органу, але й критерії оцінки ефективності його рішень.

Четверта ознака: підзвітність як системний принцип. На відміну від класичної моделі, де підзвітним є підконтрольний суб'єкт (перед наглядовим органом), у сфері захисту персональних даних принцип підзвітності є двостороннім: контролер підзвітний наглядовому органу, але і наглядовий орган підзвітний суспільству. Цей принцип, закріплений у статті 5(2) GDPR, принципово змінює архітектуру контрольних відносин.

П'ята ознака: ризик-орієнтованість як методологічна основа. Класичний нагляд передбачає однаковий обсяг уваги до всіх підконтрольних суб'єктів (або відбір за черговістю). Ризик-орієнтований контроль концентрує ресурси на суб'єктах і операціях обробки, що несуть найвищий ризик для прав суб'єктів даних. Для прикладу, в системі діяльності наглядового органу доцільно передбачити обов'язкову оцінку впливу на захист даних для систем ШІ, що обробляють персональні дані у сферах охорони здоров'я,

правоохоронної діяльності та публічного управління, з наданням результатів наглядовому органу.

Таку логіку, у тому числі реалізує система оцінки ризиків при обробці персональних даних, реєстру обробки підвищеного ризику та категорій штучного інтелекту високого ризику у відповідному Регламенті ЄС та проєктах Керівних принципів щодо класифікації систем штучного інтелекту високого ризику [181].

Важливо зауважити щодо гарантування процедур реальної незалежності наглядових органів. Поряд із нещодавно ухваленим Верховним судом США в рішенні Trump v. Slaughter [113], схожою є практика звільнення Уповноваженого Верховної Ради України з прав дитини в умовах воєнного стану, що здійснювалася у 2022 році [203; 204], попри пряме застереження у профільному законі щодо неможливості припинення повноважень Уповноваженого в умовах воєнного стану [78].

Особливої уваги заслуговують результати моніторингу виконання вимоги статті 24 Закону України «Про захист персональних даних» щодо обов'язкового визначення в органах державної влади та органах місцевого самоврядування структурного підрозділу або відповідальної особи з питань захисту персональних даних. За підсумками 2014 року із 62 центральних органів виконавчої влади лише 5 повідомили Уповноваженого про визначення такого підрозділу або особи [182, с. 225–253]. Зазначений показник – менше 10% від загальної кількості суб'єктів, зобов'язаних виконати відповідну вимогу, – є емпіричним підтвердженням системної неспроможності інституту внутрішнього контролю на рівні операторів персональних даних та відсутності дієвих механізмів примусового виконання нормативних приписів. Аналогічні дані у Щорічних доповідях за 2022-2025 відсутні.

Надалі внаслідок аналізу ситуації щодо реального стану додержання прав дитини як суб'єкта персональних даних, зважаючи на виявлені та відображені у підрозділі 2.1. дисертації недоліки законодавства,

запропоновано заходи нормативно-правового регулювання з метою забезпечення права дитини на приватність, що має підвищений рівень захисту.

Зокрема, на прикладі медійної сфери продемонстровано, що чинна багаторівнева система контролю не забезпечує належного рівня захисту прав дитини як суб'єкта персональних даних. Отже окремо необхідно звернути увагу на підставах додержання інформаційних прав дитини, а також безпосередньо правових та етичних підстав щодо поширення інформації про дитину.

У преамбулі GDPR наголошено, що діти потребують особливого захисту щодо персональних даних, оскільки можуть бути менш обізнаними про відповідні ризики, наслідки, гарантії та власні права; такий особливий захист має застосовуватися, зокрема, до використання персональних даних дітей для цілей маркетингу, створення профілів особистості чи користувача та збирання даних щодо дітей під час користування послугами, що пропонуються безпосередньо дитині [16]. Пунктом 75 преамбули GDPR також віднесено дітей до вразливої категорії з огляду на ризики, що можуть наставати внаслідок обробки їхніх персональних даних [16].

У статті «Адміністративно-правовий захист персональних даних дитини в соціально-гуманітарній сфері цифрової держави» І. Г. Ігнатченко та Я. С. Рябченко [183], розглядаючи правовий статус дитини як суб'єкта персональних даних, визначають кожну дитину складовою загальнонаціональної цифрової екосистеми. Автори приходять до висновку, що у цифрову добу персональні дані (включно із персональними даними неповнолітніх) стали новим стратегічним ресурсом.

В. М. Брижко, узагальнюючи міжнародні стандарти, відповідно до яких персональні дані мають оброблятися із законною метою та на законних підставах, визначає, що однією з таких підстав беззаперечено є згода на обробку персональних даних [184, с. 54]. Очевидно, що вказані вимоги мали б поширюватися і на дітей – неповнолітніх суб'єктів персональних даних.

Водночас О. А. Явор, В. Ф. Піддубна та О. О. Рубан у дослідженні «Правові проблеми захисту персональних даних неповнолітніх осіб відповідно до вимог вітчизняного законодавства та вимог GDPR», аналізуючи підстави обробки персоанльних даних неповнолітніх, доходять висновку про відсутність чітко визначеного віку згоди дитини та про наявність особливостей надання згоди неповнолітніми залежно від віку дитини та сфери суспільних відносин [185, с. 28].

Цей висновок є наскрізним стосовно предмету дослідження цього підрозділу, однак особливого значення він набуває за насупних обставин. Зокрема, науковцями, орієнтуючись виключно на визначені у статті 11 Закону України «Про захист персональних даних» підстави для обробки персоанльних даних, згода на обробку персональних даних дітей розглядається як самостійна та достатня правова підстава для публікації інформації. Однак такий підхід не враховує специфіки правового статусу дитини, її вразливості та обмеженої здатності усвідомлювати наслідки прийнятих рішень [186, с. 401]. Крім того не досліджено співвідношення доктринальної концепції свободи вираження поглядів та принципу забезпечення якнайкращих інтересів дитини в умовах сьогоденного нормативно-правоовго регулювання, встановленого на рівні спеціальних Законів України: «Про медіа» [54], «Про охорону дитинства». Саме на усунення цієї прогалини спрямований подальший виклад.

Відповідно до статті 11 Закону України «Про захист персональних даних», обробка персональних даних може здійснюватися на підставі визначених законом юридичних підстав, серед яких згода суб’єкта персональних даних, наявність відповідного дозволу, укладення та виконання договору, а також інші правочини, передбачені законодавством [10]. При цьому, на підставі проаналізованих у підрозділі 1.1. цієї дисертації, ознак правомірності згоди на обробку персональнх даних (таких як добровільність, поінформованість), доведеним є висновок щодо інтерпритації загадних ознак через призму здатністі дитини усвідомлювати правові наслідки її дій, що

напряму залежить від віку та рівня розвитку дитини. На переконання автора, вказаний підхід може застосовуватися і у випадках осіб, які мають ментальні порушення, та дієздатність яких обмежана у судовому порядку.

Повнолітня та дієздатна особа, на відміну від дитини, як правило, володіє необхідним рівнем автономії та критичного мислення для самостійної оцінки потенційних ризиків, пов'язаних зі збиранням, зберіганням та використанням інформації про неї, а також для реалізації передбачених статтею 8 Закону України «Про захист персональних даних» прав суб'єкта персональних даних [186, с. 403].

Щодо персональних даних дітей та їхньої обробки, законодавець встановлює підвищені стандарти захисту, що обгрунтовано обмеженою здатністю дітей, в залежності від їхнього віку та рівня розвитку, усвідомлювати значення відповідних дій та передбачати їх можливі наслідки.

Статями 31–32 Цивільного кодексу України [38] передбачено обмеження дієздатності дітей, у зв'язку із чим правочини на їх користь здійснюється їхніми законними представниками. Як наслідок, у більшості випадків згода на обробку персональних даних неповнолітніх надається їхніми законними представниками. Вказане обумовлює дію інституту надання згоди їхніми законними представниками (батьками, опікунами або іншими особами, які у визначених законодавством випадках діють в інтересах дитини та несуть відповідальність за прийняття рішень, що можуть впливати на її права, свободи та законні інтереси). Вказане знаходить подальший розвиток і у процесуальному законодавстві та інституті представництва [186].

Удосконалення наукового розуміння згоди як підстави обробки персональних даних дітей полягає в обґрунтуванні тези про те, що згода законного представника не може розглядатися як самодостатня правова підстава для поширення персональних даних дитини. Ця теза спирається на кілька аргументів.

По-перше, дитина, особливо у стані стресу або травми, не здатна повною мірою усвідомлювати наслідки поширення інформації про себе. Вона не може

оцінити довготривалий вплив цифрового сліду, можливість повторного використання інформації або її потенційний вплив на майбутнє життя [187].

По-друге, навіть згода батьків або законних представників не гарантує дотримання найкращих інтересів дитини: на практиці нерідко трапляються випадки, коли батьки діють під впливом емоцій, прагнення привернути увагу до проблеми або отримати допомогу, не враховуючи довгострокових наслідків для дитини.

Окрему увагу слід звернути на обставини, за яких законні представники не лише свідомо нехтують правами та інтересами дитини, але й умисно порушують їх. Так, у Щорічній доповіді Уповноваженого Верховної Ради України з прав людини за 2025 рік [188] зафіксовано випадки, коли керівники закладів системи інституційного догляду та виховання зловживали повноваженнями законного представника дітей зі статусом дитини-сироти та дитини, позбавленої батьківського піклування, влаштованих до таких закладів на повне державне утримання, виправдовуючи вчинення насильства щодо дітей, права яких вони мали б захищати.

Аналогічні випадки наводяться також у Щорічній доповіді за 2024 рік [73], що свідчить про системність цієї проблеми. Автором наукової роботи здійснено вибірковий аналіз офіційних ресурсів закладів інституційного догляду та виховання в мережі Інтернет. За результатами аналізу встановлено, що значна частина оприлюднених на офіційних вебсайтах та сторінках закладів у соціальних мережах зображень дітей безпосередньо не пов’язана з метою, заради якої дитину влаштовано до закладу, – забезпеченням цілодобового догляду, виховання та реабілітації.

Резолюція Парламентської асамблеї Ради Європи (ПАРЄ) 1843 «Захист особистого життя і персональних даних в Інтернеті і ЗМІ» [189] наголошує, що «у демократичній державі кіберпростір не повинен розглядатися як простір, де не існує законів і не захищені права людини», та закликає до консолідованого підходу всіх зацікавлених структур у забезпеченні права на повагу до особистого життя.

Натомість діти нерідко представлені у вразливому стані – саме як вихованці закладу інституційного догляду, із розкриттям обставин перебування, стану здоров'я, сімейної історії або статусу дитини-сироти чи дитини, позбавленої батьківського піклування. Такі публікації супроводжують інформаційні та благодійні кампанії й фактично слугують інструментом фандрейзингу – привернення уваги донорів та залучення коштів на потреби закладу.

Отже, персональні дані дитини, зібрані для забезпечення догляду, використовуються з іншою, похідною метою, що безпосередньо не відповідає інтересам самої дитини, а обслуговує репутаційні та фінансові потреби установи.

Така обробка не узгоджується з принципами обмеження та ненадмірності, закріпленими статтею 6 Закону України «Про захист персональних даних». Зокрема, легітимна для закладу мета залучення коштів не потребує оприлюднення ідентифікуючих зображень конкретних дітей і може бути досягнута знеособленими засобами – узагальненими описами, статистичними даними, знеособленими світлинами. Відтак мета обробки є непропорційною щодо втручання у приватність дитини.

Одночасне виконання керівниками закладів інституційного догляду та виховання функцій законного представника дитини призводить до фактичного поєднання однією особою адміністративних повноважень з функцією представництва інтересів дитини. За таких умов одна особа фактично поєднує: управління закладом та його ресурсами; відповідальність за організацію роботи персоналу та умов перебування дітей; та одночасно – обов'язок представляти та захищати найкращі інтереси конкретної дитини.

Подібна модель створює потенційний конфлікт інтересів, оскільки законний представник має діяти незалежно від адміністрації закладу та, у разі потреби, оскаржувати її дії, ініціювати перевірки, зміну форми влаштування дитини або реагувати на порушення прав дитини. Відтак управлінські рішення

можуть прийматися не в найкращих інтересах дитини, а з урахуванням потреб та інтересів самого закладу.

У таких умовах дитина фактично позбавляється незалежного представництва своїх інтересів, а механізми внутрішнього захисту прав стають формальними. На цю проблему неодноразово звертав увагу Європейський комітет із запобігання катуванням (далі – КЗК) [190]. КЗК висловлював стурбованість тим, що функції опікунів у закладах соціальної опіки виконували директори установ, попри попередні рекомендації щодо неприпустимості такої практики.

КЗК наголошував, що українські органи влади мають забезпечити альтернативні механізми опіки, які гарантуватимуть незалежність та неупередженість законних представників.

Це підтверджує обґрунтовану вище тезу про те, що згода законного представника не може розглядатися як самодостатня підстава поширення персональних даних дитини.

Важливі орієнтири щодо правомірності обробки персональних даних сформульовані у судовій практиці. У постанові Великої Палати Верховного Суду від 19 вересня 2018 року (справа № 806/3265/17) [191] наголошено, що згода на обробку персональних даних має бути усвідомленою та чітко вираженою, а обсяг і зміст даних – не надмірними щодо мети їх обробки. Отже, не у кожному випадку, що стосується отримання згоди на обробку персональних даних дітей, така згода може розглядатися як самодостатня правова підстава для поширення персональних даних, у тому числі медіа: вона має оцінюватися у сукупності з іншими критеріями, насамперед із урахуванням принципу найкращих інтересів дитини.

