КОЛОТИЛО М. Ю.,
аспірант кафедри конституційного
та адміністративного права
(Запорізький національний університет),
помічник директора
(ПАТ «Укрнафта»)

УДК 342.9:351.751(477)
DOI https://doi.org/10.32842/2078-3736/2025.2.32

ГЕНЕЗИС ПРАВОВОГО РЕГУЛЮВАННЯ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ: АДМІНІСТРАТИВНО-ПРАВОВІ АСПЕКТИ

У дослідженні представлено всебічний ретроспективний огляд еволюції нормативно-правового поля захисту персональних даних на території України. Висвітлено періодизацію та ключові віхи формування законодавчого підґрунтя у царині охорони персоніфікованої інформації, з акцентом на визначальних правових документах, що заклали фундамент для розбудови адміністративно-правової системи захисту даних особистого характеру. Автори визначають динаміку трансформації інституційних механізмів та адміністративних структур для забезпечення належного рівня захисту персональних даних громадян. Простежено імплементацію міжнародних стандартів та інкорпорацію європейських правових норм у вітчизняне законодавство.

Особливу увагу приділено аналізу впливу таких міжнародно-правових актів, як Конвенція Ради Європи №108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних», Директива ЄС 95/46/ЕС та Загального регламенту про захист даних (GDPR), на національну правову політику. Показано, яким чином європейські імперативи поступово трансформували зміст адміністративно-правового регулювання в Україні та актуалізували потребу у вдосконаленні механізмів нагляду, контролю та відповідальності у сфері обробки персональних даних.

Окреслено проблематику розбалансованості нормативного забезпечення та фрагментарності правозастосовної практики, а також підкреслено необхідність гармонізації підходів до адміністративного захисту персональних даних з урахуванням засад верховенства права, пропорційності та належного врядування. У контексті процесів діджиталізації суспільства і розширення використання цифрових технологій розглянуто ризики, пов'язані з обробкою великих масивів персональної інформації, використанням алгоритмів штучного інтелекту, та зростаючою роллю кібербезпеки.

Автори пропонують системний підхід до подальшої модернізації законодавства з урахуванням практики Європейського суду з прав людини, позицій науковців і рекомендацій європейських інституцій. Розкрито стратегічні напрями розвитку державної політики у сфері захисту персональних даних як складової частини адміністративно-правового забезпечення прав і свобод людини в умовах євроінтеграційного поступу України.

Ключові слова: *персональні дані, захист інформації, генезис законодавства, адміністративно-правове регулювання, суб'єкти владних повноважень, відповідальність за порушення, євроінтеграція.*

Kolotylo M. Yu. Genesis of legal regulation of personal data in Ukraine: administrative and legal aspects

The study provides a comprehensive retrospective review of the evolution of the legal framework for personal data protection in Ukraine. The periodisation and key milestones in the formation of the legislative framework in the field of personalised information protection are highlighted, with a focus on the key legal documents that laid the foundation for the development of the administrative and legal system of personal data protection. The authors determine the dynamics of transformation of institutional mechanisms and administrative structures to ensure an adequate level of protection of personal data of citizens. The implementation of international standards and the incorporation of European legal norms into national legislation are traced.

Particular attention is paid to the analysis of the impact of international legal acts such as the Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, EU Directive 95/46/EC and the General Data Protection Regulation (GDPR) on national legal policy. The author shows how European imperatives have gradually transformed the content of administrative and legal regulation in Ukraine and have highlighted the need to improve the mechanisms of supervision, control and liability in the field of personal data processing.

The author outlines the issues of imbalance in regulatory support and fragmentation of law enforcement practice, and emphasises the need to harmonise approaches to administrative protection of personal data with due regard for the rule of law, proportionality and good governance. In the context of the digitalisation of society and the expanding use of digital technologies, the risks associated with the processing of large amounts of personal information, the use of artificial intelligence algorithms, and the growing role of cybersecurity are considered.

The authors propose a systematic approach to further modernisation of legislation, taking into account the case law of the European Court of Human Rights, the positions of scholars and recommendations of European institutions. The article reveals the strategic directions of development of the state policy in the field of personal data protection as an integral part of administrative and legal support for human rights and freedoms in the context of Ukraine's European integration.

Key words: *personal data, information protection, genesis of legislation, administrative and legal regulation, subjects of authority, liability for violations, European integration.*

Вступ. Належна охорона персоніфікованої інформації громадян виступає фундаментальним компонентом правової державності та життєздатного громадянського суспільства. В умовах експоненційного прогресу цифрових екосистем і трансформаційних процесів глобалізації проблематика адекватної нормативно-правової регламентації персональних даних набуває виняткової актуальності. Масиви індивідуалізованої інформації, що підлягають обробці, демонструють тенденцію до невпинного розширення, а механізми їх опрацювання характеризуються прогресуючою комплексністю, що обумовлює запит на впровадження релевантних юридичних та інституційних інструментів забезпечення захисту.

