УДК 347.1:342.738:341.171
DOI https://doi.org/10.51989/NUL.2026.3.9

ІМПЛЕМЕНТАЦІЯ СТАНДАРТІВ GDPR У ЦИВІЛЬНЕ ЗАКОНОДАВСТВО УКРАЇНИ



Мельник Андрій Володимирович,
orcid.org/0000-0001-6016-6422
кандидат юридичних наук, доцент,
доцент кафедри цивільного права та процесу юридичного факультету
Львівського національного університету імені Івана Франка

У статті обґрунтовано цивілістичну модель імплементації стандартів Загального регламенту про захист даних у законодавство України. Проблема полягає не у відсутності в національному праві будь-яких норм про інформацію щодо фізичної особи, а у фрагментарності їх системного зв'язку з конструкціями особистих немайнових прав, правочинів, зобов'язань і цивільно-правового захисту. Метою дослідження є визначення критеріїв, за якими окремі приписи GDPR мають бути відображені у Цивільному кодексі України, конкретизовані спеціальним законом або залишені поза межами цивільно-правової кодифікації. Методологічну основу становлять формально-юридичний, системно-структурний, порівняльно-правовий і функціональний методи, а також аналіз практики Конституційного Суду України, Великої Палати Верховного Суду, Суду Європейського Союзу та Європейського суду з прав людини. Доведено, що критерієм цивільно-правової імплементації є не формальна належність положення до GDPR, а його функція у визначенні суб'єктивного права, меж приватної автономії, змісту приватного обов'язку або способу відновлення порушеного становища. На цій підставі запропоновано розмежовувати: основоположні цивільно-правові гарантії, які доцільно закріпити у ЦК України; спеціальні регуляторні правила, що мають міститися у законі про захист персональних даних; інституційні та адміністративно-деліктні механізми, які не належать до предмета цивільної кодифікації. Обґрунтовано, що право на захист персональних даних має бути сконструйоване як особисте немайнове право з відкритим, але юридично визначеним набором правомочностей. Згода розглядається як одностороннє волевиявлення, дійсність якого не усуває обов'язків контролера і не перетворює дані на об'єкт власності. Запропоновано дворівневу модель регулювання: ЦК України повинен визначати правовий статус фізичної особи, межі договору та цивільні способи захисту, а спеціальний закон – процедури, організаційні обов'язки, нагляд і санкції.

Ключові слова: *персональні дані, цивільне законодавство, особисті немайнові права, імплементація, згода, приватна автономія, цивільно-правовий захист, моральна шкода.*

Melnyk Andrii. Implementation of GDPR Standards into the Civil Legislation of Ukraine

The article develops a private-law model for implementing the standards of the General Data Protection Regulation into Ukrainian legislation. The central problem is not the complete absence of national rules concerning information about an individual, but the fragmented relationship of those rules with the doctrines of personal non-property rights, transactions, obligations and civil remedies. The purpose of the study is to identify the criteria according to which individual GDPR standards should be incorporated into the Civil Code of Ukraine, specified in special legislation, or remain outside civil-law codification. The research employs formal legal, systemic, comparative and functional methods and analyses the case law of the Constitutional Court of Ukraine, the Grand Chamber of the Supreme Court, the Court of Justice of the European Union and the European Court of Human Rights. It is argued that the relevant criterion is not the formal location of a provision in the GDPR but its legal function in defining a subjective right, the limits of private autonomy, a private duty or a remedy restoring an infringed legal position. The article therefore distinguishes between fundamental private-law guarantees suitable for inclusion in the Civil Code, detailed regulatory rules that should remain in personal data protection legislation, and institutional or administrative enforcement mechanisms that do not belong to civil-law codification. The right to personal data protection should be constructed as a personal non-property right with an open but legally determinable set of entitlements. Consent is characterised as a unilateral legally relevant declaration of will whose validity neither removes the controller's duties nor turns personal data into property. A two-level model is proposed: the Civil Code should determine the individual's private-law status, limits of contractual autonomy and civil

remedies, while special legislation should regulate procedures, organisational duties, supervision and sanctions.