Для прикладу, у Рекомендаціях Секретаріату Уповноваженого Верховної Ради України з прав людини для медіаспільноти щодо захисту персональних даних під час публікації фото- та відеоматеріалів у журналістських розслідуваннях [192] визначено, що якщо батьки або

представники надають чутливі, негативні або недоречні коментарі про дитину, медіа мають утриматися від їх публікації в інтересах приватності дитини.

Відповідно до рекомендацій Дитячого фонду ООН (ЮНІСЕФ) для медіа [193], умови отримання згоди вимагають упевненості в тому, що дитину або її законного представника ніяк не примушували і що вони розуміють: матеріали про них можуть бути поширені як у місцевій громаді, так і в усьому світі.

Для цього згоду необхідно запитувати рідною мовою дитини, а давати її дитина має після поради з дорослим, якому довіряє. Рекомендації Комітету міністрів Ради Європи щодо керівних принципів захисту прав дітей у цифровому середовищі [194] закликають держави гарантувати дітям доступ до інформації про відповідні засоби правового захисту, зокрема про те, як і кому подавати скаргу, повідомляти про зловживання або просити про допомогу та консультування.

У практиці Європейського суду з прав людини сформовано підходи до балансування між свободою вираження поглядів і правом на приватність. Зокрема, у справі M.L. and W.W. v. Germany [195] ЄСПЛ наголосив, що свобода журналістів охоплює право визначати підхід до висвітлення теми та обирати обсяг і характер інформації, що підлягає оприлюдненню, у тому числі ідентифікаційні дані особи, однак реалізація цієї свободи підлягає оцінці з точки зору балансу з правом на повагу до приватного життя, з урахуванням принципу пропорційності та необхідності втручання у демократичному суспільстві.

У справах, що стосуються дітей, ЄСПЛ послідовно підкреслює необхідність забезпечення підвищеного рівня захисту: дитина розглядається як особа, що потребує особливого захисту, а її інтереси мають пріоритет над інтересами публічності, тому навіть за наявності суспільного інтересу втручання у приватність дитини повинно бути мінімальним і виправданим.

Стаття 85 Регламенту зобов’язує держави забезпечити узгодження між правом на захист персональних даних і свободою вираження поглядів, зокрема у сфері журналістики, допускаючи винятки з правил обробки персональних

даних лише за умови їх необхідності та пропорційності та виключно для журналістських цілей.

У науковій доктрині сформовано висновок, що сама по собі належність інформації до сфери суспільного інтересу не є достатньою підставою для її поширення, якщо таке поширення може завдати істотної шкоди правам дитини [186].

Вказана теза заходить підтвердження у практиці ЄСПЛ, де сформовано низку критеріїв оцінки балансу між свободою вираження поглядів та правом на приватність (логіка, відома за рішеннями у справах Von Hannover v. Germany [197] та Axel Springer AG v. Germany [198]): внесок публікації у суспільно значущу дискусію, ступінь публічності особи, її попередня поведінка, спосіб отримання інформації, а також зміст і наслідки її поширення. Однак ці критерії були сформульовані переважно щодо дорослих осіб [199] і не враховують у повному обсязі специфіку правового статусу дитини.

Граничний внесок пропонованої моделі порівняно з наявними підходами (рекомендаціями Секретаріату Уповноваженого та критеріями ЄСПЛ) полягає в одному: загальні критерії балансування вперше дитиноцентрично модифіковано й операціоналізовано у послідовний трискладовий тест, інтегрований зі стандартами захисту персональних даних і придатний для прямого застосування редакціями та контролюючими суб’єктами.

Першим елементом тесту є оцінка суспільної значущості інформації. Принципово важливо відмежовувати інформацію, що справді сприяє суспільно важливій дискусії, від тієї, що лише задовольняє цікавість до приватного життя. Суспільна значущість оцінюється не за рівнем емоційного відгуку аудиторії чи масштабом резонансу, а за здатністю інформації впливати на вирішення системних проблем, запобігати порушенням прав людини або забезпечувати суспільний контроль за діяльністю органів влади. Натомість сенсаційна інформація не може виправдовувати втручання у приватність дитини, навіть якщо викликає значний суспільний інтерес (рис. 4).

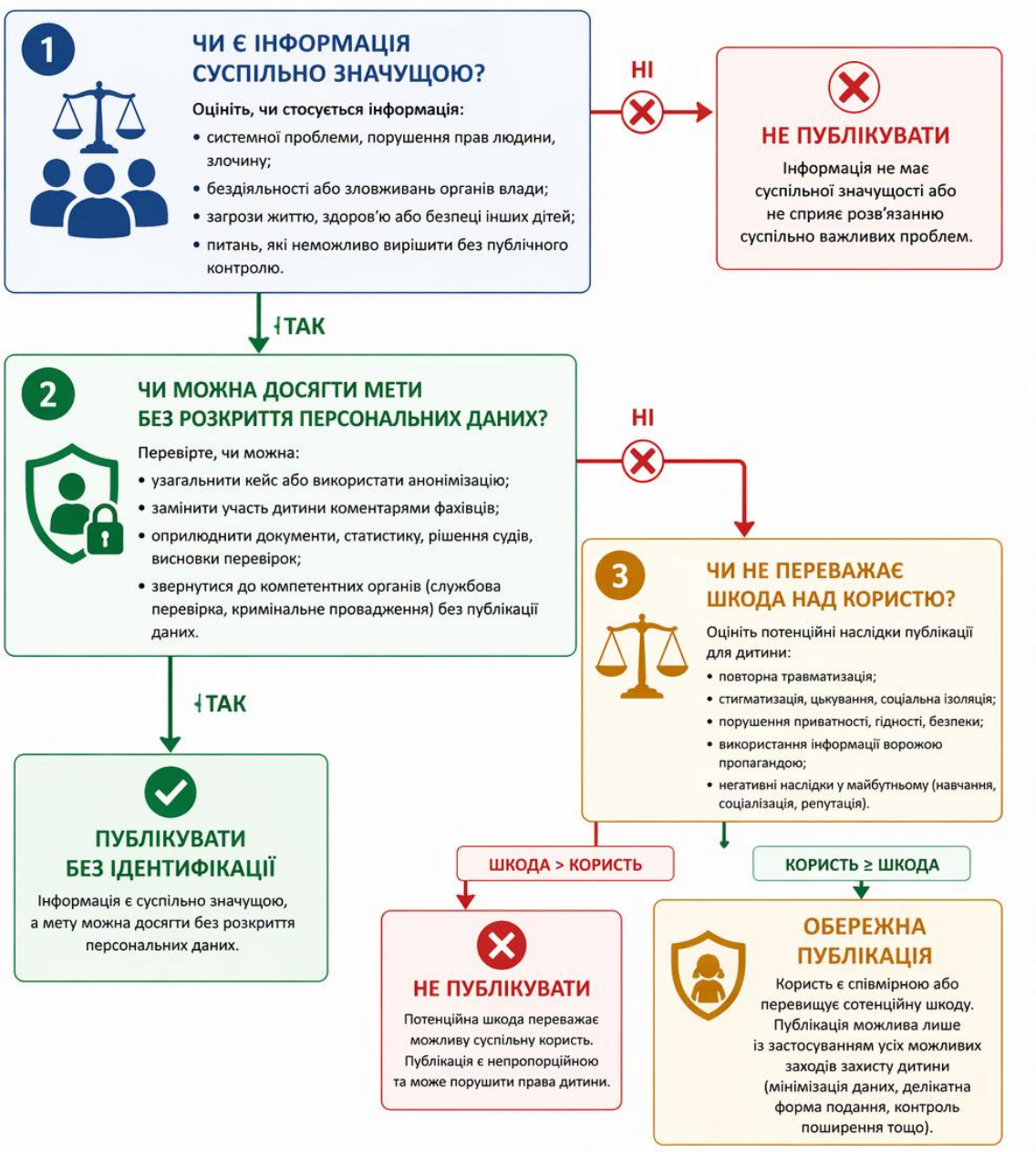

Рис. 4. Алгоритм оцінки балансу між свободою вираження поглядів та правом дитини на приватність

Зокрема, суспільно значущою може вважатися інформація, що розкриває факти системного насильства, недбалості, нехтування правами дитини або зловживань, створює передумови для реагування держави чи сприяє захисту дітей [39]. Натомість інформація, що має переважно сенсаційний характер або спрямована на підсилення емоційного ефекту, не

може виправдовувати втручання у приватність дитини, навіть якщо вона викликає значний суспільний інтерес.

Другим елементом є оцінка необхідності розкриття персональних даних. Ключовим тут є розуміння того, що участь дитини у медіа та розкриття конкретних відомостей, здатних її ідентифікувати, повинні розглядатися як виняток, а не стала практика. Необхідність розкриття персональних даних має оцінюватися з урахуванням можливості досягнення мети публікації іншими засобами – зокрема, через знеособлення (анонімізацію), узагальнення кейсів, залучення експертних коментарів замість безпосередньої участі дитини, а також оприлюднення документів, статистичних даних або результатів перевірок.

Позитивним прикладом є розслідування інтернет-видання Радіо Свобода, у якому під час висвітлення проблематики насильства щодо дітей, тимчасово переміщених (евакуйованих) до Республіки Польща [200], не лише знеособлено такі відомості про дітей як прізвище та ім’я, але й використано інші засоби анонімізації – замість реальних зображень дітей під час інтерв’ю використано ілюстративні анімації, а також змінено голос дітей.

У багатьох випадках такі альтернативні підходи дозволяють досягти суспільно значущої мети без створення додаткових ризиків для дитини, а відтак розкриття персональних даних є виправданим лише тоді, коли воно об’єктивно необхідне і без нього неможливо досягти поставленої мети.

Третім елементом є оцінка пропорційності втручання, яка передбачає зіставлення потенційної користі від поширення інформації та можливих негативних наслідків для дитини. У цьому аспекті доцільно враховувати не лише безпосередні, але й довгострокові наслідки публікації: повторної травматизації, стигматизації, соціальної ізоляції дитини, булінгу або дискримінації; втрати контролю над інформацією, ризиків для безпеки [186, с.407].

Оцінюючи пропорційність за наведеними принципами, важливим є урахування контексту кожної конкретної публікації. В умовах збройного

конфлікту або тимчасового переміщення (евакуації) дітей ризики, пов’язані з розкриттям персональних даних, значно зростають: навіть мінімальна сукупність даних, що може ідентифікувати дитину, здатна створити загрозу для безпеки дитини або її родини. Запропонований підхід узгоджується з позитивним обов’язком держави, що випливає із положень Конвенції ООН про права дитини, яка зобов’язує забезпечити захист дитини від усіх форм насильства та створити умови для її фізичного і психологічного відновлення, запобігаючи первинному та вторинному травмуванню [201].

Додатковими критеріями, що доповнюють трискладовий тест, є оцінка способу отримання інформації та її достовірності, а також аналіз змісту і форми її подання. Використання прихованих методів збору інформації, тиску на дитину або маніпуляцій з метою отримання коментарів є несумісним зі стандартами захисту прав дитини [202]; навіть за умови високої суспільної значущості інформації такі методи можуть свідчити про непропорційність втручання у приватне життя.

Водночас навіть об’єктивно значуща інформація може бути подана у спосіб, що призводить до додаткової шкоди для дитини, а тому форма та спосіб демонстрації відомостей також підлягають оцінці. Таким чином, наукова новизна запропонованого підходу полягає, по-перше, в обґрунтуванні обмеженої придатності згоди як самодостатньої підстави обробки персональних даних дітей; по-друге, в адаптації критеріїв балансування, вироблених у практиці ЄСПЛ, до особливого статусу дитини; по-третє, у побудові послідовного трискладового тесту (суспільний інтерес – необхідність – пропорційність), доповненого оцінкою способу отримання та форми подання інформації; по-четверте, в операціоналізації принципу найкращих інтересів дитини у площині захисту персональних даних, тобто у його перетворенні з декларативного орієнтира на практичний інструмент прийняття рішень.

Запропонований тест дозволяє трансформувати загальні принципи міжнародного права у практичний інструмент прийняття рішень у діяльності

медіа, що сприятиме як підвищенню рівня захисту прав дитини, так і формуванню відповідальної журналістської практики.

Водночас сам по собі трискладовий тест (суспільна значущість – необхідність – пропорційність), попри його інструментальну цінність для оцінки допустимості конкретної публікації, не здатен забезпечити реальний захист без системи гарантій, які підкріплювали б його застосування на практиці. Такі гарантії, на наше переконання, мають розгортатися у двох взаємопов'язаних площинах: посилення юридичної відповідальності медіа (зовнішній примус) та розбудови механізмів редакційного самоконтролю (внутрішні запобіжники).

Чинна редакція Закону України «Про медіа» кваліфікує порушення вимог щодо нерозголошення інформації про дитину без письмової згоди її законних представників як значне порушення [54]. Така кваліфікація, однак, не відображає дійсного ступеня суспільної небезпеки відповідних діянь. З огляду на це автором раніше обґрунтовувалася доцільність переведення зазначеного порушення до категорії «грубе порушення» [186, с. 407].