Генеза правового регулювання сфери персональних даних на теренах України відзначалася поетапністю та враховувала як загальнопланетарні тренди, так і особливості вітчизняного правового ландшафту. Ретроспективне дослідження еволюційної траєкторії нормативної регуляції даної царини в адміністративно-правовому вимірі сприяє поглибленому осмисленню її сьогоденного стану, уможливлює ідентифікацію стрижневих викликів та окреслення векторів наступної оптимізації.

Постановка завдання. Пріоритетна ціль представленого дослідження полягає у здійсненні комплексної аналітичної реконструкції процесу формування та подальшої еволюції адміністративно-правового інструментарію регулювання персональних даних в українському правовому полі, виокремленні його магістральних історичних фаз, характеристиці юридичних та інституційних механізмів захисту, а також прогностичному моделюванні перспектив модернізації законодавчого забезпечення цієї сфери.

Результати дослідження. Розгляд еволюційних процесів у сфері правової регламентації персональних даних насамперед потребує концептуальної конкретизації термінологічного апарату досліджуваної проблематики. Відповідно до Закону України «Про захист персональних даних», персональні дані визначаються як інформація, що дозволяє ідентифікувати фізичну особу [1]. Таке дефінітивне трактування корелює з загальновизнаними міжнародними нормативними стандартами, зокрема з положеннями Конвенції Ради Європи щодо захисту осіб у контексті автоматизованої обробки персональних даних.

Архітектоніка правового регулювання персональних даних інтегрує комплексний масив нормативно-правових актів, що детермінують алгоритми збору, опрацювання та депонування таких даних, встановлюють юридичний статус їхніх суб'єктів, окреслюють коло зобов'язань розпорядників і володільців, а також регламентують інструментарій контролю й юридичної відповідальності за порушення встановлених правових норм у даній царині.

Адміністративно-правовий вимір регулювання персональних даних охоплює організаційно-функціональні засади діяльності державних інституцій у відповідній сфері, процедурний порядок реєстрації баз персональних даних, контрольно-наглядові механізми за дотриманням легітимних нормативів, а також юридичні аспекти адміністративної відповідальності за їх порушення.

У науковому дискурсі, зокрема в інтерпретації І. В. Ковбаса, «адміністративно-правове регулювання захисту персональних даних доцільно розглядати як спеціалізований правовий механізм, призначений для гарантування недоторканності приватного життя осіб і реалізації їхнього права на інформаційне самовизначення шляхом встановлення регуляторних правил обробки персональних даних, імплементації контролю за їх дотриманням і застосування відповідних санкцій за порушення» [2, с. 74–78]. Даний концептуальний підхід уможливлює холістичне осмислення системи правового регулювання персональних даних крізь методологічну призму адміністративного права.

Історіографія правового регулювання персональних даних на теренах України піддається умовній періодизації з виокремленням декількох хронологічних етапів, кожен з яких характеризується специфічними особливостями у площині нормативно-правового забезпечення та інституційних механізмів захисту персоніфікованої інформації.

Ініціальний етап формування правового регулювання персональних даних бере свій початок після прокламації незалежності України у 1991 році. У цей часовий проміжок домінуючий акцент був зосереджений на конституюванні фундаментальних принципів інформаційного законодавства, однак спеціалізовані нормативно-правові акти, що безпосередньо регламентували б захист персональних даних, все ще перебували у стадії концептуального опрацювання.

Парадигмальними документами цього хронологічного періоду стали Закон України «Про інформацію» від 2 жовтня 1992 року та Конституція України від 28 червня 1996 року. Зокрема, стаття 32 Основного Закону імплементувала положення про те, що жодна особа не може підлягати інтервенції у її приватно-сімейну сферу, за винятком казуїстичних випадків, експліцитно передбачених Конституцією. Паралельно було запроваджено імперативну заборону на акумуляцію, зберігання, використання та дисемінацію конфіденційних відомостей про особу за відсутності її вербалізованої згоди [3].

У нормативному полі Закону України «Про інформацію» вперше було інкорпоровано поняття «інформація про фізичну особу», що стало семантичним прекурсором сучасної дефініції терміну «персональні дані». Даний законодавчий акт також артикулював загальні принципи оперування особистісною інформацією [4].

Важливою віхою у розвитку національного законодавства стало офіційне приєднання України у 2005 році до Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року [5]. Цей міжнародно-правовий документ заклав базові основи для подальшого розвитку національної нормативно-правової бази у сфері захисту персональних даних.

Утім, попри наявність сингулярних законодавчих постулатів, орієнтованих на забезпечення охорони інформації про особу, цей хронологічний період характеризувався дефіцитом спеціалізованого законодавства та релевантних інституційних механізмів гарантування захисту персональних даних, що демонструвало дисонанс із загальноприйнятими міжнародними нормативами.