Key words: *personal data, civil legislation, personal non-property rights, implementation, consent, private autonomy, civil remedies, non-pecuniary damage.*

Постановка проблеми. Стаття 15 Угоди про асоціацію орієнтує Україну на належний рівень захисту персональних даних відповідно до європейських і міжнародних стандартів [1]. Проте це зобов'язання не вимагає відтворення у ЦК України структури Регламенту (ЄС) 2016/679 (GDPR) [2]. Регламент поєднує права суб'єкта даних, підстави обробки, приватні й організаційні обов'язки, нагляд, санкції та судовий захист. Тому належність припису до GDPR сама по собі не обґрунтовує його включення до цивільної кодифікації.

Конституційною основою захисту є стаття 32 Конституції України [3], зміст якої конкретизовано у Рішенні Конституційного Суду України № 2-рп/2012 [4]. ЦК України охороняє інформаційну сферу особи у статтях 200, 277, 285, 286, 296, 299, 301 і 302 [5]; закони України «Про захист персональних даних» та «Про інформацію» визначають спеціальні права, підстави обробки й режим конфіденційної інформації [6; 7]. Отже, проблема полягає у фрагментарності регулювання та відсутності системного розмежування особистого немайнового права, приватноправових обов'язків і публічно-правових механізмів. Законопроєкт № 8153 може свідчити про напрям реформи, але до набрання чинності не є нормативною підставою [8].

Аналіз останніх досліджень і публікацій. Ю. О. Заіка та В. Л. Скрипник пояснюють нематеріальний характер інформації, її відтворюваність і залежність режиму від змісту та доступу [9, с. 240–245]. С. О. Сліпченко розмежовує нематеріальність блага і немайновий характер правового зв'язку [10, с. 87–92], що не дозволяє ототожнювати комерційну цінність даних із правом власності на них. Ю. Бєлова визначає добровільність, поінформованість, конкретність та однозначність умовами дійсності згоди [11, с. 14–18]. О. А. Тимошенко пов'язує цивільно-правовий захист даних із гарантіями статті 8 Конвенції та ефективністю припинення порушення і компенсації [12, с. 165–172]. Водночас критерій віднесення окремих стандартів GDPR до ЦК України та модель його узгодження зі спеціальним законом залишаються недостатньо визначеними.

Мета і методологія дослідження. Метою статті є обґрунтування критерію цивільно-правової імплементації стандартів GDPR і дворівневої моделі узгодження ЦК України зі спеціальним законом. Формально-юридичний, системно-структурний, порівняльно-правовий і функціональний методи використано для розмежування суб'єктивного права, приватного обов'язку, регу-ляторної вимоги та санкції; метод правового моделювання – для визначення їх місця у законодавстві. Враховано автономне закріплення приватності й захисту даних у статтях 7 і 8 Хартії ЄС [21] та модернізовані стандарти Конвенції 108 [22].

Виклад основного матеріалу. Імплементація як функціональна адаптація. Включенню до ЦК України підлягає стандарт, основна функція якого полягає у визначенні правового становища фізичної особи, меж приватної автономії, змісту обов'язку приватного учасника або способу відновлення порушеного права. Термінологія, процедури здійснення прав, документаційні та безпекові вимоги мають конкретизуватися спеціальним законом; статус наглядового органу, перевірки й адміністративні штрафи перебувають поза предметом цивільної кодифікації. Такий критерій запобігає як розчиненню особистого немайнового права в адміністративному контролі, так і перевантаженню Кодексу мінливими процедурами.

Функціональна адаптація передбачає також цивілістичну кваліфікацію європейських конструкцій. Право на видалення може виступати способом здійснення права, коли особа звертається до контролера, і способом захисту – за відмови припинити неправомірне зберігання. Підзвітність контролера є організаційним принципом, але створені на його виконання документи мають доказове значення у спорі. Порушення безпеки породжує регуляторний обов'язок повідомлення і водночас може стати юридичним фактом деліктного зобов'язання. Отже, один стандарт здатний мати кілька галузевих проявів, однак до ЦК України включається лише його стабільне приватноправове ядро.

Практичне значення функціонального критерію полягає у розподілі складових стандарту GDPR між рівнями регулювання. До ЦК України має включатися його стабільне приватноправове ядро: суб'єктивне право, межа автономії, приватний обов'язок, спосіб захисту

або умова відповідальності. Порядок здійснення прав, організаційні вимоги, нагляд і санкції належать спеціальному закону [2]. Отже, належність припису до одного акта ЄС не виключає різної галузевої форми його відтворення у національному праві. Це запобігає дублюванню, підтримує системність цивільної кодифікації та дозволяє оновлювати процедури без зміни цивільно-правового статусу особи.