Логічним продовженням цієї пропозиції є розширення самого переліку грубих порушень трьома самостійними складами. Перший охоплює випадки, коли збирання інформації (у процесі безпосередньої роботи з дитиною, включно з інтерв'юванням) або її подальше оприлюднення здійснюються у такій формі чи спосіб, що спричиняють ретравматизацію – повторне переживання дитиною травматичного досвіду. Другий стосується застосування до дитини прихованих прийомів фіксації інформації, психологічного тиску або маніпулятивних технік, спрямованих на її одержання. Третій полягає в умисному оприлюдненні персональних даних, сукупність яких нівелює ефект умовного знеособлення та фактично уможливлює ідентифікацію дитини. Тобто ситуацій, коли має місце умисне поширення в медіа персональних даних, які, попри умовне знеособлення дитини, дозволяють її ідентифікувати [186].

Принципово, що кожен із наведених складів має чітку прив’язку до відповідного елемента трискладового тесту, тобто санкційна конструкція відтворює доктринальну: ретравматизація свідчить про недотримання вимоги пропорційності; приховані методи, тиск і маніпуляції – про порушення стандарту допустимого способу одержання інформації; фактична ідентифікація дитини всупереч знеособленню – про відсутність необхідності розкриття даних. Відтак посилення відповідальності не є довільним законодавчим рішенням, а виступає юридичним забезпеченням кожного з критеріїв допустимості публікації.

Поряд із посиленням юридичної відповідальності необхідно запровадити у діяльності медіа внутрішні запобіжники на рівні самоконтролю – інтеграцію в редакційну політику так званих процедур Child safeguarding, які передбачають розроблення та прийняття медіа внутрішьорегуляційних політик запобіганню порушенню прав дитини, впроваджували у діяльність «екологічні» принципи взаємодії та роботи з дітьми.

Показовим орієнтиром тут можуть слугувати редакційні настанови BBC (Editorial Guidelines) [203], що містять окремий блок вимог до участі дітей і молоді у створенні контенту, включно з оцінкою потенційної шкоди ще на етапі підготовки матеріалу. Аналогічно, такими механізмами можуть бути також інформаційні, освітні та правопросвітницькі заходи: проведення спеціалізованих навчань і тренінгів; залучення до взаємодії з дітьми (зокрема, у формі інтерв’ю) не лише працівників медіа, але й психологів та соціальних педагогів.

Завершальним елементом системи запобіжників має стати процедура попередньої оцінки контенту. До оприлюднення матеріалів за участю дітей доцільно застосовувати посилений редакційний контроль, а до експертизи залучати фахівців у сфері захисту прав дитини, зокрема представників неурядового сектору. Предметом такої оцінки є прогнозування ризиків порушення прав дитини внаслідок публікації та встановлення того, чи є втручання у приватне життя обґрунтованим, а чи набуває ознак надмірності.

У сукупності ці гарантії операціоналізують трискладовий тест, перетворюючи його з аналітичного інструмента на систему практичних запобіжників, розподілених між кількома рівнями контролю – нормативним (секторальний регулятор), етичним (саморегулювання) та внутрішнім (редакційні процедури). Тим самим запропонований комплекс гарантій підвищує не формальну, а реальну спроможність контролю у медійній сфері – відповідно до загальної концепції, обґрунтованої у підрозділах 1.2 та 2.1 цієї дисертації.

Висновки до розділу ІІІ

1. Підтверджено авторську гіпотезу дослідження: ефективність механізму контролю за обробкою персональних даних знаходиться у прямій залежності від трьох чинників – інституційної незалежності наглядового органу, повноти та визначеності його контрольних повноважень, а також наявності пропорційного і реально здійснюваного санкційного механізму. Серед трьох досліджених юрисдикцій лише модель Європейського Союзу забезпечує системну присутність усіх трьох чинників. Встановлено, що Китайська модель є принципово неприйнятною як зразок для запозичення Україною – через відсутність інституційної незалежності наглядового органу, подвійну природу CAC як інструменту одночасного захисту даних і державного нагляду за громадянами, а також через відсутність судового контролю за рішеннями регулятора. Американська модель галузевого регулювання не є придатною в цілому через обмеженість інституційних ресурсів і горизонтальний характер вимог GDPR, до адаптації до якого орієнтована Україна; водночас досвід CPPA (незалежний спеціалізований орган) та захист специфічних категорій чутливих даних у трудових відносинах мають конкретний потенціал імплементації.

2. Виявлено, що міжнародний режим контролю за обробкою персональних даних у системах штучного інтелекту у його теперішньому вигляді є режимом, що тримається на м’якому праві та запозичує обов’язкову

силу ззовні – від GDPR, Акта ЄС про штучний інтелект, Конвенції 108+ та Рамкової конвенції Ради Європи про штучний інтелект. Виявлена закономірність генези регуляторного корпусу полягає в послідовному розширенні об'єкта контролю: від окремих персональних даних – до бази даних, алгоритму, автоматизованого рішення, моделі штучного інтелекту і, врешті, до екосистеми та ланцюга постачання моделей.

3. Обґрунтовано, що технології штучного інтелекту вимагають трансформації методології державного нагляду за трьома напрямами: розвитку технічної спроможності аудиту алгоритмічних систем (незалежне тестування, оцінка технік мінімізації); переходу від індивідуалізованої моделі контролю до системного аудиту; активної участі наглядових органів у законотворчому процесі задля запобігання скороченню їхніх повноважень під гаслом дерегуляції.

4. Запропоновано комплекс організаційних та нормативно-правових напрямів підвищення ефективності контролю в Україні, що охоплює: закріплення на рівні закону гарантій незалежності наглядового органу; запровадження триланцюгової системи контрольних повноважень відповідно до статті 58 GDPR; введення інституту обов'язкової процедури оцінки впливу на захист даних; законодавче закріплення санкційного механізму, прив'язаного до масштабу та тривалості порушення; уточнення термінологічної конструкції статті 22 Закону України «Про захист персональних даних» щодо ролі судів; а також доповнення переліку складів правопорушень у статті 188-39 Кодексу України про адміністративні правопорушення.

ВИСНОВКИ

Цією дисертацією наведено не лише теоретичне узагальнення, але й нове вирішення наукового завдання, що виявляється в розкритті поняття контролю за обробкою персональних даних. За результатами дисертаційного дослідження сформульовано такі основні висновки:

1. Доведено, що ключовою ознакою персональних даних є їх здатність прямо або опосередковано ідентифікувати особу, а ідентифікація не потребує повного набору персональних ідентифікаторів – за певних умов достатньою є обмежена сукупність даних, здатних у контексті конкретної інформаційної системи забезпечити виокремлення особи.

Виявлено нормативну неузгодженість між законодавчою категорією «спеціальних персональних даних» (стаття 7 Закону України «Про захист персональних даних») та підзаконною категорією «даних, що становлять підвищений ризик»: розбіжність юридичної сили джерел цих категорій унеможливлює їх системне співвіднесення і породжує правову невизначеність обсягу підвищених гарантій захисту. Окремо обґрунтовано існування самостійної прогалини правового регулювання щодо статусу інформації про померлу особу, зумовленої механічним поширенням на посмертні відомості режиму, розрахованого на живих суб’єктів персональних даних. Викладене засвідчує, що коректне розмежування персональних даних від суміжних категорій є функціональною, а не термінологічною передумовою розбудови диференційованої моделі контролю, оскільки саме межі предмета обробки визначають межі предмета контролю.

2. Досліджено співвідношення конституційних гарантій приватності (статті 28, 30–32 Конституції України) з міжнародно-правовими джерелами регулювання обробки персональних даних та встановлено похідний характер права на захист даних відносно права на повагу до приватного життя. Доведено пряме методологічне значення цього висновку: оскільки захист даних є складовою приватності одразу у чотирьох її вимірах (фізичному,

територіальному, комунікаційному, інформаційному), контроль за обробкою не може обмежуватися формальним адмініструванням і повинен забезпечувати субстанційний захист кожного з цих вимірів.

Обґрунтовано, що система принципів обробки персональних даних, закріплена у національному законодавстві, має суттєві структурні розбіжності з міжнародними стандартами – насамперед у частині принципу підзвітності, ризик-орієнтованого підходу та *privacy by design*. Встановлено, що ця розбіжність знижує ефективність правового регулювання в умовах цифрового середовища, оскільки саме вона визначає, чи будується законодавство на реактивному, чи на превентивному фундаменті, що є першим емпіричним підтвердженням центральної гіпотези дисертації на рівні джерел регулювання. Зокрема, на відміну від GDPR, законодавство України не містить вимоги проведення оцінки впливу на захист даних, а аналог цієї вимоги – повідомлення Уповноваженого про обробку підвищеного ризику – є суттєво вужчим за обсягом та змістом.

3. Досліджено багатоманітність доктринальних підходів до розуміння контролю за обробкою персональних даних та сформульовано авторське визначення цього поняття як здійснюваної на систематичній основі або за зверненням діяльності уповноважених суб'єктів, спрямованої на встановлення відповідності обробки персональних даних вимогам законодавства та захист прав суб'єктів персональних даних із застосуванням засобів впливу, – яке, на відміну від наявних у доктрині визначень, що зводять контроль до повноважень єдиного наглядового органу, фіксує його багатосуб'єктну природу як системну ознаку.

Обґрунтовано сферозалежний (секторальний) характер контролю: доведено, що конфігурація контрольного механізму – коло суб'єктів, обсяг повноважень, застосовні форми – визначається природою суспільних відносин, у межах яких здійснюється обробка, унаслідок чого уніфікована модель контролю є помилковою по суті предмета регулювання, а не лише практично недосконалою. На цій основі запропоновано п'ятирівневу

типологію суб'єктів контролю за критерієм природи суб'єкта та юридичної сили його рішень (загальний регулятор; секторальні державні регулятори; органи професійного самоврядування; етичні органи саморегулювання; внутрішній самоконтроль володільця), доповнену виокремленням громадського контролю як самостійного наскрізного квазіконтрольного елемента, підтверджену емпірично на медійному кейсі, у якому одночасно реалізуються чотири з п'яти рівнів типології.

4. Досліджено суб'єктний склад системи контролю за обробкою персональних даних в Україні, включно з інституційною позицією судів у цій системі, та доведено доктринальну некоректність віднесення судів до суб'єктів контролю за статтею 22 Закону: встановлено, що судова діяльність структурно протилежна адміністративному контролю за критеріями систематичності, ініціативності, превентивності та можливості прямого владного втручання, унаслідок чого запропоновано термінологічну корекцію законодавства – заміну щодо судів категорії «суб'єкт контролю» на категорію «суб'єкт судового захисту прав у сфері обробки персональних даних». Класифіковано повноваження Уповноваженого Верховної Ради України з прав людини за функціональним призначенням та стадією контрольного циклу (превентивна, розслідувальна, коригувальна, постконтрольна), що дало змогу встановити структурну асиметрію: у розслідувальному та дорадчому вимірах структура повноважень відповідає універсальному стандарту статті 58 GDPR, однак демонструє системне ослаблення в коригувально-санкційному вимірі – відсутність права самостійного накладення штрафу – за одночасного непропорційного розширення в нормотворчому вимірі, що не має прямого аналога в жодній із порівнюваних юрисдикцій. Виявлено, що ця асиметрія є інституційним джерелом розриву між дорадчою активністю Уповноваженого та статистично підтвердженою неефективності фактичного правозастосування.

Обґрунтовано, що для переходу до ризик-орієнтованої моделі контролю визначальним є саме коригувально-санкційний вимір повноважень, оскільки

лише він перетворює виявлення порушення на реальний превентивний стимул для суб'єктів обробки, – що є прямим структурним елементом авторської концепції ефективного контролю, операціоналізованої надалі через індекс SEI.

5. Досліджено статистичну динаміку та судову практику застосування адміністративної відповідальності за 2022–2025 роки та встановлено емпірично підтверджену диспропорцію: зростання кількості звернень громадян на 67 відсотків супроводжується скороченням кількості протоколів за статтею 188-39 Кодексу України про адміністративні правопорушення більш ніж на 77 відсотків, що доводить структурний, а не ситуативний характер неефективності механізму відповідальності і є прямим емпіричним підтвердженням центральної гіпотези дисертації на рівні правозастосування. Доведено функціональне співвідношення статей 188-39 і 188-40 Кодексу України про адміністративні правопорушення як «матеріальної» та похідної «процесуальної» санкцій; кількісне домінування статті 188-40 над статтею 188-39 у співвідношенні приблизно 5:1 дало змогу встановити, що первинною системною проблемою є не сама неправомірна обробка персональних даних, а неналежна взаємодія володільців і розпорядників персональних даних із наглядовим органом під час здійснення контрольних заходів.

Виявлено п'ять груп причин неефективності інституту адміністративної відповідальності – законодавчі, організаційні, правозастосовні, інституційні та системні; зокрема встановлено, що об'єктивно недостатній тримісячний строк притягнення до відповідальності за статтею 38 Кодексу України про адміністративні правопорушення зумовлює закриття 43,2 відсотка справ без застосування санкцій. Обґрунтовано, що прийняття проєкту Закону України від 25.10.2022 року № 8153 та Закону України від 18.10.2021 року № 6177 є необхідною, але недостатньою умовою підвищення ефективності відповідальності.