Другий етап еволюційного розвитку правової регламентації персональних даних на теренах України ознаменувався прийняттям 1 червня 2010 року Закону України «Про захист персональних даних», що набув легітимної сили 1 січня 2011 року [1]. Даний нормативно-правовий акт постав першим вузькоспеціалізованим законом, котрий комплексно регулював проблематику захисту персональних даних в українському правовому полі, детермінуючи юридичні принципи їхньої обробки та захисту.

Законодавчий текст надав основні визначення персональних даних, інфраструктури персональних даних, володільця персональних даних, контролера персональних даних та суб'єкта персональних даних. Регламент інституціоналізував основні принципи та умови обробки персональних даних, уточнив обсяг повноважень суб'єкта персональних даних, окреслив коло обов'язків володільця та розпорядника, а також передбачив нормативний механізм державного контролю за дотриманням вимог законодавства у цій сфері.

Одним із ключових нововведень стало створення спеціалізованого державного органу, відповідального за захист персональних даних. Відповідно до первинної редакції Закону України «Про захист персональних даних», таким регуляторним органом було визначено Державну службу України з питань захисту персональних даних, засновану на підставі Указу Президента України від 9 грудня 2010 року [6].

Ця інституція відповідала за ведення Національного реєстру персональних даних, розгляд скарг щодо можливих порушень у сфері захисту персональної інформації, проведення адміністративних і наглядових перевірок діяльності володільців і розпорядників персональних даних, а також за надання роз'яснень і методичних рекомендацій щодо застосування відповідних законодавчих норм.

Паралельно, до Кодексу України про адміністративні правопорушення були інкорпоровані зміни, якими передбачалась адміністративна відповідальність за порушення законодавства про захист персональних даних (стаття 188–39) [7].

Таким чином, другий етап став трансформаційним у процесі становлення системи правового регулювання персональних даних в Україні, оскільки було сформовано спеціальне галузеве законодавство, концептуалізовано базові принципи та механізми їхнього захисту, а також створено профільний державний орган, відповідальний за здійснення контрольно-наглядових функцій у даній сфері.

За цей період набула чинності низка підзаконних актів, що деталізують законодавчі положення Закону України «Про захист персональних даних». Серед ключових документів варто відзначити наступні:

– «Положення про державну реєстрацію баз персональних даних та порядок їх ведення», затверджене Постановою Кабінету Міністрів України № 616 від 25 травня 2011 року [8];

– Розпорядження Комітету з прав людини Верховної Ради України № 1/02-14 від 8 січня 2014 року встановлює «Порядок повідомлення Комітету Верховної Ради України з прав людини про обробку персональних даних, які містять спеціальні ризики для прав і свобод суб'єктів персональних даних». Цей документ був затверджений відповідним Рішенням Комітету Верховної Ради України з прав людини від тієї ж дати – 8 січня 2014 року, № 1/02-14 [9].

Цей етап характеризувався динамічним формуванням спеціалізованого законодавства у сфері захисту персональних даних, а також конституюванням інституційних механізмів, призначених для забезпечення ефективної охорони персоніфікованої інформації громадян. Водночас, практична імплементація виявила суттєві дисфункції, серед яких надмірна бюрократизація процедурних аспектів реєстрації баз персональних даних та інсуфіцієнтність (недостатня ефективність) державного контролю.

Наступний третій етап еволюції правового регулювання персональних даних в Україні розпочався у 2014 році, коли були внесені принципові зміни до механізму інституційного нагляду за дотриманням законодавства у цій сфері: Законом України від 3 липня 2013 року «Про деякі законодавчі акти України щодо удосконалення системи захисту персональних даних. Про внесення змін» функція управління та нагляду була передана від Державної служби України з питань захисту персональних даних до Комітету з прав людини Верховної Ради України [10].

Такий регуляторний підхід демонстрував конвергенцію з європейськими нормативними стандартами, адже у країнах Європейського Союзу функціональні повноваження з контролю за обробкою персональних даних покладаються на незалежні регуляторні органи, часто афілійовані з інститутом омбудсмена. В організаційній структурі Секретаріату Уповноваженого було інституціоналізовано Департамент із питань захисту персональних даних, котрий реалізовував функції моніторингу та нагляду за дотриманням законодавчих норм у даній сфері.

Стрижневою інновацією цього етапу стала елімінація облігаторної реєстрації баз персональних даних, що уможливило суттєву редукцію адміністративно-бюрократичних процедур та мінімізацію регуляторного навантаження на суб'єктів господарювання й інституційні утворення, які здійснюють опрацювання персональних даних. Натомість було імплементовано альтернативний механізм обов'язкової нотифікації Уповноваженого про здійснення операцій з обробки персональних даних, які потенційно можуть генерувати ескалацію ризиків для правових гарантій та свобод громадян.

У цей період також продовжувалася модернізація квазі-правових регуляторних структур. Зокрема, було легалізовано такі нормативно-правові акти, як типовий порядок обробки персональних даних був затверджений Рішенням Комітету з прав людини Верховної Ради України від 8 січня 2014 року № 1/02-14 [11].