Право на захист персональних даних і межі приватної автономії. Статті 270, 275, 301 і 302 ЦК України частково охоплюють інформаційну автономію, але не утворюють цілісного права на захист персональних даних. Його доцільно закріпити як особисте немайнове право, що охоплює правомочності знати про факт, мету і підставу обробки; одержувати доступ і копію; вимагати виправлення; заперечувати; припиняти незаконну обробку; домагатися видалення за наявності підстав; вимагати людського перегляду істотного автоматизованого рішення. Це право не означає абсолютного контролю над будь-яким згадуванням особи: його здійснення узгоджується із законом, правами інших осіб та пропорційністю.

Самостійність цього права зумовлена його змістом: приватність охороняє особисту сферу від непропорційного втручання, а захист даних надає позитивні правомочності щодо правомірно одержаних відомостей [21]. Доступ є лише передумовою контролю, тому це право не зводиться до права на інформацію. Економічне використання даних не створює речового панування [9, с. 240–245; 10, с. 87–92]. Можливість стягнення збитків або моральної шкоди характеризує наслідки порушення, а не змінює природи самого права. Відкрите коло правомочностей охоплює нові способи обробки без постійного розширення Кодексу, зберігаючи немайновий характер правового зв’язку.

Згода є одностороннім юридично значущим волевиявленням, а не універсальною підставою обробки чи способом передання даних у власність. Вона легітимує лише визначену обробку в межах повідомленої мети; її дійсність залежить від реальної свободи вибору, поінформованості, конкретності й однозначності [11, с. 14–18]. Згода не усуває обов’язків контролера щодо добросовісності, мінімізації та безпеки. Її відкликання діє на майбутнє, однак контролер не може довільно замінити відкликану згоду іншою підставою без перевірки умов її застосування.

Договірна необхідність охоплює лише операції, без яких об’єктивно неможливо надати основну послугу. Включення обробки до стандартних умов саме по собі не робить її необхідною. Договором не можна скасувати доступ, надати невизначений дозвіл на будь-які майбутні цілі, виключити припинення незаконної обробки або наперед усунути відповідальність за умисне порушення. Такі умови мають оцінюватися з урахуванням імперативної природи особистого немайнового права, добросовісності та заборони зловживання правом.

Включення згоди до тексту договору не перетворює її на договірну умову: вона залишається окремим одностороннім волевиявленням із можливістю відкликання. Відмова від факультативної обробки не повинна перешкоджати отриманню основної послуги, а стандартні умови не можуть штучно конструювати договірну необхідність [2; 11, с. 14–18]. Інакше контролер одержав би змогу обходити вимогу добровільності простим включенням надмірної операції до типового договору. Невизначені цілі, об’єднання несумісних операцій або попередня відмова від прав мають оцінюватися з позицій імперативних вимог, добросовісності, дійсності правочину та заборони зловживання правом [5].

Доступ, копія та інформація про одержувачів. У справі C-487/21 CRIF Суд ЄС встановив, що копія має забезпечити зрозуміле й повне відтворення персональних даних; витяги з документів або баз надаються настільки, наскільки це необхідно для ефективного здійснення прав [13]. Для українського права це визначає мінімальний зміст доступу: не формальну довідку, а інформацію, достатню для перевірки законності обробки. У справі C-154/21 Österreichische Post Суд визнав право знати конкретних одержувачів, якщо їх можливо ідентифікувати; категорії достатні лише за об’єктивної неможливості або явно необґрунтованого запиту [14]. Отже, доступ виконує не лише інформаційну, а й доказово-забезпечувальну функцію.

Із цих рішень випливає, що обсяг відповіді не може визначатися винятково формою зберігання даних або внутрішньою будовою інформаційної системи. Контролер повинен надати зміст персональних даних у формі, яка дозволяє особі зіставити їх із метою, джерелом, строком зберігання та колом одержувачів. Водночас право на копію не тотожне безумовному праву на весь документ: права й свободи інших осіб можуть зумовити ретушування або надання

витягу, але не позбавлення відповіді практичної корисності. У ЦК України доцільно закріпити саму правомочність доступу, тоді як строки, електронна форма, перевірка особи заявника та випадки плати за повторні запити мають залишатися у спеціальному законі.