Доведено, що оптимальна стратегія реформування передбачає трирівневу синхронізацію: 1) на рівні матеріального права – диференціація санкцій залежно від масштабу й тривалості порушення та запровадження

обов’язкового статусу виконавчого документа для приписів Уповноваженого; 2) на рівні процесуального права – продовження строків за статтею 38 Кодексу України про адміністративні правопорушення до шести (дванадцяти для триваючих правопорушень) місяців, надання органу, який склав протокол, права на апеляційне оскарження, та законодавче визначення критеріїв малозначності й триваючого правопорушення; 3) на рівні інституційної архітектури – створення спеціалізованого наглядового органу відповідно до проєкту Закону України від 18.10.2021 № 6177 одночасним перенесенням до нього функцій контролю, передбачених наразі для Уповноваженого, але без повторення дволанкової моделі «орган контролю – суд» у її нинішньому вигляді стосовно фінансових санкцій помірного розміру. Лише одночасна реалізація цих трьох рівнів реформи здатна перетворити інститут адміністративної відповідальності за порушення законодавства про обробку персональних даних в Україні з переважно декларативного на реально діючий механізм захисту прав суб’єктів персональних даних.

6. Розроблено та застосовано авторський Supervisory Effectiveness Index (SEI) – інструмент оцінки ефективності наглядового органу за шістьма субіндексами. Встановлено, що лише модель Європейського Союзу забезпечує системну одночасну наявність трьох визначальних чинників ефективності контролю (9,0 з 10 балів за SEI), тоді як українська модель демонструє одночасний дефіцит за всіма трьома чинниками (4,0 з 10 балів). Обґрунтовано принципову неприйнятність китайської моделі для запозичення Україною як державою – кандидатом на членство в Європейському Союзі: відсутність незалежності регулятора, його подвійна функція органу захисту даних і водночас інструменту державного нагляду за громадянами, а також відсутність судового контролю за його рішеннями роблять цю модель системно несумісною з конституційними засадами правової держави. Встановлено обмежену, фрагментарну придатність американської моделі: цілісному запозиченню підлягає не галузева архітектура регулювання в цілому, а окремі елементи – досвід California Privacy Protection Agency як

спеціалізованого незалежного органу та GINA-підхід до захисту специфічних категорій чутливих даних у трудових відносинах. Доведено, що для України єдиним структурно релевантним орієнтиром реформування є модель незалежного спеціалізованого органу захисту даних за зразком нагялового органу за GDPR.

Виявлено засадничий розрив між формою і змістом чинної моделі контролю за трьома напрямами: 1) покладення наглядових функцій на Уповноваженого Верховної Ради України з прав людини – конституційного органу загальної правозахисної компетенції – об'єктивно обмежує інституційну, кадрову та експертну спроможність спеціалізованого нагляду; 2) адміністративно-деліктний механізм виявлення порушення (Секретаріат Уповноваженого) і застосування санкції (суд), що подовжує процедуру і послаблює невідворотність відповідальності; 3) закладений на момент прийняття профільного закону європейський орієнтир гармонізації відтоді суттєво змістився з ухваленням GDPR і Конвенції 108+, тоді як українське законодавство не встигає за цим зміщенням системно. Встановлено, що ключовими нормативними прогалинами є відсутність принципу підзвітності, обов'язкової оцінки впливу на захист даних (DPIA) та вимоги *privacy by design* як юридично обов'язкового стандарту, а також відсутність права наглядового органу на самостійне накладення адміністративного штрафу, що структурно послаблює превентивну функцію контролю. Доведено, що ці прогалини є не ізольованими технічними недоліками, а взаємопов'язаними проявами єдиної концептуальної помилки – побудови контролю за логікою ex post реагування на порушення замість ex ante оцінки та мінімізації ризиків.

7. Запропоновано комплекс взаємопов'язаних законодавчих заходів, що потребують синхронної реалізації на трьох рівнях. На інституційному рівні – завершення переходу від моделі Уповноваженого Верховної Ради України з прав людини до спеціалізованого незалежного органу захисту персональних даних відповідно до проєкту Закону України від 18.10.2021 року № 6177, з наділенням його повним обсягом контрольних повноважень за статтею 58

GDPR, включно з правом самостійного накладення адміністративного штрафу. На матеріально-правовому рівні – законодавче закріплення принципу підзвітності та обов'язкової процедури оцінки впливу на захист даних; запровадження вимоги *privacy by design* як юридично обов'язкового стандарту; диференціація санкцій пропорційно масштабу і тривалості порушення замість чинних фіксованих розмірів штрафів. На процесуальному рівні – продовження строків притягнення до відповідальності за статтею 38 Кодексу України про адміністративні правопорушення до строку, що враховує реальну тривалість процедури взаємодії наглядового органу із судом; надання органу, який склав протокол, права на апеляційне оскарження закриття справи.

Запропоновано трискладовий тест-підхід щодо оцінки допустимості публікації персональних даних дітей у медіа, що адаптує критерії балансування, вироблені у практиці Європейського суду з прав людини, з урахуванням принципу найкращих інтересів дитини та стандартів захисту персональних даних. Довершено запропонованим у дисертації законопроєктом змін до законів України «Про медіа» та «Про охорону дитинства», що вводить тест пропорційності поширення персональних даних дитини на засаді презумпції нерозкриття – як приклад галузевої імплементації авторської ризик-орієнтованої концепції контролю.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Рогова О.Г. Захист персональних даних у законодавстві Європейського Союзу та України. Теорія та практика державного управління. 2011. Вип. 3. С. 464-471. URL: http://nbuv.gov.ua/UJRN/Tpdu_2011_3_71.

2. Потіп М.М., Онищенко В.В. Обробка персональних даних в умовах воєнного стану. Молодь: наука та інновації : матеріали XII Міжнародної науково-технічної конференції студентів, аспірантів та молодих вчених: НТУ «Дніпровська політехніка», 2024. С. 171–172

3. Баранов О.А. Правове забезпечення інформаційної сфери: теорія, методологія і практика. Монографія, К., 2014. 497 с.

4. Баранов О.А., Брижко В.М. Захист персональних даних в сфері Інтернет речей. Інформація і право. 2016. №2 (17). С. 85-91 URL: https://il.ippi.org.ua/article/view/272899/268423

5. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України: дис. … канд. юрид. наук. К., 2007. 280 с.

6. Hijmans H. The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: the Story of Article 16 TFEU. University of Amsterdam, 2016. С. 15. URL: https://pure.uva.nl/ws/files/2676807/169421_DEFINITIEF_ZELF_AANGEPAST_full_text_.pdf

7. Bygrave L.A. Data Privacy Law: an International Perspective. Oxford : Oxford University Press, 2014. URL: https://discovered.ed.ac.uk/permalink/44UOE_INST/4phsfh/alma9924149501502466

8. Rouvroy A., Poullet Y. The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy.
URL:https://www.researchgate.net/publication/225248944_The_Right_to_Informa

tional_Self-Determination_and_the_Value_of_Self-Development_Reassessing_the_Importance_of_Privacy_for_Democracy

9. Cavoukian A., Taylor S., Abrams M. E. Privacy by Design: essential for organizational accountability and strong business practices. Identity in the Information Society, 2010. URL:https://link.springer.com/content/pdf/10.1007/s12394-010-0053-z.pdf

10. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

11. Караванський С. Практичний словник синонімів української мови. 5-те вид. БаК, 2014. XIV, С. 151

12. 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

13. 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

14. Рішення Конституційного Суду України від 20 січня 2012 року № 2-рп/2012 у справі № 1-9/2012 за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12#Text

15. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» Європарламент, Рада ЄС, Директива від 24.10.1995 № 95/46/ЄС. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text

16. Загальний регламент Європейського Парламенту і Ради (ЄС) «Про захист фізичних осіб у зв’язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ ЄС» від 27.04.2016 № 2016/679. URL: https://zakon.rada.gov.ua/laws/show/984_008-16

17. Bărbulescu v. Romania, рішення Великої палати Європейського суду з прав людини, 2017. URL: https://hudoc.echr.coe.int/fre?i=001-177082

18. Конвенція про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини) від 04 листопада 1950 р. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

19. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.

20. Онищенко В.В. Контроль за обробкою персональних даних та адміністративна відповідальність за порушення законодавства про захист персональних даних в умовах війни. Юридичний науковий електронний журнал. 2025. №12. С. 524-527

21. Конвенція про захист осіб у зв’язку з автоматизованою обробкою персональних даних Рада Європи; Конвенція, Міжнародний документ від 28.01.1981. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text

22. Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних. URL: https://zakon.rada.gov.ua/laws/show/994_363#Text

23. Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних: Закон України від 03.07.2013 № 383-VII. URL: https://zakon.rada.gov.ua/laws/show/383-18#Text

24. Пояснювальна записка до проєкту Закону України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних». URL: https://w2.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=46647&pf35401=258675

25. Національний план з виконання Плану дій щодо лібералізації Європейським Союзом візового режиму для України : затв. Указом Президента України від 22.04.2011 № 494/2011. URL: https://www.president.gov.ua/docs/288_1.pdf.

26. Про внесення змін до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Протокол від 10 жовтня 2018 року (CETS № 223).

27. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання та захисту прав і свобод людини і громадянина в Україні за 2013 рік. URL: https://ombudsman.gov.ua/uk/shchorichni-ta-specialni-dopovidi

28. Peruzzo and Martens v. Germany, no. 7841/08 : Decision of the European Court of Human Rights, 4 June 2013. URL: https://hudoc.echr.coe.int/eng?i=001-121998

29. Vukota-Bojic v. Switzerland, no. 61838/10 : Judgment of the European Court of Human Rights, 18 October 2016. URL: https://hudoc.echr.coe.int/fre?i=001-167490.

30. European Data Protection Board. Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects. Version 2.0. 8 October 2019. URL: https://www.edpb.europa.eu/system/files/documents/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

31. Пояснювальна доповідь до Протоколу про внесення змін до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних (CETS №223): схвалена Комітетом міністрів Ради Європи від 18.05.2018. URL:https://rm.coe.int/16808ac91a

32. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/ show/2657-12#Text

33. Про доступ до судових рішень. Закон України від 22.12.2005 № 3262-IV. URL: https://zakon.rada.gov.ua/laws/show/3262-15

34. Про Національний архівний фонд та архівні установи. Закон України від 24.12.1993 № 3814-XII. URL: https://zakon.rada.gov.ua/laws/show/3814-12#Text

35. Про доступ до архівів репресивних органів комуністичного тоталітарного режиму 1917-1991 років : Закон України від 09.04.2015 № 316-VIII. URL: https://zakon.rada.gov.ua/laws/show/316-19#Text

36. Про поховання та похоронну справу : Закон України від 10.07.2003 №1102-IV. URL: https://zakon.rada. gov.ua/laws/show/1102-15#Text

37. Стефанчук Р.О. Особисті немайнові права фізичних осіб (поняття, зміст, система, особливості здійснення та захисту) : монографія, 2008. С. 625

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

39. Про практику застосування адміністративними судами законодавства про доступ до публічної інформації : Постанова від 29.09.2016 № 10, Пленум Вищого адміністративного суду України. URL: https://zakon.rada.gov.ua/laws/show/v0010760-16#Text

40. Коваленко Н.В. Окремі складові адміністративно-правового режиму конфіденційної інформації. *Вісник Національного університету «Львівська політехніка»*. 2016. № 845. С. 75-82 URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/vnulpurn_2016_845_13.pdf

41. Уповноважений Верховної Ради України з прав людини : Лист-роз'яснення від 25.01.2018 р. № 2/9-К30665517/26-131, 2018. С. 1

42. Онищенко В.В. Проблемні аспекти інформаційного законодавства України: поширення інформації про померлого. Журнал «Правова позиція», 2023. Випуск № 3. С. 674-676 URL:https://www.lsej.org.ua/6_2023/157.pdf

43. Теорія держави і права: навчальний посібник : Крестовська Н.М., Матвєєва Л.Г., Тицька Я О., Атаманова Н.В., Арабаджи Н.Б. Міжнародний гуманітарний ун-т. 2021. С. 193 URL: library.megu.edu.ua:8180/jspui/bitstream/123456789/3344/1/2021-ТЕОРІЯ%20ДЕРЖАВИ%20І%20ПРАВА%20навч%20посібник.pdf

44. Бутинець Ф.Д., Виговська Н.Г., Малога Н.М., Петренко Н.І. Контроль і ревізія: Підручник для студентів спеціальності «Облік і аудит» вищих навчальних закладів. 3-є вид., доп. і перєроб. 2002. 543 с. URL:https://www.scribd.com/doc/50596161/%D0%91%D1%83%D1%82%D0%B8%D0%BD%D0%B5%D1%86%D1%8C-%D0%9A%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8C-%D1%96-%D1%80%D0%B5%D0%B2%D1%96%D0%B7%D1%96%D1%8F

45. Терещенко М.М. Державний контроль: сутність, основні підходи та концепції. *Вчені записки ТНУ імені В.І. Вернадського*. Серія: Державне управління. 2019. С. 117-121 URL: https://www.pubadm.vernadskyjournals.in.ua/journals/2019/4_2019/23.pdf.