Окрім цього, розроблено «Порядок здійснення контролю Комітетом з прав людини Верховної Ради України за дотриманням законодавства у сфері захисту персональних даних» [12], який регламентує механізми та процедури нагляду за виконанням нормативних вимог у цій сфері [12].

Даний період еволюції правової регламентації персональних даних характеризувався трансформацією державних контрольно-наглядових механізмів, спрощенням адміністративно-процедурних алгоритмів та поступовою конвергенцією національного законодавства з європейськими нормативними канонами й стандартами.

Четвертий етап правової регуляції захисту персональних даних в українському правовому полі започаткувався у 2018 році, синхронно з набуттям юридичної сили в країнах Європейського Союзу Загальним регламентом про захист даних (General Data Protection Regulation, GDPR) [13]. Незважаючи на те, що Україна не є інтегрованим членом ЄС, євроінтеграційна траєкторія її державного розвитку та глобалізаційні тенденції у сфері дигітальних технологій актуалізували проблематику гармонізації законодавства до безпрецедентного рівня.

Визначальним імператором у цьому нормотворчому векторі стало парафування Угоди про асоціацію між Україною та Європейським Союзом, котра детермінує, inter alia, зобов'язання української сторони щодо приведення законодавчого корпусу у сфері захисту персональних даних у відповідність до європейських нормативних стандартів [14].

У 2021 році на законотворчому майданчику Верховної Ради було ініційовано проєкт Закону України «Про захист персональних даних» (реєстр. № 5628 від 7 червня 2021 року),

фундаментальна інтенція якого полягала в імплементації положень GDPR у національну правову архітектоніку [15, с. 135–138]. У нормативному документі передбачалися кардинальні трансформації у правовому регулюванні персональних даних, серед яких варто акцентувати увагу на таких:

– Розширення правових можливостей суб'єктів персональних даних, включаючи право на забуття, обмеження обробки та перенесення даних;

– Запровадження ризик-орієнтованого підходу до захисту персональної інформації;

– Встановлення обов'язкової посади спеціаліста із захисту персональних даних у корпоративних структурах та організаціях;

– Посилення юридичної відповідальності за порушення вимог законодавства у сфері персональних даних;

– Чітке врегулювання процедур транскордонної передачі персональних даних.

Цей хронологічний період характеризується динамічними процесами адаптаційної конвергенції національного законодавства до нормативних вимог європейських стандартів, посиленням юридичних гарантій прав суб'єктів персональних даних та ампліфікацією відповідальності операторів, які здійснюють їхню обробку.

Квінтесенційним елементом правового регулювання у сфері персональних даних постає детермінація кола суб'єктів владних прерогатив, які забезпечують контроль за дотриманням відповідного законодавчого масиву. Як було артикульовано раніше, у різні темпоральні періоди еволюції законодавчої інфраструктури ці функціональні обов'язки делегувалися різним державним інституціям.

На сучасному етапі Комітет з прав людини Верховної Ради України відіграє домінуючу роль у системі органів влади, наділених повноваженнями щодо захисту персональних даних. Відповідно до статті 23 Закону України «Про захист персональних даних», Уповноважений з прав людини здійснює різні повноваження, передбачені цим законом.

– прийом та аналіз скарг на порушення законодавства (утиски) у сфері захисту персональних даних;

– імплементує контрольно-верифікаційні заходи стосовно володільців та розпорядників персональних даних як на підставі апеляцій, так і за власною ініціативою;

– валідує нормативно-правові акти, що корелюють із захистом персональних даних;

– оформлює адміністративні протоколи у випадку ідентифікації порушень законодавчих приписів;

– артикулює рекомендації та консультативні роз'яснення щодо правозастосовчої практики у сфері захисту персональних даних;

– реалізує моніторингові заходи щодо дотримання нормативних вимог законодавства про захист персональних даних.

Окрім Уповноваженого Верховної Ради України з прав людини, функціональні обов'язки у цій нормативній сфері виконують також інші державні інституції, серед яких варто диференціювати: • судові органи, які розглядають адміністративно-правові казуси про порушення законодавства щодо захисту персональних даних та апеляційне оскарження рішень, дій чи бездіяльності уповноважених органів; • структурні підрозділи Національної поліції, котрі здійснюють досудове розслідування кримінально-правових деліктів, асоційованих із неправомірним обігом персональних даних; • регуляторні органи в різних секторах, такі як Національний банк України та Державна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, запровадили спеціальні вимоги щодо захисту персональних даних у своїх галузях.

Таким чином, система суб'єктів владно-управлінських прерогатив у сфері захисту персональних даних в українському правовому просторі характеризується багаторівневою структурованістю та інкорпорує як універсальний наглядовий механізм, що реалізується Уповноваженим, так і секторальні регуляторні функції, делеговані спеціалізованим державним органам.

Механізми правового регулювання персональних даних значною мірою визначаються адміністративними процедурами, які формують основу взаємовідносин між різними

учасниками інформаційних правовідносин: суб'єктами персональних даних, їх володільцями, розпорядниками та контролюючими державними органами.