Автоматизовані рішення. У справі C-634/21 SCHUFA Суд ЄС кваліфікував скорингове значення як автоматизоване рішення, коли третя сторона надає йому визначальне значення під час укладення або виконання договору [15]. Для цивільного права алгоритмічна оцінка може бути елементом формування волі контрагента й істотно впливати на доступ до кредиту, страхування, оренди чи іншої послуги. Тому ЦК України має гарантувати людський перегляд рішення з правовими або подібними істотними наслідками, можливість висловити позицію та оскаржити результат; спеціальний закон – визначити критерії автоматизованості, обсяг пояснення логіки й процедуру перегляду.

Ця гарантія не забороняє використання алгоритмів і не перетворює будь-яке автоматизоване обчислення на юридичне рішення. Визначальними є відсутність змістовного людського втручання та істотність наслідків для особи. Формальне підтвердження результату працівником, який не має повноважень змінити його, не є людським переглядом. Цивільно-правове значення пояснення полягає у можливості виявити помилкові дані, дискримінаційний критерій або неналежне врахування обставин, після чого вимагати виправлення, повторної оцінки чи відшкодування шкоди. Отже, гарантія поєднує здійснення особистого немайнового права з контролем за формуванням волі сторони договору.

Цивільно-правові способи захисту і компенсація шкоди. Відкриті переліки статей 16 і 275 ЦК України дозволяють пристосувати спосіб захисту до характеру обробки. Визнання права доречне за заперечення статусу суб’єкта або доступу; припинення дії – щодо незаконного збирання, використання, передання чи зберігання; відновлення становища – через виправлення, обмеження доступу, відкликання даних від одержувачів або видалення. Можливі також спростування недостовірної інформації, відшкодування майнової та моральної шкоди. Спосіб має усувати конкретне порушення, а не створювати надмірне обмеження правомірного обігу інформації.

Вибір вимоги залежить від стадії порушення. За реальної загрози незаконного розкриття пріоритетним є запобігання; під час триваючої обробки – її припинення або обмеження; після передання третім особам – повідомлення одержувачів і відкликання даних; за збереження недостовірного профілю – виправлення та повторний розгляд рішення. Поєднання кількох способів допустиме, якщо кожен усуває окремий наслідок і не веде до подвійного відшкодування. Така диференціація має бути відображена не у вичерпному спеціальному переліку, а через загальну норму ЦК України, яка дозволяє суду пристосувати захист до змісту правомочності та характеру обробки.

Захист конкретизується за стадією порушення: реальна загроза обґрунтовує запобігання, триваюча обробка – припинення або обмеження, неточність – виправлення, а передання даних – повідомлення одержувачів. Видалення потребує матеріально-правової підстави; ретушування може зберегти правомірний зміст документа [18]. Істотне автоматизоване рішення допускає вимогу про людський перегляд, а доведені наслідки – компенсацію [5]. Вимога про перегляд спрямована на повторне індивідуальне оцінювання, тому не поглинається виправленням окремих даних. Кілька способів можуть поєднуватися, якщо кожен усуває самостійний наслідок і їх сукупність не створює подвійного відшкодування.

У постанові від 9 квітня 2024 року у справі № 925/1440/22 Велика Палата Верховного Суду поєднала право співвласника на інформацію про діяльність ОСББ із конфіденційністю інших осіб: документи підлягають наданню після ретушування закритих персональних даних [18]. Для теми статті це підтверджує вимогу пропорційності: видалення даних не завжди потребує знищення документа або повної відмови в доступі; належним способом може бути вилучення лише конфіденційних фрагментів.

Стаття 82 GDPR пов’язує компенсацію з порушенням, шкодою та причинним зв’язком [2]. У справі C-300/21 Österreichische Post Суд ЄС відкинув як автоматичну компенсацію за саме порушення, так і вимогу мінімального порогу серйозності нематеріальної шкоди [16]. Український суд, застосовуючи статті 22, 23, 1166 і 1167 ЦК України, має встановлювати конкретний негативний наслідок: втрату контролю, обґрунтовану тривогу, репутаційну шкоду, дискримінаційний ефект, витрати на відновлення безпеки або інший доведений вплив.