46. Про основні засади державного нагляду (контролю) у сфері господарської діяльності. Закон України від 05.04.2007 №877-V. URL: https://zakon.rada.gov.ua/laws/show/877-16#Text

47. Про припинення заходів державного нагляду (контролю) в умовах воєнного стану: Постанова Кабінету Міністрів України від 13 березня 2022 р. № 303. URL: https://zakon.rada.gov.ua/laws/show/303-2022-%D0%BF#Text

48. Правила зберігання, захисту, використання та розкриття банківської таємниці : Постанова Правління Національного банку України від 14 липня 2006 року № 267. URL: https://zakon.rada.gov.ua/laws/show/z0935-06#Text

49. Про Національний банк України Закон України від 20.05.1999 № 679-XIV. URL: https://zakon.rada.gov.ua/laws/show/679-14#Text

50. Марущак А.В., Правові основи контрольно-наглядових повноважень Національного Банку України, автореферат, 2015. С. 1-10 URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/17c34f67-ba1f-44fc-9e55-732f92acffaa/content

51. Про затвердження Положення про порядок прийняття та розгляду скарг щодо неналежної поведінки адвоката, яка може мати наслідком його дисциплінарну відповідальність : Рішення Ради адвокатів України від 30.08.2014 № 120 (в редакції рішення Ради адвокатів України від «13» грудня

2025 року № 149). URL: https://unba.org.ua/assets/uploads/l%20egislation/pologennya/2025-12-13-polozhennya-149_6953f651b7eed.pdf

52. Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації. Проєкт закону від 18.10.2021 № 6177. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72992

53. Проєкт Цивільного кодексу України від 09.04.2026 № 15150. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/69837

54. Про медіа: Закон України від 13.12.2022 № 2849-IX. URL: https://zakon.rada.gov.ua/laws/show/2849-IX#Text

55. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання та захисту прав і свобод людини і громадянина в Україні за 2011 рік. Київ, 2012. С. 112–115.

56. Етичний кодекс українського журналіста : Пленум Національної спілки журналістів України, 2013. URL: https://cje.org.ua/ethics-codex/

57. Про охорону дитинства: Закон України від 26.04.2001 № 2402-III. URL: https://zakon.rada.gov.ua/laws/show/2402-14/ed20100727#Text

58. Про затвердження Положення про Державну службу України з питань захисту персональних даних : Указ Президента України від 6 квітня 2011 року №390/2011. URL: https://zakon.rada.gov.ua/laws/show/390/2011#Text

59. Про оптимізацію системи центральних органів виконавчої влади Постанова Кабінету Міністрів України; Схема від 10.09.2014 № 442. URL: https://zakon.rada.gov.ua/laws/show/442-2014-п#Text

60. Про затвердження Порядку здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних : Наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14, 2014. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text

61. Берлач А.І., Дзісяк О.П., Сусак М.С. Судовий контроль у системі адміністративного судочинства України: теоретико-правові та прикладні

аспекти. *Юридичний науковий електронний журнал*. 2025. № 1. С. 594–597. С. 594-597 URL: https://lsej.org.ua/1_2025/140.pdf

62. Біла книга з регулювання штучного інтелекту в Україні: бачення Мінцифри (версія для консультацій): Міністерство цифрової трансформації України. 2024. 30 с. URL:https://storage.thedigital.gov.ua/files/d/9d/0bbc3a705c821a197bedfcdfe00899d9.pdf

63. Пузириниа Н.С., Галушка Д.Ю. Судовий контроль за постановами органів національної поліції: аналіз практики скасування постанов як індикатор якості адміністративного провадження. С. 121-131 URL: https://journals.ondise.in.ua/index.php/herald/article/view/116/105

64. Про організацію роботи з оформлення матеріалів про адміністративні правопорушення: наказ Уповноваженого Верховної Ради України з прав людини від 22.12.2025 р. № 161.15/25. URL: https://www.ombudsman.gov.ua/storage/ app/media/uploaded-files/1-29122025-1640-161152025.pdf

65. Шкелебей. О.В. Судовий контроль в адміністративному судочинстві як конституційна гарантія захисту прав у публічно-правовій сфері. *Київський часопис права*. 2025. Випуск № 3. С. 264–271. https://doi.org/10.32782/klj/2025.3.37

66. Погорецький М. Судовий контроль за законністю проведення оперативно-розшукових заходів, що обмежують права та свободи людини і громадянина. Міжнародна поліцейська енциклопедія: у 10, 2010. С. 960–963.

67. Кодекс адміністративного судочинства України : Закон України від 06.07.2005 № 2747-IV. URL: https://zakon.rada.gov.ua/laws/show/2747-15

68. Татулич І. Ю., Федрак А. М., Новели судового контролю за виконанням судових рішень у цивільному судочинстві. *Аналітично-порівняльне правознавство* № 1 (2026): URL: https://journal-app.uzhnu.edu.ua/article/view/352649/339355

69. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні, 2015. С. 552

70. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

71. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2022 році. URL: https://ombudsman.gov.ua/report-2022/informatsiini-prava

72. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2023 році. Розділ 9 «Інформаційні права», підрозділ 1 «Захист персональних даних». URL: https://ombudsman.gov.ua/report-2023/rozdil-9-informatsiini-prava

73. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2024 році. Розділ 9 «Інформаційні права», підрозділи 9.1–9.1.3. URL: https://ombudsman.gov.ua/report-2024/informatsiini-prava

74. Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації : Наказ Уповноваженого Верховної Ради України з прав людини від 8 січня 2014 року № 1/02-14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#n215

75. Постанова Монастириського районного суду Тернопільської області від 06.09.2021 у справі № 603/455/21. URL: https://youcontrol.com.ua/catalog/court-document/99430574/

76. Захист персональних даних: правове регулювання та практичні аспекти, науково-практичний посібник, Рада Європи, 2021. URL:https://ombudsman.gov.ua/storage/app/media/uploaded-files/handbook_pers_data_protect_2021.pdf

77. Про звернення громадян : Закон України від 02.10.1996 № 393/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/393/96-вр#Text

78. Про Уповноваженого Верховної Ради України з прав людини : Закон України від 23.12.1997 № 776/97-В. URL: https://zakon.rada.gov.ua/go/776/97-%D0%B2%D1%80

79. Про затвердження Положення про представників Уповноваженого Верховної Ради України з прав людини : Наказ Уповноваженого Верховної Ради України з прав людини від 20.10.2022 № 84.15/22. URL: https://zakon.rada.gov.ua/laws/show/v84_1715-22#n11

80. Кодекс України про адміністративні правопорушення : Закон від 07.12.1984 № 8073-X. URL: https://zakon.rada.gov.ua/laws/show/8073-10#Text

81. Постанова Жовтневого районного суду м. Дніпропетровська від 23 січня 2017 року №201/188/17-п. URL: https://reyestr.court.gov.ua/Review/64254021

82. Конституційна скарга щодо конституційності статті 188-40 Кодексу України про адміністративні правопорушення, статті 22 Закону України «Про Уповноваженого Верховної Ради України з прав людини». URL: https://ccu.gov.ua/sites/default/files/18_3352024_0.pdf

83. Постанова Харківського апеляційного суду від 17 червня 2025 року у справі № 625/358/24. URL: https://reyestr.court.gov.ua/Review/128296864

84. Аналіз практики розгляду судами справ про адміністративні правопорушення, передбачені статтями 188-39, 188-40, 212-3 Кодексу України про адміністративні правопорушення щодо протоколів, складених уповноваженими особами Секретаріату Уповноваженого Верховної Ради України з прав людини та представниками Уповноваженого Верховної Ради України з прав людини в 2022–2024 роках. Вдовенко О., Воробйов Є.,

Васильняк Р., Гринишак М. Київ : ГО «Платформа прав людини», 2025. 31 с. URL: https://ppl.org.ua/wp-content/uploads/2025/02/analiz-sudovoyi-praktyky-188-39-188-40-212-3-v-2022-24.pdf

85. Спеціальна доповідь Уповноваженого Верховної Ради України з прав людини щодо додержання конституційного права на інформацію в умовах дії правового режиму воєнного стану https://ombudsman.gov.ua/storage/app/media/uploaded-files/spetsdopovid-vipravleno-1.pdf

86. Звіт Директорату інформаційного суспільства та протидії злочинності Департаменту інформаційного суспільства, медіа та інтернету : Генеральний директорат з прав людини і верховенства права : DGI SASG/2016/0733 . 2016. С. 106-115 URL: https://www.researchgate.net/publication/382489905%20_Report_of_DGI_Directorate_of_Information_Society_and_Action_Against_Crime_Information_Society_Department_Media_and_Internet_Division_Prepared_on_the_basis_of_the_expert_opinion_by_Eve_Solomon_Tanja_Ke

87. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

88. Про внесення змін до Порядку оформлення матеріалів про адміністративні правопорушення : Наказ Уповноваженого Верховної Ради України з прав людини від 02.02.2026 № 10.15/26. URL: https://zakon.rada.gov.ua/laws/show/v0010715-26#Text

89. Постанова Амур-Нижньодніпровського районного суду міста Дніпропетровська від 30.04.2024 у справі № 199/840/24. URL: https://reyestr.court.gov.ua/Review/118706191

90. Постанова Дніпровського апеляційного суду від 06 червня 2024 року у справі № 199/840/24. URL: https://reyestr.court.gov.ua/Review/119587303

91. Щодо встановлення вини особи під час закриття провадження про адміністративні правопорушення у зв’язку із закінченням строків притягнення до адміністративної відповідальності: узагальнений науково-консультативний

висновок від 07.11.2017. Науково-консультативна рада при Вищому адміністративному суді України.

92. Klass and Others v. Germany, рішення Європейського суду з прав людини від 06.09.1978 р. URL: https://hudoc.echr.coe.int/eng?i=001-57510

93. Leander v. Sweden, заява № 9248/81, рішення Європейського суду з прав людини від 26.03.1987 р. URL: https://hudoc.echr.coe.int/eng?i=001-57519

94. Rotaru v. Romania, рішення Великої палати Європейського суду з прав людини від 04.05.2000 р. URL: https://hudoc.echr.coe.int/eng?i=001-58586

95. Amann v. Switzerland, заява № 27798/95, рішення Великої палати Європейського суду з прав людини від 16.02.2000 р. URL: https://hudoc.echr.coe.int/eng?i=001-58497

96. S. and Marper v. The United Kingdom, заяви № 30562/04 і 30566/04, рішення Великої палати Європейського суду з прав людини від 04.12.2008 р. URL: https://hudoc.echr.coe.int/eng?i=001-90051

97. Roman Zakharov v. Russia, заява № 47143/06, рішення Великої палати Європейського суду з прав людини від 04.12.2015 р. URL: https://hudoc.echr.coe.int/eng?i=001-159324

98. Big Brother Watch and Others v. The United Kingdom, рішення Великої палати Європейського суду з прав людини від 25.05.2021 р. URL: https://hudoc.echr.coe.int/eng?i=001-210077

99. Malone v. The United Kingdom, рішення Європейського суду з прав людини від 02.08.1984 р. URL: https://hudoc.echr.coe.int/eng?i=001-57533

100. Liberty and Others v. The United Kingdom, рішення Європейського суду з прав людини від 01.07.2008 р. URL: https://hudoc.echr.coe.int/eng?i=001-87207

101. Регламент (ЄС) 2024/1689 Європейського Парламенту і Ради від 13.06.2024 р., що встановлює гармонізовані правила щодо штучного інтелекту (Акт про штучний інтелект). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202401689

102. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2021 році. URL: https://ombudsman.gov.ua/report-2021

103. M.K. v. France, заява № 19522/09, рішення Європейського суду з прав людини від 18.04.2013 р. URL: https://hudoc.echr.coe.int/eng?i=001-118703

104. Gaughran v. The United Kingdom, заява № 45245/15, рішення Європейського суду з прав людини від 13.02.2020 р. URL: https://hudoc.echr.coe.int/eng?i=001-200817

105. Centrum för Rättvisa v. Sweden, заява № 35252/08, рішення Великої палати Європейського суду з прав людини від 25.05.2021 р. URL: https://hudoc.echr.coe.int/eng?i=001-210078

106. Garnaga v. Ukraine, заява № 20390/07, рішення Європейського суду з прав людини від 16.05.2013 р. URL: https://hudoc.echr.coe.int/eng?i=001-119681

107. Zaichenko v. Ukraine (No. 2), заява № 45797/09, рішення Європейського суду з прав людини від 26.02.2015 р. URL: https://hudoc.echr.coe.int/eng?i=001-152437

108. Surikov v. Ukraine, заява № 42788/06, рішення Європейського суду з прав людини від 26.01.2017 р. URL: https://hudoc.echr.coe.int/eng?i=001-170462

109. Хартія основних прав Європейського Союзу від 07.12.2000. URL:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT

110. Case C-131/12 Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González: Judgment of the Court (Grand Chamber) of 13 May 2014. ECLI:EU:C:2014:317. URL: https://curia.europa.eu/juris/liste.jsf?num=C-131/12 .

111. Case C-362/14 Maximillian Schrems v. Data Protection Commissioner: Judgment of the Court (Grand Chamber) of 6 October 2015. ECLI:EU:C:2015:650. URL: https://curia.europa.eu/juris/liste.jsf?num=C-362/14.