У правовій системі України функціонує низка ключових адміністративних процедур, що спрямовані на забезпечення ефективного захисту персональних даних:

1. Офіційно встановлена процедура інформування Комітету з прав людини Верховної Ради України про обробку персональних даних, що можуть нести підвищені ризики для прав і свобод громадян. Регламентація цієї процедури здійснюється відповідно до Порядку повідомлення, затвердженого наказом Комісії № 1/02-14 від 8 січня 2014 року [9];

2. Комплекс адміністративних заходів, спрямованих на забезпечення дотримання вимог законодавства у сфері персональних даних. До таких заходів належать планові та позапланові перевірки діяльності володільців і розпорядників даних, порядок проведення яких визначено у Порядку здійснення перевірок, затвердженому Наказом Уповноваженого № 1/02-14 від 8 січня 2014 року [12];

3. Механізм розгляду звернень і скарг суб'єктів персональних даних щодо можливих порушень їхніх прав. Нормативне регулювання цієї процедури здійснюється на основі Закону України «Про звернення громадян» [16] у взаємодії з положеннями Закону України «Про захист персональних даних» [1];

4. Визначений порядок застосування адміністративних санкцій у випадку порушення вимог законодавства щодо захисту персональних даних. Відповідні положення закріплені в Кодексі України про адміністративні правопорушення [7] і охоплюють оформлення адміністративних проваджень, судовий розгляд і накладення штрафних санкцій.

Еволюція адміністративних процедур у досліджуваній сфері характеризується переходом від обов'язку реєструвати всі бази персональних даних до вибіркового повідомлення про обробку лише тих даних, які становлять високий ризик. Ця тенденція корелює з європейськими регуляторними стандартами та сприяє оптимізації адміністративного навантаження на операторів, які обробляють персональні дані.

Важливою складовою системи правового регулювання персональних даних є система адміністративної відповідальності за порушення відповідного законодавства. Санкційна частина цієї системи визначена у статтях 188-39 Кодексу України про адміністративні правопорушення [7].

Відповідно до правових норм цих статей, фінансові санкції накладаються за неподання або несвоєчасне подання інформації про обробку персональних даних до Комітету з прав людини Верховної Ради України, а також за неповідомлення про зміну інформації або передачу даних третій особі. Зокрема, для громадян передбачені штрафи від 100 до 500 неоподатковуваних мінімумів доходів громадян, а для посадових осіб та суб'єктів господарювання – більші штрафи від 200 до 1000 неоподатковуваних мінімумів доходів громадян.

Якщо аналогічне правопорушення повторюється протягом року після першого стягнення, штраф значно збільшується. Для громадян – від 200 до 1000 неоподатковуваних мінімумів доходів громадян; для посадових осіб та підприємців – від 400 до 2000 неоподатковуваних мінімумів доходів громадян.

У разі невиконання законних вимог щодо усунення виявлених порушень у сфері захисту персональних даних, до Уповноваженого Верховної Ради України з прав людини або його представника можуть бути застосовані штрафні санкції. Для фізичних осіб розмір штрафу становить від 200 до 500 неоподатковуваних мінімумів доходів громадян, тоді як для посадових осіб та суб'єктів підприємницької діяльності – від 300 до 1000 неоподатковуваних мінімумів.

Порушення законодавства щодо захисту персональних даних, зокрема несанкціонований доступ або інші дії, що обмежують законні права суб'єктів персональних даних, передбачає значні фінансові санкції. Для фізичних осіб штраф може коливатися від 1 до 5 мільйонів доларів США, а для посадових осіб і суб'єктів господарювання – від 3 до 10 мільйонів доларів США.

Аналіз фактичного застосування адміністративно-правових санкцій за порушення Закону «Про захист персональних даних» свідчить про недостатню ефективність цього

механізму правозастосування. Зокрема, існує дисбаланс між розміром штрафів та потенційною шкодою, завданою порушеннями у цій сфері, а процедури притягнення до адміністративної відповідальності характеризуються надмірною забюрократизованістю та тривалими часовими витратами.

В контексті наближення вітчизняної нормативно-правової бази до стандартів Європейського Союзу, особливо актуальним постає питання трансформації інституту адміністративної відповідальності у галузі захисту персональних даних. Комплексна модернізація передбачає суттєве підвищення штрафних санкцій, розширення класифікації адміністративних деліктів та вдосконалення моніторингових процедур щодо дотримання законодавчих приписів.

Фундаментальним вектором реформування правового регулювання інформаційної приватності в українському законодавстві виступає імплементація принципів Загального регламенту про захист даних (GDPR). Цей нормативний акт Європейського Союзу встановлює підвищені вимоги до захисту персональних даних та поширюється не тільки на організації, розташовані в межах ЄС, але й на суб'єкти господарювання поза його територією, якщо вони опрацьовують персональні дані громадян Євросоюзу чи пропонують їм продукцію або послуги [13].