У справі C-340/21 Natsionalna agentsia za prihodite Суд ЄС визнав, що обґрунтований страх майбутнього зловживання даними може становити

нематеріальну шкоду, а факт кібератаки сам по собі не доводить неналежності заходів безпеки; відповідність цих заходів має довести контролер [17]. Для українського права це вимагає розмежовувати доказування шкоди потерпілим і доказування належної поведінки контролером, у розпорядженні якого перебувають журнали доступу, оцінки ризиків та інша внутрішня документація. Адміністративний штраф не замінює компенсації, оскільки має каральну й превентивну, а не відновлювальну функцію.

Практика ЄСПЛ визначає межі втручання і позитивних обов'язків. У справі S. and Marper v. the United Kingdom Суд визнав втручанням саме зберігання біометричних даних, а безстрокове й загальне зберігання даних незасуджених осіб — непропорційним [19, пункти 67, 103–125]. В Antović and Mirković v. Montenegro гарантії статті 8 Конвенції поширено на відеоспостереження у професійному середовищі [20, пункти 40–45]. Для цивільного права ці рішення вимагають оцінювати законну підставу, визначеність мети, передбачуваність, необхідність і пропорційність, а не виходити з абсолютної заборони зберігання чи спостереження.

Модель узгодження ЦК України та спеціального закону. ЦК України має стабільно визначати право на захист персональних даних як особисте немайнове, його базові правомочності, межі згоди й договору, гарантії щодо автоматизованих рішень, способи захисту та право на компенсацію. Спеціальний закон повинен регулювати принципи і підстави обробки, статус контролера та оператора, строки й форми відповіді, документацію, оцінку впливу, безпеку, повідомлення про порушення, міжнародне передання, нагляд і санкції.

Рівні взаємодіють: порушення спеціального обов'язку може доводити цивільну протиправність; рішення наглядового органу – мати доказове значення; спеціальне правило – конкретизувати стандарт належної поведінки. Проте адміністративний припис не замінює цивільного відновлення, а спеціальний закон не повинен закривати перелік способів захисту всупереч статтям 16 і 275 ЦК України. Доцільною є окрема стаття або компактна група статей у книзі другій ЦК України без дублювання процедур. Предметна, функціональна, системна, автономна, пропорційна та вимога правової визначеності окреслюють межі такої кодифікації.

Порушення спеціального обов'язку може підтверджувати цивільну протиправність, а рішення наглядового органу – мати доказове значення у цивільному процесі. Проте виконання адміністративного припису не позбавляє права на позов, а штраф не замінює відновлення чи компенсації. Так само відсутність адміністративного рішення не повинна бути обов'язковою передумовою судового захисту особистого немайнового права. Спеціальний закон має конкретизувати здійснення права без закриття переліку способів захисту всупереч статтям 16 і 275 ЦК України [5; 6]. Перевагою дворівневої моделі є стабільність кодифікованих гарантій за можливості оперативно оновлювати процедури відповідно до технологічних ризиків.

Висновки. 1. Критерієм цивільно-правової імплементації є функція стандарту GDPR: визначення суб'єктивного права, меж приватної автономії, приватноправового обов'язку або способу відновлення порушеного становища. Механічне відтворення структури Регламенту не відповідає системі ЦК України.

2. Конституція України, ЦК України та спеціальні закони містять окремі гарантії, але не утворюють завершеної цивілістичної моделі захисту персональних даних; фрагментарність стосується передусім змісту права, обов'язків приватних осіб і способів захисту.

3. У ЦК України доцільно закріпити особисте немайнове право на захист персональних даних із правомочностями на інформацію, доступ, копію, виправлення, заперечення, припинення незаконної обробки, видалення за наявності підстав і людський перегляд істотного автоматизованого рішення.

4. Згода є одностороннім волевиявленням, а не універсальною підставою обробки чи переданням даних у власність. Договір не може усувати сутнісні правомочності суб'єкта, невизначено розширювати цілі обробки або звільняти контролера від імперативних обов'язків.

5. Спосіб цивільно-правового захисту має бути ефективним і пропорційним: поряд із припиненням обробки та видаленням можливі виправлення, обмеження доступу, відкликання даних від одержувачів, ретушування конфіденційних фрагментів, спростування та компенсація.