112. Case C-311/18 Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems: Judgment of the Court (Grand Chamber) of 16 July 2020. ECLI:EU:C:2020:559. URL: https://curia.europa.eu/juris/liste.jsf?num=C-311/18.

113. Trump, President of the United States, et al. v. Slaughter, No. 25-332 : рішення Верховного Суду Сполучених Штатів Америки від 29 червня 2026 р. URL: https://www.supremecourt.gov/opinions/25pdf/25-332_qn12.pdf

114. Case C-40/17 Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV: Judgment of the Court (Second Chamber) of 29 July 2019. ECLI:EU:C:2019:629. URL: https://curia.europa.eu/juris/liste.jsf?num=C-40/17

115. Case C-252/21 Meta Platforms Inc. and Others v. Bundeskartellamt: Judgment of the Court (Grand Chamber) of 4 July 2023. ECLI:EU:C:2023:537. URL: https://curia.europa.eu/juris/liste.jsf?num=C-252/21.

116. Case C-13/16 Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA «Rīgas satiksme»: Judgment of the Court (Second Chamber) of 4 May 2017. ECLI:EU:C:2017:336. URL: https://curia.europa.eu/juris/liste.jsf?num=C-13/16

117. H&M fined €35,3 Million for violation of the GDPR. URL:https://dataprivacymanager.net/german-dpa-issued-e353-million-gdpr-fine-to-hm-for-violation-of-the-general-data-protection-regulation

118. The CNIL’s restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC. URL:https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en

119. Максіменцев М. Г. Відповідальність за правопорушення у сфері кіберзахисту персональних даних: кейси світових цифрових гігантів і виклики для України. Актуальні проблеми кримінального права і процесу та шляхи їх вирішення: *Матеріали Всеукраїнської науково-практичної конференції*. Державний податковий університет, 2024. С. 195–201.

120. Zalnieriute M. Google LLC v. Commission nationale de l'informatique et des libertés (CNIL). *American Journal of International Law*. 2020. – Vol. 114. Iss. 2. C. 261–267. URL: https://doi.org/10.1017/ajil.2020.5

121. State Of The Digital Decade 2026 – Closing Structural Gaps And Mobilising Investments for 2030 and Beyond. Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, 17.6.2026 COM(2026) 288 Final. URL.: Https://Ec.Europa.Eu/Newsroom/Dae/Redirection/Document/128542

122. California Privacy Rights Act of 2020 (CPRA), amending the California Consumer Privacy Act (CCPA). URL: https://cppa.ca.gov

123. Federal Trade Commission : FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook. 2019. URL: https://www.ftc.gov/.

124. Луценко О.Є. Правове регулювання приватності працівників у Сполучених Штатах Америки. Аналітично-порівняльне правознавство, 2023. Випуск № 1. С. 254-258 URL: https://journal-app.uzhnu.edu.ua/article/view/279187/273759

125. Genetic Information Nondiscrimination Act of 2008 : Public Law №110-233, 21 May 2008. URL: https://www.govinfo.gov/content/pkg/PLAW-110publ233/html/PLAW-110publ233.htm

126. Personal Information Protection Law of the People's Republic of China. URL:https://www.chinalawtranslate.com/en/personal-information-protection-law-of-the-p-r-c-pipl/

127. Ma A. La régulation du numérique : Chine, États-Unis, France. Fondation pour l'Innovation Politique, 2023. C. 69 URL: https://hal.science/hal-04653589v1

128. Пристай Р.А. Національні органи захисту даних в європейському союзі: роль і практика в сфері захисту персональних даних в соціальних мережах. *Науковий вісник Ужгородського Національного Університету*. 2024. Випуск 83. Ч.2. С. 245 – 252 URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/05/41-1.pdf

129. Про затвердження Положення про порядок здійснення провадження Уповноваженого Верховної Ради України з прав людини у справах про порушення прав і свобод людини і громадянина : Наказ Уповноваженого Верховної Ради України з прав людини від 10.03.2023 року № 30.15/23. URL:https://ombudsman.gov.ua/uk/organizacijno-rozporyadchi-dokumenti

130. Машненков К.А., Деркаченко Ю.В. Цифровізація публічного адміністрування як інструмент превентивного управління соціальними конфліктами та зміцнення економічної стійкості (безпеки). *Економічний простір*. 2026. № 210. С. 31–36 URL: https://economicspace.pgasa.dp.ua/article/view/353948/340401

131. Гумін О.М., Гачкевич А.О. Застосування сучасних технологій для модернізації системи кримінальної юстиції та стандарти Ради Європи зі штучного інтелекту. *Вісник кримінологічної асоціації України*. 2025. №2 (35). ч. 2. URL: https://vca.univd.edu.ua/ index.php/vca/article/view/595

132. Басиста І.В., Удовенко Ж.В., Кулинич М.А. Огляд тенденцій щодо штучного інтелекту та його перспектив для процесуальних рішень під час кримінального провадження. *Науковий вісник Ужгородського національного університету*. Серія: Право. 2024. № 81(3). С. 19–38. URL: https://doi.org/10.24144/2307-3322.2024.81.3.3

133. Леонов Б.Д., Казьмірук С.Д. Інноваційні підходи застосування ШІ як інструменту парламентського контролю. *Трансформаційні процеси правотворчої діяльності та парламентського контролю*: матеріали конференції, 2025. С.55–58 URL: https://ippi.org.ua/sites/default/files/zbirnik_tez_30.10.2025.pdf

134. IEEE. Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems. 2016. URL: https://standards.ieee.org/industry-connections/ec/autonomous-systems/

135. Montréal Declaration for a Responsible Development of Artificial Intelligence. Université de Montréal, 2018. URL: https://montrealdeclaration-responsibleai.com

136. International Conference of Data Protection and Privacy Commissioners. Declaration on Ethics and Data Protection in Artificial Intelligence : adopted at the 40th International Conference of Data Protection and Privacy Commissioners, Brussels, 23 October 2018. URL: https://globalprivacyassembly.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf

137. Declaration on Ethics and Data Protection in Artificial Intelligence: 40th International Conference of Data Protection and Privacy Commissioners, 2018. URL: https://www.edps.europa.eu/data-protection/our-work/publications/international-conferences/resolutions-and-declaration-2018_en

138. OECD. Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449. Adopted 22 May 2019; updated 3 May 2024. URL: https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449#mainText

139. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text

140. Бакуменко А. В., Загребельна Н. А. Штучний інтелект і правові виклики у добу автономних технологій. Право і суспільство. 2025. Випуск № 4. Т. 1. С. 9–16. URL: https://doi.org/10.32842/2078-3736/2025.4.1.2

141. High-Level Expert Group on Artificial Intelligence. Ethics Guidelines for Trustworthy Artificial Intelligence. Brussels: European Commission, 2019. URL: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

142. Recommendation on the Ethics of Artificial Intelligence : UNESCO, 2021. URL: https://unesdoc.unesco.org/ark:/48223/pf0000381137

143. Попович Т. П., Маслюк О. В., Мацола А. А. Штучний інтелект та право на приватність: актуальні виклики цифрової епохи. Науковий вісник Ужгородського національного університету. Серія: Право, 2025. Випуск 90. Ч. 5. URL: https://doi.org/10.24144/2307-3322.2025.90.5.63

144. G7 Data Protection and Privacy Authorities' Action Plan. 3rd G7 DPA Roundtable. 2023, C. 20–21 URL: https://www.ppc.go.jp/en/aboutus/roles/international/conference/g7rt_communique

145. Рекомендація Rec (2020) 1 Комітету Міністрів Ради Європи державам-членам щодо впливу алгоритмічних систем на права людини . URL: https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154

146. Козир О. О. Використання штучного інтелекту в медіа. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Випуск 91. Ч. 1. С. 337–342. URL: https://doi.org/10.24144/2307-3322.2025.91.1.49.

147. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225), 2024. URL: https://rm.coe.int/1680afae3c

148. Берназюк І.М. Рамкова конвенція Ради Європи про штучний інтелект у контексті захисту прав людини: Виклики та значення для України. Науковий вісник Ужгородського Національного Університету, 2026. Серія Право. Випуск 93: частина 3. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2026/03/4-2.pdf

149. Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework: adopted on 16 July 2024. European Data Protection Board. URL: https://www.edpb.europa.eu/our-work-tools/our-documents/statements_en

150. Garante per la protezione dei dati personali. ChatGPT: closure of investigation and administrative sanction against OpenAI. URL : https://www.gpdp.it/web/guest/home%20/docweb/-/docweb-display/docweb/10085432?utm_source=chatgpt.com

151. Global Privacy Assembly. Resolution on Generative Artificial Intelligence Systems : adopted at the 45th Closed Session of the Global Privacy Assembly, 2023. URL: https://globalprivacyassembly.com/wp-content/uploads/2023/10/5.-Resolution-on-Generative-AI-Systems-101023.pdf

152. The Bletchley Declaration by Countries Attending the AI Safety Summit, 2023. URL: https:// www.gov.uk/government/publications/ai-safety-summit2023-the-bletchley-declaration/the-bletchley-declaration-bycountries-attending-the-ai-safety-summit-1-2-november-202

153. Резолюція Генеральної Асамблеї ООН «Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development», 2024 p. URL: https://docs.un.org/en/A/RES/78/265

154. Резолюція Генеральної Асамблеї ООН «Enhancing international cooperation on capacity-building of artificial intelligence», 2024 p. URL: https://docs.un.org/en/A/RES/78/311

155. «Statement on the Role of Data Protection Authorities in Fostering Trustworthy AI». 4th G7 DPA Roundtable, 2024 p. URL: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2024/communique-g7_241011/

156. Резолюція Генеральної Асамблеї ООН «Terms of reference and modalities for the establishment and functioning of the Independent International Scientific Panel on Artificial Intelligence and the Global Dialogue on Artificial Intelligence Governance» (A/RES/79/325), 2025 p. URL: https://docs.un.org/en/A/RES/79/325

157. Resolution on the Collection, Use and Disclosure of Personal Data to Pre-train, Train and Fine-tune AI Models. 47th Global Privacy Assembly, 2025 p. URL:https://globalprivacyassembly.com/wp-content/uploads/2025/10/Resolution-on-the-collection-use-and-disclosure-of-personal-data-to-pre-train-train-and-fine-tune-AI-models.pdf

158. Resolution on Meaningful Human Oversight of Decisions Involving AI Systems». 47th Global Privacy Assembly, 2025 p. URL: https://globalprivacyassembly.com/wp-content/uploads/2025/10/GPA-Resolution-Human-Oversight-of-Automated-Decisions.pdf

159. Joint Statement on Building Trustworthy Data Governance Frameworks to Encourage Development of Innovative and Privacy-protective AI, 47th Global

Privacy Assembly (signing ceremony), 2025. URL: https://www.pcpd.org.hk/english/news_events/media_statements/files/New_JointStatementonDataGovernance_Signed.pdf

160. Global AI Governance Action Plan. Ministry of Foreign Affairs of the People's Republic of China. World Artificial Intelligence Conference, 26 July 2025. URL: https://un.china-mission.gov.cn/eng/zgyw/202507/t20250729_11679232.htm

161. Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework : European Data Protection Board, 2024. URL:https://www.edpb.europa.eu/system/files/2024-07/edpb_statement_202403_dpasroleaiact_en.pdf

162. Посикалюк О. Штучний інтелект і персональні дані: до питання про пошук балансу інтересів. Право України. 2025. Випуск № 7. С. 122-137 URL: https://pravoua.com.ua/storage/files/magazines/files/article-pravo_2025_7-s4398.pdf

163. Гачкевич А. Сірі зони правового регулювання штучного інтелекту та обробки персональних даних. *Ius Modernum*. 2026. № 1. С. URL: https://journals.knute.edu.ua/foreign-trade/article/download/2447/2502/2941

164. Guidelines 01/2022 on data subject rights : Right of access. Version 2.0: adopted on 28 March 2023. European Data Protection Board. URL: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines_en

165. Про уповноваження О. Борнякова на підписання Рамкової конвенції Ради Європи про штучний інтелект і права людини, демократію та верховенство права: Розпорядження Президента України від 12.05.2025 №54/2025-рп. URL: https://zakon.rada.gov.ua/laws/show/54/2025-%D1%80%D0%BF#Text

166. Онищенко В.В. Трансформація контролю за обробкою персональних даних в умовах застосування штучного інтелекту : International scientific conference. Riga, Latvia : Baltija Publishing, 2026. С. 276-280

167. Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the

simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), adopted on 29 June 2026 (Interinstitutional File 2025/0359 (COD)). URL: https://eur-lex.europa.eu/procedure/EN/2025_359

168. Про забезпечення рівних прав та можливостей жінок і чоловіків : Закон України від 08.09.2005 №2866-IV. URL: https://zakon.rada.gov.ua/laws/show/2866-15#Text

169. Про засади запобігання та протидії дискримінації в Україні : Закон України від 06.09.2012 №5207-VI. URL: https://zakon.rada.gov.ua/laws/show/5207-17#Text

170. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

171. Факультативний протокол до Конвенції проти катувань та інших жорстоких, нелюдських або таких, що принижують гідність, видів поводження та покарання : Протокол ООН від 21.07.2006 № 22-V. URL: https://zakon.rada.gov.ua/laws/show/995_f48