Впровадження положень GDPR у правову систему України забезпечить низку стратегічних переваг: • синхронізацію українського законодавства з європейськими нормативними стандартами; • зміцнення правових гарантій для фізичних осіб при обробці їхніх персональних даних; • формування правових передумов для безперешкодного транскордонного обміну інформацією персонального характеру між Україною та державами-членами ЄС; • зростання конкурентних позицій українських підприємств у європейському економіко-правовому просторі.

Пріоритетні сфери адаптації GDPR у національному законодавстві включають: • якісне розширення правових можливостей фізичних осіб щодо контролю за їхніми персональними даними; • впровадження ризик-орієнтованого підходу при регулюванні відносин у сфері захисту персональної інформації; • нормативне закріплення інституту спеціаліста з питань захисту персональних даних; • кардинальне посилення юридичної відповідальності за правопорушення у досліджуваній сфері; • розробка юридичних механізмів для забезпечення міжнародної передачі персональних даних.

Ключовим елементом оновлення нормативно-правової бази щодо персональних даних в українському правовому полі виступає модернізація інституційної архітектури контролю за їх захистом. Наразі Уповноважений Верховної Ради України з прав людини здійснює наглядову функцію у цій сфері, що відображає європейський принцип незалежності наглядових органів. Проте існуюча модель демонструє певні функціональні обмеження, які потребують системного вирішення.

Зокрема, слід відзначити, що функціональне навантаження на Уповноваженого Верховної Ради України з прав людини охоплює численні напрями правозахисної діяльності, які виходять далеко за межі проблематики захисту персональних даних. Така широка компетенція об'єктивно знижує потенціал результативного нагляду в цій специфічній галузі. Як справедливо зазначає Бем Маркян, «значне функціональне перевантаження Комітету Верховної Ради України з прав людини у сфері захисту персональних даних негативно впливає на продуктивність його діяльності та унеможливлює повноцінне здійснення його адміністративних та наглядових повноважень» [17].

У законодавчій практиці європейських держав компетенція щодо контролю за дотриманням нормативних вимог у сфері персональних даних переважно зосереджена в спеціалізованих інституціях, які концентруються виключно на цій проблематиці. Показовими прикладами є: Національна комісія з інформатики і свобод (Commission Nationale de l'Informatique et des Libertés, CNIL) у Французькій Республіці, Федеральний уповноважений із захисту даних та свободи інформації (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, BfDI) у Федеративній Республіці Німеччина, а також Орган із захисту даних (Garante per la protezione dei dati personali) в Італійській Республіці.

Оптимальною інституційною моделлю для України може стати формування автономного державного органу, відповідального за сферу захисту персональних даних, з належним обсягом повноважень та ресурсним забезпеченням для ефективної реалізації контрольно-наглядових функцій. Така інституція могла б функціонувати або як цілком незалежна структура, або як спеціалізований підрозділ у системі Офісу Уповноваженого Верховної Ради України з прав людини, наділений розширеними компетенціями.

Іншим аспектом удосконалення інституційних механізмів є оптимізація координації між державними органами, що здійснюють діяльність, пов'язану з регулюванням персональних даних. Це означає формування ефективних каналів взаємодії між Комітетом Верховної Ради України з прав людини, регуляторами у різних галузях (такими як Національний банк України, Державна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації тощо), правоохоронними органами та органами судової влади.

Паралельно з інституційним реформуванням важливого значення набуває розвиток саморегулятивних механізмів у цьому сегменті, що включає формування галузевих етичних стандартів, запровадження сертифікаційних процедур для систем захисту персональних даних тощо. Як справедливо підкреслює І. В. Ковбас, «інструменти саморегулювання становлять важливий комплементарний елемент до державного нагляду у сфері захисту персональних даних, оскільки забезпечують врахування галузевої специфіки та впровадження гнучких регуляторних підходів» [2, с. 74–78].

Стрімкий поступ інформаційно-комунікаційних технологій формує принципово нові правові виклики у сфері регулювання відносин щодо персональних даних. Комплекс інноваційних технологічних феноменів, серед яких аналітика великих масивів даних (Big Data), системи штучного інтелекту, екосистема пристроїв Інтернету речей, хмарні обчислювальні платформи, розподілені реєстри на основі блокчейн-технологій та інші авангардні цифрові рішення, кардинально трансформують методологію опрацювання персоніфікованої інформації та генерують безпрецедентні ризики для інформаційного суверенітету суб'єктів персональних даних.

У парадигмі технологій Big Data особливої гостроти набуває проблематика дотримання фундаментальних принципів опрацювання персональної інформації, насамперед принципу мінімізації обсягів збору даних та принципу цільового обмеження їх використання. Функціонування систем аналітики великих даних ґрунтується на акумуляції та опрацюванні колосальних інформаційних масивів, часто без попередньої конкретизації цільового призначення на момент первинного збору. Подібна практика входить у концептуальне протиріччя з традиційними доктринальними підходами до правового захисту персональних даних.