6. Компенсація потребує встановлення порушення, шкоди та причинного зв'язку; формальне порушення не є достатнім, але нематеріальна шкода не залежить від наперед установленого порогу серйозності. Обґрунтований страх майбутнього зловживання може бути шкодою, тоді як належність заходів безпеки доводить контролер.

7. Оптимальною є дворівнева модель: ЦК України закріплює базові приватно-

правові гарантії, межі автономії, способи захисту й відповідальність; спеціальний закон – процедурні, організаційні, наглядові та санкційні механізми.

ЛІТЕРАТУРА:

1. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, від 27 червня 2014 року. URL: https://zakon.rada.gov.ua/laws/show/984_011 (дата звернення: 18.06.2026).
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. Official Journal of the European Union. 2016. L 119. P. 1–88. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (date of access: 18.06.2026).
3. Конституція України : Закон України від 28 червня 1996 року № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 18.06.2026).
4. Рішення Конституційного Суду України від 20 січня 2012 року № 2-рп/2012. URL: https://ccu.gov.ua/sites/default/files/ndf/2-rp/2012.doc (дата звернення: 18.06.2026).
5. Цивільний кодекс України : Закон України від 16 січня 2003 року № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15 (дата звернення: 18.06.2026).
6. Про захист персональних даних : Закон України від 1 червня 2010 року № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 18.06.2026).
7. Про інформацію : Закон України від 2 жовтня 1992 року № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 18.06.2026).
8. Проєкт Закону про захист персональних даних № 8153 від 25 жовтня 2022 року. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/40707 (дата звернення: 18.06.2026).
9. Заіка Ю. О., Скрипник В. Л. Інформація в системі об'єктів цивільних прав. *Підприємництво, господарство і право.* 2017. № 1. С. 240–245.
10. Сліпченко С. О. Місце об'єктів особистих немайнових правовідносин у системі об'єктів цивільного права. *Право і суспільство*. 2013. № 6-2. С. 87–92.
11. Бєлова Ю. Умови дійсності згоди на обробку персональних даних. *Підприємництво, господарство і право.* 2017. № 11. С. 14–18.
12. Тимошенко О. А. Захист персональних даних у цивільних правовідносинах: вітчизняне правове забезпечення крізь призму практики Європейського суду з прав людини. *Аналітично-порівняльне правознавство.* 2023. № 4. С. 165–172. DOI: https://doi.org/10.24144/2788-6018.2023.04.27
13. Judgment of the Court of Justice of the European Union of 4 May 2023, Österreichische Datenschutzbehörde v CRIF GmbH, C-487/21, ECLI:EU:C:2023:369.
14. Judgment of the Court of Justice of the European Union of 12 January 2023, RW v Österreichische Post AG, C-154/21, ECLI:EU:C:2023:3.
15. Judgment of the Court of Justice of the European Union of 7 December 2023, SCHUFA Holding (Scoring), C-634/21, ECLI:EU:C:2023:957.
16. Judgment of the Court of Justice of the European Union of 4 May 2023, UI v Österreichische Post AG, C-300/21, ECLI:EU:C:2023:370.
17. Judgment of the Court of Justice of the European Union of 14 December 2023, VB v Natsionalna agentsia za prihodite, C-340/21, ECLI:EU:C:2023:986.
18. Постанова Великої Палати Верховного Суду від 9 квітня 2024 року у справі № 925/1440/22. URL: https://reyestr.court.gov.ua/Review/118465133 (дата звернення: 18.06.2026).
19. S. and Marper v. the United Kingdom [GC], applications nos. 30562/04 and 30566/04, judgment of 4 December 2008. URL: https://hudoc.echr.coe.int/eng?i=001-90051 (date of access: 18.06.2026).
20. Antović and Mirković v. Montenegro, application no. 70838/13, judgment of 28 November 2017. URL: https://hudoc.echr.coe.int/eng?i=001-178904 (date of access: 18.06.2026).
21. Charter of Fundamental Rights of the European Union. Official Journal of the European Union. 2012. C 326. P. 391–407.
22. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, ETS No. 108; Protocol amending the Convention, CETS No. 223.

Дата першого надходження статті до видання: 01.07.2026
Дата прийняття статті до друку після рецензування: 22.07.2026
Дата публікації (оприлюднення) статті: 26.08.2026

Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)