172. Лелеченко А.П., нормативно-правове забезпечення діяльності омбудсмана в умовах демократичного врядування. 2025. Інвестиції: практика та досвід. Випуск № 18, С. 192-197 URL: https://www.nayka.com.ua/index.php/investplan/article/view/7487

173. Про внесення змін до структури Секретаріату Уповноваженого Верховної Ради України з прав людини : наказ Уповноваженого Верховної Ради України з прав людини від 03.07.2023 р. № 608/к URL: https://ombudsman.gov.ua/uk/pro-nashu-robotu/struktura-sekretariatu

174. Звіт за результатами оцінки спроможності Уповноваженого Верховної Ради України з прав людини : ENNHRI, УВКПЛ, ПРООН. 2023 URL: https://ennhri.org/wp-content/uploads/2023/12/Capacity-assessment-of-Ukrainian-Parliament-Commissioner-for-Human-Rights-report-in-UKR.pdf

175. Світличний В. А. Захист персональних даних в умовах воєнного стану в Україні. Право і безпека. 2023. № 3 (90). С. 226-236

URL:https://dspace.univd.edu.ua/server/api/core/bitstreams/9917684f-5a39-466e-9cff-dc4a0b5681de/content

176. Наймасштабніша кібератака на державні реєстри України: зупинено роботу систем Мін'юсту : Українська правда, 2024. URL:https://www.pravda.com.ua/news/2024/12/20/7489933/

177. Truth Beneath Silence: Russia's Weaponisation of Sexual Violence Against Men in Ukraine : Truth Hounds Report, 2026. https://truth-hounds.org/wp-content/uploads/2026/06/truth-beneath-silence-russias-weaponisation-of-sexual-violence-against-men-in-ukraine.pdf

178. Посібник з європейського права у сфері захисту персональних даних: К. 2020. 436 с. URL: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_ukr.pdf

179. Про внесення змін до Закону України «Про захист персональних даних» : Проєкт Закону України від 25.10.2022 року № 8153. URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1517426

180. Про Військового омбудсмана. Закон України від 17.09.2025 № 4603-IX. URL: https://zakon.rada.gov.ua/laws/show/4603-20#Text

181. Проєкт Керівних принципів щодо класифікації систем штучного інтелекту високого ризику : Рада Європи, 2026. URL: https://ec.europa.eu/newsroom/dae/redirection/document/128561

182. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання та захисту прав і свобод людини і громадянина в Україні за 2014 рік. Київ, 2015. С. 538

183. Ігнатченко І.Г., Рябченко Я.С. Адміністративно-правовий захист персональних даних дитини в соціально-гуманітарній сфері цифрової держави. Актуальні дослідження правової та історичної науки. Випуск 77: матеріали Міжнародної конференції, 2025, С. 23-34. URL: https://www.lex-line.com.ua/data/downloads/file_1768127656.pdf#page=12

184. Брижко В. М. (2016). Сучасні основи захисту персональних даних в Європейських правових актах. *Інформація і право*, 3 (18), 45–57. URL: http://ippi.org.ua/sites/default/files/8_1.pdf

185. Явор О.А., Піддубна В.Ф., Рубан О.О. Правові проблеми захисту персональних даних неповнолітніх осіб відповідно до вимог вітчизняного законодавства та вимог GDPR ScienceRise. Juridical Science. 2023. № 3. С. 23–34. URL: http://nbuv.gov.ua/UJRN/srjusc_2023_3_6

186. Цивільний процесуальний кодекс України Кодекс України; Кодекс, Закон від 18.03.2004 № 1618-IV. URL: https://zakon.rada.gov.ua/laws/show/1618-15#Text

187. Онищенко В.В. Право дитини на приватність у діяльності медіа: співвідношення свободи вираження поглядів та принципу забезпечення якнайкращих інтересів дитини. *Правові новели*. 2025. Випуск № 27. С. 401-411 URL: https://legalnovels.in.ua/journal/27_2025/27_2025.pdf

188. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2025 році. URL: https://www.ombudsman.gov.ua/storage/app/media/uploaded-files/Щорічна_доповідь_Уповноваженого_у_ 2025_році.pdf

189. Захист особистого життя і персональних даних в Інтернеті і ЗМІ : Резолюція Парламентської асамблеї Ради Європи 1843, 2011 р. URL: https://pace.coe.int/en/files/18018

190. Report to the Ukrainian Government on the visit to Ukraine carried out by the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT) from 8 to 21 December 2017. URL: https://rm.coe.int/16808d2c2a

191. Постанова Верховного Суду від 19.09.2018 у справі № 806/3265/17. URL: https://reyestr.court.gov.ua/Review/76822787

192. Рекомендації для медіаспільноти щодо захисту персональних даних під час публікації фото- та відеоматеріалів у журналістських розслідуваннях.

Секретаріат Уповноваженого Верховної Ради України з прав людини, 2026. URL:https://www.ombudsman.gov.ua/storage/app/media/uploaded-files/1-28012026-1609-rekomendatsii-dlya-mediaspilnoti.pdf

193. Принципи та керівні вказівки для ЗМІ, які висвітлюють проблеми дітей. Дитячий фонд ООН (ЮНІСЕФ) в Україні. URL: https://www.unicef.org/ukraine/guidelines-journalists-reporting-children

194. Рекомендація Rec (2018) 7 Комітету Міністрів Ради Європи державам-членам про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі. URL: https://www.coe.int/en/web/children/-/new-recommendation-adopted-on-children-s-rights-in-the-digital-environment

195. M.L. and W.W. v. Germany, рішення Великої палати Європейського суду з прав людини URL:https://hudoc.echr.coe.int/eng?i=002-12041

196. Proposal for a Regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act) : COM(2026) 502 final, 2026/0138 (COD) від 03.06.2026. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52026PC0502

197. Case of Von Hannover v. Germany, рішення Великої палати Європейського суду з прав людини від 07.02.2012 р. URL: https://hudoc.echr.coe.int/eng?i=001-109029

198. Case of Axel Springer Ag v. Germany , рішення Великої палати Європейського суду з прав людини від 07.02.2012 р. URL: https://hudoc.echr.coe.int/eng?i=001-109034

199. Свобода вираження поглядів. Міжнародні стандарти, практика Європейського суду з прав людини і національне законодавство України в умовах воєнного стану. Огляд правових підходів. Серія: Свобода слова і національна безпека. Київ: УНЦПД, 2022. 25 с.

200. Radio Free, Відеоматеріал, 2024. «Насильство над дітьми в евакуйованому дитбудинку. Розслідування Радіо Свобода». URL: https://www.youtube.com/watch?v=FuWGbfFV7Ik

201. Конвенція ООН про права дитини від 20 листопада 1989 р. URL: https://zakon.rada.gov.ua/laws/show/995_021#Text

202. Рекомендації для журналістів щодо роботи з соціально вразливими групами. Діти в медіа : 1+1 media, ГО «Української мережі за права дитини», МБО «Благодійний фонд «СОС дитяче містечко», ГО «Соціальна синергія», Українська фундація громадського здоров'я. URL: https://sos-ukraine.org/wp-content/uploads/2022/05/rekomendacii_dla_zhurnalistiv_dity_v_media.pdf

203. BBC Editorial Guidelines : British Broadcasting Corporation. URL: https://www.bbc.com/editorialguidelines

203. Рада звільнила Денісову з посади омбудсмена. Радіо Свобода: Стаття, 2022. URL: https://www.radiosvoboda.org/a/news-rada-ombudsmen-denisova-vidstavka/31876755.html

204. Про висловлення недовіри Уповноваженому Верховної Ради України з прав людини Денісовій Л.Л. : Постанова Верховної Ради України від 31.05.2022 № 2294-IX URL: https://zakon.rada.gov.ua/laws/show/2294-20#Text

ДОДАТКИ

Додаток А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ:

1. Онищенко В.В. Право дитини на приватність у діяльності медіа: співвідношення свободи вираження поглядів та принципу забезпечення якнайкращих інтересів дитини. *Правові новели*. 2025. Випуск № 27. С. 401-411 URL.: https://legalnovels.in.ua/journal/27_2025/27_2025.pdf

2. Онищенко В.В. Контроль за обробкою персональних даних та адміністративна відповідальність за порушення законодавства про захист персональних даних в умовах війни. *Юридичний науковий електронний журнал*. 2025. №12. С. 524-527

3. Онищенко В.В. Проблемні аспекти інформаційного законодавства України: поширення інформації про померлого. *Юридичний науковий електронний журнал*. 2023. №6. С. 674-677

4. Потіп М. М., Онищенко В. В. Обробка персональних даних в умовах воєнного стану. Молодь: наука та інновації : матеріали XII *Міжнародної науково-технічної конференції студентів, аспірантів та молодих вчених*. Дніпро : НТУ «Дніпровська політехніка», 2024. С. 171–172.

5. Онищенко В.В. Трансформація контролю за обробкою персональних даних в умовах застосування штучного інтелекту : *International scientific conference*. Riga, Latvia : Baltija Publishing, 2026. С. 276-280

Додаток Б

Таблиця оцінки ефективності наглядового органу «Supervisory Effectiveness Index»

Субіндекс	Показники	Україна (Омбудсман)	GDPR / DPA-ЄС	США (FTC)	КНР (CAC)
Незалежність	Гарантії незалежності, строкові мандати, бюджетна автономія	4/10 (формально незалежний, система ВРУ, процедура непрозорого звільнення в умовах воєнного стану	9/10 (гарантії, визначені у ст. 52 GDPR)	4/10 (формально незалежний, призначає Президент, процедура непрозорого звільнення)	2/10 (підпорядкований Партії; відсутні гарантії незалежності)
Обсяг повноважень	Розслідувальні, коригувальні, дорадчі; право доступу, право видачі приписів	6/10 (розслідувальні і дорадчі; коригувальні, санкційні потребують удосконалення)	9 / 10 – ст. 58 GDPR: повний спектр із правом прямих штрафів	6/10 – прямих штрафів за первинне порушення немає	8/10 – широкі, включно з блокуванням без рішення суду
Санкційна спроможність	Право прямого накладення штрафу; диференціація санкцій;	4/10 (лише складення протоколу суд; макс. 2000 НМДГ)	10/10 (до €20 млн або 4% обороту; прямо; без суду	6/10 – $5 млрд за consent decree порушення	6/10 – до 50 млн CNY або 5% обороту;

	максимальний розмір			; 0 за первинне	прямо САС
Рівень виконання рішень	% рішень, що виконуються добровільно або примусово	3/10 (приписи ігноруються; 77% протоколів не дають стягнення,)	8/10 (публічність рішень, репутаційний ефект)	6/10 (наказ про згоду сторін, з моніторингом)	7/10 (державний примус)
Превентивна функція	Privacy by Design, реєстр обробки підвищеного ризику	3/10 (повідомлення про обробку; оцінка впливу відсутня)	9/10 (оцінка впливу; Privacy by Design; реєстр)	4/10 (оцінка впливу відсутня)	5/10 (процедура оцінки впливу опціональна)
Загальний показник	**Середній бал**	**4,0/10**	**9,0/10**	**5,0/10**	**5,6/10**

Додаток В

Проєкт вноситься народними депутатами України

ЗАКОН УКРАЇНИ

«Про внесення змін до деяких законодавчих актів України щодо посилення захисту персональних даних дитини»

Верховна Рада України постановляє:

Розділ І. Зміни до Закону України «Про медіа»

1. Доповнити Закон України «Про медіа» статтею 36-1 такого змісту:

«Стаття 36-1. Особливості поширення персональних даних дитини

1. Поширення суб'єктами у сфері медіа персональних даних дитини, що дозволяють або можуть дозволити її ідентифікацію (далі – ідентифікуючі дані дитини), здійснюється з дотриманням принципу найкращих інтересів дитини та презумпції нерозкриття ідентифікуючих даних дитини.

2. Згода дитини та/або її батьків чи інших законних представників на поширення персональних даних дитини не є самостійною та достатньою правовою підставою для поширення ідентифікуючих даних дитини. Така згода оцінюється у сукупності з вимогами, передбаченими частиною третьою цієї статті.

3. Поширення ідентифікуючих даних дитини допускається лише за умови одночасного дотримання таких вимог (тест пропорційності поширення персональних даних дитини):

1) поширення переслідує легітимну суспільно значущу мету, зокрема виявлення системних порушень прав людини, насильства, недбалості чи зловживань, забезпечення публічного контролю за діяльністю органів влади або захист самої дитини; сенсаційний характер інформації або значний суспільний інтерес самі по собі такою метою не є;

2) досягнення мети, передбаченої пунктом 1 цієї частини, є об’єктивно неможливим без розкриття ідентифікуючих даних дитини, зокрема шляхом знеособлення (анонімізації), узагальнення відомостей, залучення експертних коментарів замість безпосередньої участі дитини, оприлюднення документів, статистичних чи знеособлених даних;

3) поширення не суперечить найкращим інтересам дитини та не створює для неї ризику шкоди, зокрема ретравматизації, стигматизації, дискримінації, втрати контролю над інформацією про себе, загрози безпеці дитини або членів її сім’ї;

4) суспільний інтерес у поширенні ідентифікуючих даних дитини переважає потенційну шкоду її правам, свободам та найкращим інтересам; у разі рівнозначності або переважання шкоди поширення ідентифікуючих даних дитини не допускається;

5) враховано незворотний характер наслідків поширення, зокрема довготривале збереження інформації в інформаційно-комунікаційних системах та її вплив на подальше життя, розвиток, соціалізацію і репутацію дитини; за наявності ризику настання незворотних наслідків поширення ідентифікуючих даних дитини не допускається, якщо мету може бути досягнуто в інший спосіб.