Технології штучного інтелекту також породжують комплекс фундаментальних викликів у системі правового регулювання персональних даних. Алгоритмічні структури машинного навчання демонструють здатність ідентифікувати неявні закономірності та формувати прогностичні моделі на основі персоніфікованої інформації, що потенційно створює передумови для алгоритмічної дискримінації та інших форм порушення прав суб'єктів даних. Додатковою проблемою виступає характерна для багатьох систем штучного інтелекту непрозорість процесів формування рішень та складність їх інтерпретації, що суттєво ускладнює механізми юридичного оскарження автоматизованих рішень, ухвалених подібними системами.

Концепція Інтернету речей (IoT) передбачає інтеграцію різноманітних пристроїв до глобального інформаційного простору, що генерує специфічні ризики в контексті забезпечення безпеки персональних даних. Така архітектура значно ускладнює практичну реалізацію ключових прав суб'єктів персональних даних, зокрема права на інформаційну обізнаність щодо процесів опрацювання їхніх даних та права на добровільне та інформоване волевиявлення щодо такого опрацювання.

Впровадження хмарних обчислювальних платформ та розподілених реєстрів на основі блокчейн-технологій також актуалізує низку правових дилем у системі регулювання

персональних даних, зокрема питання юрисдикційного характеру, забезпечення інформаційної безпеки персоніфікованих даних та практичних механізмів реалізації права на остаточне видалення інформації.

З огляду на окреслену проблематику, нагальною необхідністю постає модернізація системи правового регулювання відносин щодо персональних даних з урахуванням викликів цифрової епохи. Це охоплює такі стратегічні напрями:

− формування спеціалізованого нормативного інструментарію щодо регламентації процесів опрацювання персональних даних у середовищі технологій великих даних, систем штучного інтелекту, інфраструктури Інтернету речей та інших інноваційних технологічних платформ;

− імплементація концептуального підходу «приватність за архітектурним задумом» (privacy by design), що передбачає інтеграцію механізмів захисту інформаційної приватності в архітектуру технологічних рішень ще на стадії їх проєктування та розробки;

− стимулювання розвитку технологій підвищення інформаційної конфіденційності (privacy enhancing technologies), функціонал яких спрямований на мінімізацію ризиків порушення інформаційних прав суб'єктів персональних даних;

− розробка методологічних підходів до забезпечення інтерпретованості рішень, генерованих алгоритмічними системами штучного інтелекту;

− трансформація механізмів практичної реалізації правових можливостей суб'єктів персональних даних з урахуванням специфіки сучасного технологічного ландшафту.

В умовах глобалізації обробки інформації та інтенсифікації транскордонного переміщення персональних даних розвиток міжнародного співробітництва у сфері захисту персональних даних має стратегічне значення. Хоча Україна є стороною Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року [5], питання поглиблення міжнародного співробітництва у цій сфері залишається актуальним.

Пріоритетним вектором міжнародного співробітництва виступає інтеграція України до регуляторних механізмів, передбачених Загальним регламентом про захист даних (GDPR), насамперед до системи визнання адекватності рівня захисту персональних даних. Реалізація цього завдання сприятиме суттєвому спрощенню процедур транскордонної передачі персональних даних між Україною та державами-членами Європейського Союзу. Досягнення цієї мети потребує комплексної гармонізації національного нормативно-правового поля з вимогами GDPR та забезпечення дієвого механізму імплементації відповідних норм.

Додатковим перспективним напрямом виступає розвиток інституційної співпраці України з Європейською радою із захисту даних (European Data Protection Board, EDPB) – колегіальним органом, який забезпечує координацію діяльності національних регуляторів у сфері захисту персональних даних держав-членів ЄС та сприяє уніфікованому застосуванню стандартів інформаційної приватності у європейському правовому просторі.

Активізація міжнародної взаємодії у галузі захисту персональних даних становить стратегічно важливий напрямок для України. Особливо цінною видається інтеграція до Глобальної мережі забезпечення приватності (Global Privacy Enforcement Network, GPEN), яка функціонує як платформа для регуляторних органів різних держав. Участь у цьому об'єднанні забезпечує можливість інтенсивного обміну практичним досвідом, інноваційними підходами та координації спільних зусиль у сфері забезпечення приватності даних.

Еволюція нормативно-правового регулювання персональних даних на території України віддзеркалює загальносвітові тенденції розвитку інформаційного суспільства та процеси євроінтеграції. Ретроспективний аналіз дозволяє виділити чотири фундаментальні етапи становлення законодавчої бази:

– Фундаментальний період (1991–2010 рр.) – формування базових юридичних положень щодо інформаційної безпеки та охорони персональних відомостей громадян.

– Етап систематизації спеціалізованої нормативної бази (2010–2014 рр.) – впровадження основоположного Закону України «Про захист персональних даних» і запуск первинних регуляторних механізмів.

– Період трансформації інституційної архітектури (2014–2018 рр.) – модернізація національного законодавства з інтеграцією міжнародних стандартів та делегування контрольних функцій Уповноваженому Верховної Ради України з прав людини.

– Етап гармонізації з європейськими нормативами (з 2018 р. дотепер) – синхронізація законодавчого поля України з вимогами GDPR та зміцнення інституційних важелів моніторингу за дотриманням правових норм у сфері персональних даних.

Кожен із зазначених етапів характеризується відмінними особливостями правового регулювання і механізмів гарантування приватності. Загальна динаміка демонструє послідовну конвергенцію нормативно-правової бази України з європейськими стандартами, насамперед із положеннями Загального регламенту про захист даних (GDPR).

В адміністративно-правовому аспекті система регулювання захисту персональних даних охоплює організацію державного нагляду, засоби забезпечення дотримання вимог законодавства та адміністративну відповідальність за порушення стандартів обробки персональних даних. На сучасному етапі основним наглядовим органом є Комітет з прав людини Верховної Ради України, який уповноважений здійснювати контрольні функції та ініціювати притягнення до адміністративної відповідальності суб'єктів, які порушують вимоги законодавства.

Стратегічні напрямки вдосконалення нормативно-правового регулювання персональних даних в Україні включають:

− транспонування положень GDPR до національної правової системи та забезпечення їх належної імплементації;

− оптимізацію інституційних механізмів державного контролю та підвищення їх результативності;

− актуалізацію законодавства відповідно до викликів цифрової трансформації, зумовлених прогресом інноваційних технологій, зокрема великих даних (Big Data), систем штучного інтелекту, Інтернету речей тощо;

− інтенсифікацію міжнародної співпраці у секторі забезпечення приватності, включаючи конвергенцію правових норм із міжнародними стандартами.

Вагоме значення має розбудова інструментів саморегулювання у сфері обробки персональних даних. Цей напрямок передбачає заохочення розробки галузевих кодексів поведінки, запровадження систем добровільної сертифікації механізмів захисту даних, а також налагодження конструктивного діалогу між підприємницькими структурами та державними інституціями для формування ефективних політик захисту персональної інформації.

В умовах прискорення цифрової трансформації особливу увагу необхідно приділяти адаптації правового регулювання до новітніх технологічних викликів. З цією метою важливо розробити спеціальну нормативну базу для обробки персональних даних в умовах функціонування систем штучного інтелекту, екосистеми Інтернету речей, технології блокчейн та платформ хмарних обчислень.

Висновки. Таким чином, правове регулювання персональних даних в Україні зазнає поступової еволюції, що відображає як внутрішньодержавні трансформації політичного курсу, так і глобальні тенденції у сфері захисту приватності. Подальша траєкторія розвитку законодавства визначатиметься необхідністю дотримання європейських стандартів, забезпечення ефективного захисту прав громадян в епоху цифровізації та посилення міжнародної кооперації у сфері гарантування інформаційної безпеки.

Список використаних джерел:

1. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481.

2. Ковбас І. В. "Адміністративно-процесуальна правосуб'єктність громадян." Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького 11 (2015): 74-78.

3. Конституція України від 28.06.1996. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

4. Про інформацію: Закон України від 02.10.1992 № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650.

5. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981. *Офіційний вісник України*. 2011. № 1. Ст. 85.

6. Про утворення Державної служби України з питань захисту персональних даних: Указ Президента України від 09.12.2010 № 1085/2010. *Офіційний вісник України*. 2010. № 94. Ст. 3334.

7. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-X. *Відомості Верховної Ради* УРСР. 1984. Додаток до № 51. Ст. 1122.

8. Про затвердження Положення про Державний реєстр баз персональних даних та порядок його ведення: Постанова Кабінету Міністрів України від 25.05.2011 № 616. *Офіційний вісник України*. 2011. № 41. Ст. 1671.

9. Про затвердження Порядку повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних: Наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14. *Офіційний вісник України*. 2014. № 16. Ст. 499.

10. Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних: Закон України від 03.07.2013 № 383-VII. *Відомості Верховної Ради України*. 2014. № 14. Ст. 252.

11. Про затвердження Типового порядку обробки персональних даних: Наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14. *Офіційний вісник України*. 2014. № 16. Ст. 499.

12. 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. *Офіційний вісник України*. 2014. № 16. Ст. 499.

13. 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). URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text

14. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Угода від 27.06.2014. *Офіційний вісник України*. 2014. № 75. Ст. 2125.

15. Ковбас І. В. "Щодо функцій органів місцевого самоврядування як суб'єктів адміністративного права." *Юридичний науковий електронний журнал* 2 (2015): 135-138.

16. Про звернення громадян: Закон України від 02.10.1996 № 393/96-ВР. *Відомості Верховної Ради України*. 1996. № 47. Ст. 256.

17. Бем, Маркіян, and Іван Городиський. "Відповідальність за порушення законодавства про захист персональних даних: проблеми відповідності законодавства України вимогам регламенту Європейського Союзу щодо захисту персональних даних (GDPR)." *Law of Ukraine/Pravo Ukraini* 2 (2019).