4. Незалежно від наявності згоди забороняється:

1) поширення ідентифікуючих даних дитини, отриманих із застосуванням прихованих методів збору інформації, тиску на дитину або маніпуляцій з метою їх отримання;

2) поширення інформації про дитину у формі та спосіб, що призводять до повторного переживання дитиною травматичних подій (ретравматизації), у тому числі під час роботи з дитиною у форматі інтерв’ю;

3) умисне поширення персональних даних, які, попри умовне знеособлення дитини, дозволяють її ідентифікувати;

4) поширення ідентифікуючих даних дитини, яка зазнала фізичного чи сексуального насильства, задіяна у провадженні у справах про адміністративні

правопорушення або у кримінальному провадженні у будь-якому статусі, а також інформації, що стосується факту самогубства дитини та ідентифікує її, – крім виняткових випадків, коли інакше неможливо забезпечити найкращі інтереси дитини і дотримано вимоги частини третьої цієї статті.

5. Перед поширенням ідентифікуючих даних дитини суб'єкт у сфері медіа зобов'язаний:

1) запровадити та застосовувати внутрішні редакційні політики взаємодії та роботи з дітьми (процедури захисту дитини, child safeguarding), забезпечити навчання працівників і обов'язкове залучення психолога або соціального педагога до взаємодії з дитиною, зокрема у формі інтерв'ю;

2) забезпечити посилений редакційний контроль і, за можливості, залучення експертів у сфері захисту прав дитини, у тому числі з числа представників неурядового сектору, для оцінки ризиків порушення прав дитини внаслідок поширення;

3) задокументувати проходження тесту, передбаченого частиною третьою цієї статті, та зберігати відповідні матеріали впродовж строку, визначеного Національною радою України з питань телебачення і радіомовлення спільно з органом спільного регулювання.».

2. У статті 110 «Відповідальність суб'єктів у сфері аудіовізуальних медіа»:

1) виключити з частини десятої (значні порушення) пункт, що передбачає відповідальність за розголошення інформації про дитину без письмової згоди хоча б одного з батьків або інших законних представників (пункт 11 частини десятої статті 110);

2) доповнити частину четверту (грубі порушення) новим пунктом такого змісту: «поширення персональних даних дитини з порушенням вимог статті 36-1 цього Закону».

3. Внести аналогічні зміни до статей 111, 112 і 113 цього Закону в частині встановлення відповідальності медіа, онлайн-медіа та провайдерів

аудіовізуальних сервісів за порушення вимог статті 36-1 як за грубе порушення.

Розділ ІІ. Зміни до Закону України «Про охорону дитинства»

1. Статтю 10 Закону України «Про охорону дитинства» доповнити частинами такого змісту:

«Кожна дитина має право на захист своїх персональних даних від надмірного розкриття. Поширення персональних даних дитини, що дозволяють або можуть дозволити її ідентифікацію, здійснюється на засаді презумпції нерозкриття ідентифікуючої інформації дитини та з пріоритетом найкращих інтересів дитини.

Згода законного представника дитини не є самостійною та достатньою правовою підставою для поширення ідентифікуючих даних дитини. Допустимість такого поширення визначається за результатами тесту пропорційності поширення персональних даних дитини, передбаченого законом.

Положення цієї статті застосовуються незалежно від сфери та способу поширення інформації, у тому числі у медіа, мережі Інтернет та інших публічних інформаційних ресурсах.».

Розділ ІІІ. Прикінцеві положення

1. Цей Закон набирає чинності з дня, наступного за днем його опублікування, та вводиться в дію через три місяці з дня набрання чинності.

2. Національній раді України з питань телебачення і радіомовлення спільно з органами спільного регулювання у тримісячний строк затвердити критерії застосування тесту пропорційності поширення персональних даних дитини та методичні рекомендації щодо процедур захисту дитини (child safeguarding).

3. Кабінету Міністрів України привести свої нормативно-правові акти у відповідність із цим Законом.

Голова Верховної Ради України _____

ПОЯСНЮВАЛЬНА ЗАПИСКА
до проєкту Закону України «Про внесення змін до деяких законодавчих актів України щодо посилення захисту персональних даних дитини»

1. Обґрунтування необхідності прийняття законопроєкту

Необхідність прийняття цього проєкту Закону обумовлена тим, що чинне законодавство не забезпечує належного рівня захисту персональних даних дитини під час їх поширення у медіа та публічному просторі.

Допустимість поширення інформації про дитину пов’язується насамперед із наявністю згоди законного представника (стаття 10 Закону України «Про охорону дитинства»; частина десята статті 36 Закону України «Про медіа»), тоді як така згода не гарантує дотримання найкращих інтересів дитини та не враховує знижену здатність дитини усвідомлювати наслідки поширення.

Загальний «трискладовий тест» (частина друга статті 6 Закону України «Про доступ до публічної інформації») сконструйований для вирішення спору про доступ до інформації і не є достатнім для дітей.

Він виявляє щонайменше п’ять структурних дефіцитів: розрахований на логіку відмови розпорядника у доступі, а не на самостійне поширення поширювачем чутливих даних вразливого суб’єкта; припускає звичайний рівень автономії суб’єкта даних; не містить наскрізного фільтра найкращих інтересів дитини як пріоритетного міркування; оцінює шкоду станом на момент розголошення, ігноруючи незворотність цифрового сліду; розглядає згоду представника як достатню підставу, тоді як для дітей вона ненадійна.

Запропоноване регулювання узгоджується з міжнародними стандартами: статтями 3, 16, 19 і 39 Конвенції ООН про права дитини; статтею 8 Конвенції про захист прав людини і основоположних свобод та практикою Європейського суду з прав людини щодо балансування свободи вираження поглядів і права на приватність (Von Hannover v. Germany, Axel Springer AG v.

Germany, M.L. and W.W. v. Germany); пунктами 38 і 75 преамбули та статтею 85 Загального регламенту про захист даних (ЄС) 2016/679; Керівними принципами Комітету міністрів Ради Європи щодо захисту прав дітей у цифровому середовищі; модернізованою Конвенцією Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108+).

Прийняття законопроєкту відповідає курсу на наближення законодавства України до стандартів Європейського Союзу та Ради Європи у сфері захисту персональних даних і сприяє виконанню євроінтеграційних зобов'язань України, зокрема в межах Стратегії інтеграції України до Єдиного цифрового ринку Європейського Союзу («Дорожня карта»).

2. Проблема, яка потребує розв'язання

Головна проблема полягає у відсутності спеціального правового стандарту поширення персональних даних дитини, який враховував би її підвищену вразливість. Згода законного представника часто має номінальний характер, а в системі інституційного догляду супроводжується конфліктом інтересів: керівник закладу одночасно виконує функції законного представника дитини, на дії закладу щодо якої може знадобитися скаржитися. На таку проблему неодноразово звертали увагу Уповноважений Верховної Ради України з прав людини (щорічні доповіді за 2024 і 2025 роки) та Європейський комітет із запобігання катуванням.

Чинне регулювання не містить механізму перевірки того, чи є розкриття саме ідентифікуючих даних необхідним, чи є воно пропорційним і якими будуть незворотні наслідки поширення. Як наслідок, поширення ідентифікуючих даних дитини відбувається без послідовної оцінки, що створює ризики ретравматизації, стигматизації та дискримінації, втрати контролю над інформацією, а також загрози безпеці дитини та її родини, які особливо зростають в умовах збройного конфлікту та вимушеного переміщення дітей.

Окремою проблемою є хибне сприйняття суспільного інтересу або згоди законного представника як самодостатньої підстави для поширення, що не враховує специфіки правового статусу дитини, її вразливості та обмеженої здатності усвідомлювати наслідки прийнятих рішень.

3. Цілі та завдання проєкту

Метою проєкту Закону є запровадження спеціального правового стандарту поширення персональних даних дитини – тесту пропорційності, заснованого на презумпції нерозкриття ідентифікуючої інформації та пріоритеті найкращих інтересів дитини, з одночасним посиленням відповідальності суб'єктів у сфері медіа та запровадженням редакційних процедур захисту дитини.

Законопроєкт передбачає:

закріплення презумпції нерозкриття ідентифікуючих даних дитини та правила, за яким згода представника не є самостійною та достатньою правовою підставою для їх поширення;

запровадження тесту пропорційності поширення персональних даних дитини з п'яти послідовних елементів – легітимна суспільно значуща мета, необхідність розкриття саме ідентифікуючих даних, оцінка шкоди найкращим інтересам дитини, перевага суспільного інтересу над приватністю та критерій незворотності наслідків;

встановлення абсолютних заборон, що діють незалежно від згоди (ретравматизація, приховані методи збору, тиск і маніпуляції, умисна ідентифікація попри знеособлення);

запровадження обов'язкових редакційних процедур захисту дитини (child safeguarding), посиленого редакційного контролю та залучення фахівців;

посилення відповідальності шляхом переведення відповідного порушення з категорії значного до категорії грубого порушення законодавства у сфері медіа;

закріплення у Законі України «Про охорону дитинства» права дитини на захист від надмірного розкриття персональних даних.

4. Загальна характеристика і основні положення проєкту

Проєкт Закону складається з трьох розділів і вносить зміни до Закону України «Про медіа» та Закону України «Про охорону дитинства».

Розділ I доповнює Закон України «Про медіа» статтею 36-1, яка закріплює презумпцію нерозкриття ідентифікуючих даних дитини, встановлює, що згода не є самостійною підставою їх поширення, та запроваджує кумулятивний тест пропорційності, абсолютні заборони і обов'язки суб'єктів медіа щодо процедур захисту дитини. Розділ I також переводить поширення персональних даних дитини з порушенням нових вимог із категорії значного до категорії грубого порушення (зміни до статей 110–113).

Розділ II доповнює статтю 10 Закону України «Про охорону дитинства» правом дитини на захист від надмірного розкриття персональних даних та загальною презумпцією нерозкриття ідентифікуючої інформації, що застосовується незалежно від сфери та способу поширення. Розділ III визначає порядок набрання чинності та доручення Національній раді й Кабінету Міністрів України. Концептуально проєкт відповідає на три ключові питання правозастосування. По-перше, суспільний інтерес може виправдовувати розкриття персональних даних дитини лише як виняток і за умови проходження тесту. Належність інформації до сфери суспільного інтересу сама по собі не легітимізує розкриття, якщо мети можна досягти знеособлено або якщо шкода переважає користь; суспільну значущість слід відмежовувати від сенсаційності, а найкращі інтереси дитини є пріоритетним міркуванням. По-друге, баланс між свободою вираження поглядів і правом дитини на приватність вирішується на користь підвищеного захисту дитини: свобода вираження поглядів не є абсолютною та підлягає обмеженню для захисту прав інших осіб, а право дитини на приватність має пріоритет над інтересом публічності, тому ідентифікація дитини розглядається як виняток. По-третє, регулятор (Національна рада України з питань телебачення і радіомовлення) або суд застосовує тест пропорційності, послідовно перевіряючи легітимну

суспільно значущу мету, необхідність розкриття саме ідентифікуючих даних, ризик шкоди найкращим інтересам дитини, перевагу суспільного інтересу над приватністю та незворотність наслідків, а також спосіб отримання інформації і форму її подання; тягар доведення допустимості поширення покладається на поширювача.

Примітка щодо законодавчої техніки. Конкретні номери частин і пунктів статей 110–113 Закону України «Про медіа» підлягають синхронізації з чинною консолідованою редакцією на дату внесення проєкту.

5. Фінансово-економічне обґрунтування

Реалізація проєкту Закону не потребує додаткових видатків з Державного бюджету України. Затвердження критеріїв застосування тесту та методичних рекомендацій щодо процедур захисту дитини здійснюється в межах повноважень і коштів Національної ради України з питань телебачення і радіомовлення. Запровадження редакційних процедур захисту дитини покладається на суб’єктів у сфері медіа та забезпечується за рахунок їхніх власних коштів.

6. Прогноз впливу

Прийняття проєкту Закону забезпечить зниження ризиків ретравматизації, стигматизації та довготривалої шкоди дітям внаслідок поширення їхніх персональних даних; перетворення принципу найкращих інтересів дитини з декларативного орієнтира на практичний інструмент прийняття редакційних рішень; підвищення передбачуваності правозастосування для суб’єктів медіа та регулятора; формування відповідальної журналістської практики щодо дітей. Законопроєкт сприятиме наближенню законодавства України до стандартів Європейського Союзу та Ради Європи і виконанню євроінтеграційних зобов’язань України у сфері захисту персональних даних.

7. Підстава розроблення проєкту акта

Проєкт акта розроблено в порядку реалізації права законодавчої ініціативи народних депутатів України на виконання статті 32 Конституції

України, з урахуванням Конвенції ООН про права дитини (статті 3, 16, 19, 39), статті 8 Конвенції про захист прав людини і основоположних свобод [19], зобов'язань України за Угодою про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, а також Стратегії інтеграції України до Єдиного цифрового ринку Європейського Союзу («Дорожня карта») та модернізованої Конвенції 108+.

Народні депутати України _____